Algebra 901-902 Notes

Robert Huben
With help from Matt Mills

2015-2016

Contents

List of Named Theorems

Chapter 1

MATH 901

1 Roots of Unity

1.1 Day 1 - August 24

Here we go!

Let $n \geq 1 \in \mathbb{N}$, and let $U_n = \{\omega \in \mathbb{C} : \omega^n = 1\}$. Recall that this is a cyclic group generated by $e^{\frac{2\pi i}{n}}$, or generated by $e^{\frac{2k\pi i}{n}}$ for $\gcd(k, n) = 1$. These generators are called *primitive n-th roots of unity*.

Remark 1. We will typically remember n and let ω be a primitive n-th root of unity. We will use $|\omega|$ to denote the order of ω, i.e. n.

Definition 1. For $n \geq 1$, let $\Phi_n(x) = \prod_{|\omega|=n} (x - \omega)$.

Example 1.

$$\begin{aligned} \Phi_1(x) &= x - 1 \\ \Phi_2(x) &= x + 1 \\ \Phi_4(x) &= x^2 + 1 \end{aligned}$$

Remark 2. Note that $\deg(\Phi_n(x) = \phi(n)$.

Note also that $x^n - 1 = \prod_{|\omega| \text{ dividing } n} (x - \omega) = \prod_{\substack{d \geq 1 \\ d|n}} \prod_{|\omega|=d} (x - \omega) = \prod_{d|n} \Phi_d(x)$.

Lemma 1. $\Phi_n(x) \in \mathbb{Z}[x]$

Proof. Induct on n: Base case is true as $\Phi_1 = x - 1$.

Inductive case: $n > 1$. Let $f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$. By the inductive hypothesis, $f(x) \in \mathbb{Z}[x]$. Note that $x^n - 1 = f(x)\Phi_n(x)$, and note also that $f(x)$ is monic.

Recall that for all rings R, $R[x]$ has a division algorithm for monic polynomials. In this case, there exists a unique $q(x), r(x) \in \mathbb{Z}[x]$ such that $x^n - 1 = f(x)q(x) + r(x)$ and where $\deg(r) < \deg(f)$ or $r(x) = 0$.

But this is also true in $\mathbb{C}[x]$. Since the quotient and remainder are unique, and $f(x)$ divides $x^n - 1$ in $\mathbb{C}[x]$, then there is no remainder, and thus $x^n - 1 = f(x)q(x)$, so $q(x) = \Phi_n(x)$, but $q(x) \in \mathbb{Z}[x]$. $\square$

Theorem 1. $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Assume for sake of contradiction that $\Phi_n(x)$ is reducible in $\mathbb{Q}[x]$. Then by Gauss' Lemma, we can in fact factor it in $\mathbb{Z}[x]$. That is, there exist $f(x), g(x) \in \mathbb{Z}[x]$ (non-constant), such that $\Phi_n(x) = f(x)g(x)$.

Furthermore, we can assume WLOG that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Also, since $\Phi_n(x)$ is monic, then $f(x)$ and $g(x)$ are (WLOG) monic as well.

Recall that the roots of $\Phi_n(x)$ are precisely the primitive n-th roots of unity. Let $\omega \in \mathbb{C}$ be a root of $f(x)$. Then $|\omega| = n$. Let p be any prime such that $p \not| n$. Then $|\omega^p| = n$, so ω^p is a root of $\Phi_n(x)$.

We wish to show that $f(\omega^p) = 0$. If this is not true, then $g(\omega^p) = 0$. Then, ω is a root of $g(x^p) \in \mathbb{Z}[x]$. Note that since $f(x)$ is irreducible, then $f(x) = Min(\omega, \mathbb{Q})$ (that is, it is the unique monic polynomial of least degree for which ω is a root). Then we know that $f(x)|g(x^p)$ (in $\mathbb{Q}[x]$).

Since $f(x)$ is monic, we can argue (as we did in the lemma) that $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$.

Now consider this in $\mathbb{Z}_p[x]$. Then $\overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$. But $\overline{g}(x^p) = \overline{g}(x)^p$ (basically because of the Frobenius Automorphism). Let β be a root of $\overline{f}(x)$ (in some algebraic closure of $\mathbb{Z}_p[x]$). Then $\overline{g}(\beta)^p = 0$, so $\overline{g}(\beta) = 0$.

Then $\overline{\Phi}_n(x) = \overline{f}(x)\overline{g}(x)$ in $\mathbb{Z}_p[x]$. Thus β is a multiple root of $\overline{\Phi}_n(x)$. However, $\overline{\Phi}_n(x)|x^n - 1$. Hence, $x^n - 1 \in \mathbb{Z}_p[x]$ has a multiple root. But p was chosen so that $p \not| n$, so the formal derivative of $x^n - 1$ is nx^{n-1}, which only has roots at $x = 0$ (and 0 is certainly not a root of $x^n - 1$). This is a contradiction.

Thus $f(\omega^p) = 0$. But by the same argument, ω^{p^2} is a root, and so is ω^{p^3}, and so on. But this gives that every primitive n-th root of unity is a root of $f(x)$, so $\deg(f) = \deg(\Phi_n)$, which is a contradiction. $\square$

1.2 Day 2 - August 26

Recall from last class that we proved that each cyclotomic polynomial $\Phi_n(x)$ is irreducible and has integer coefficients.

Example 2. Let's find $\Phi_{12}(x)$. We know it is a divisor of $x^{12} - 1 = (x^6 - 1)(x^6 + 1)$. The roots of $\Phi_{12}(x)$ have order 12, so none of them are roots of $x^6 - 1$ (which have order dividing 6). Thus $\Phi_{12}(x)$ divides $x^6 + 1$. We can factor like so: $x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$. Similarly, the roots of $x^2 + 1$ have order 4, so $\Phi_{12}(x)$ divides $x^4 - x^2 + 1$. But $\Phi_{12}(x)$ is monic and has degree 4, so $\Phi_{12}(x) = x^4 - x^2 + 1$.

Corollary 1. Let E be a splitting field of $x^n - 1$ over $\mathbb{Q}$. Then $[E : \mathbb{Q}] = \phi(n)$.

Proof. We know that $E = \mathbb{Q}(\omega)$ (where $\omega = e^{\frac{2\pi i}{n}}$). Then $[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(Min(\omega, \mathbb{Q})) = \deg \Phi_n(x) = \phi(n)$. $\square$

2 Separable Extensions

Definition 2. Let F be a field, and let $\overline{F}$ be a fixed algebraic closure of F. Let $f(x) \in F[x]$ and let $\alpha \in \overline{F}$ be a root of $f(x)$. If $(x - \alpha)^2 | f(x)$ (in $\overline{F}[x]$), then we say α is a *multiple root* of $f(x)$. Otherwise, α is called a *simple root*.

Proposition 1. If $f(x)$ is a polynomial, then $f(x)$ has no multiple roots (in $\overline{F}$) if and only if $\gcd(f, f') = 1$.

Definition 3. Let $f(x) \in F[x]$ be irreducible. Then $f(x)$ is called *separable* if $f(x)$ has no multiple roots in $\overline{F}$.

Proposition 2. Let $f(x) \in F[x]$ be irreducible. Then (1) if $char F = 0$, then $f(x)$ is separable. Also, (2) if $char F = p$, then $f(x)$ has multiple roots if and only if $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Definition 4. Let E/F be an algebraic extension. An element $\alpha \in E$ is *separable* over F if $Min(\alpha, F)$ is separable. We say E/F is a separable extension if every element of E is separable over F.

Definition 5. A field F is called *perfect* if every algebraic extension of F is separable. (Equivalently, every irreducible polynomial in $F[x]$ is separable.)

Theorem 2. Let F be a field. Then (1) if $char F = 0$, then F is perfect. Also, (2) if $char F = p$, then F is perfect if and only if $F = F^p = \{\alpha^p : \alpha \in F\}$.

Proof. (1) follows immediately from proposition 2.

We shall now prove (2). Suppose F is perfect. Let $\alpha \in F$. Consider $x^p - \alpha \in F[x]$. Let β be a root of $x^p - \alpha$ in $\overline{F}$. Then $\beta^p = \alpha$.

Also, $Min(\beta, F) | x^p - \alpha$. But $x^p - \alpha = x^p - \beta^p = (x-\beta)^p$. Thus $Min(\beta, F) = (x-\beta)^i$ for some $1 \leq i \leq p$. But we assumed F is perfect, so β is separable, so its minimal polynomial has no multiple roots. Thus $i = 1$. But by definition of minimal polynomial, $Min(\beta, F) \in F[x]$, so $x - \beta \in F[x]$, and thus $\beta \in F$. Thus $\alpha = \beta^p \in F^p$.

Therefore, $F \subset F^p$. But the opposite direction, that $F^p \subset F$, is easy, so $F^p = F$.

Conversely, assume $F = F^p$. Suppose for the sake of contradiction that F is not perfect. Then there exists a minimal polynomial $f(x) \in F[x]$ which has multiple roots. So $f(x) = g(x^p)$ for some $g(x) \in F[x]$. Then $f(x) = b_m x^{pm} + b_{m-1}x^{0(m-1)} + ... + b_0$ where the $b_i \in F$. By hypothesis, for each b_i, we can find an $a_i \in F$ such that $b_i = a_i^p$.

Thus $f(x) = (a_m x^m + a_{m-1}x^{m-1} + ... + a_0)^p$. This contradicts the fact that $f(x)$ is irreducible. Thus F is perfect. □

Recall the following: Let E/F be an algebraic extension, and let $\sigma : F \to L$ be a nonzero field map (recall that these must be injective, so we call them embeddings) where L is algebraicly closed. Then, there exists an "extension" or "lifting" of σ to a $\tau : E \to L$ such that $\tau\Big|_F = \sigma$. (You draw this with a diagram too.)

In this context, let $S_\sigma = \{\tau : E \to L \mid \tau\Big|_F = \sigma\}$.

Proposition 3. Let E/F be as above, and let $\sigma : F \to L_1$, $\pi : F \to L_2$ be nonzero field maps. Suppose also L_1 and L_2 are algebraically closed. Then, $|S_\sigma| = |S_\pi|$.

Proof. "Without loss of generality", we can assume that L_1 and L_2 are algebraic closures of $\sigma(F)$ and $\pi(F)$ respectively. We can do this because E/F is algebraic, so $\tau(E)$ will be algebraic over $\sigma(F)$. Thus $\tau(E)$ lies inside the algebraic closure of $\sigma(F)$ inside L_1. We can make a similar argument for L_2.

Consider the following diagram which I can't draw.

The long story short is that we get a $\lambda_1 : L_1 \to L_2$ such that $\lambda\Big|_{\sigma(F)} = \pi\sigma^{-1}$.

We claim that λ is an isomorphism.

This follows because L_1 is an algebraic closure of $\sigma(F)$. Since $\lambda(L_1)$ is an algebraic closure of $\pi(F)$ inside L_2, $L_2/\lambda(L_1)$ is an algebraic extension. As $\lambda(L_1)$ is algebraicly closed, then $L_2 = \lambda(L_1)$. Thus λ is surjective. Also, λ is a field map, so it is automatically injective. Thus λ is an isomorphism.

Let $\tau \in S_\sigma$. Then $\lambda\tau : E \to L_1 \to L_2$ and $\lambda\tau\Big|_F = \lambda(\tau\Big|_F) = \lambda\sigma = \pi\sigma^{-1}\sigma = \pi$. Thus $\lambda\tau \in S_\pi$. This gives a map $\widetilde{\lambda} : S_\sigma \to S_\pi$ by $\widetilde{(}\sigma) = \lambda\sigma$. Similarly we can get an $\widetilde{\lambda^{-1}} : S_\pi \to S\sigma$ by $\widetilde{\lambda^{-1}}(\sigma) = \lambda^{-1}\sigma$. But $\widetilde{\lambda^{-1}}$ and $\widetilde{\lambda}$ are inverses, so $|S_\sigma| = |S_\pi|$.

□

Definition 6. Let E/F be algebraic. The *separable degree* of E/F, denoted $[E : F]_S$ is $|S_\sigma|$ for any embedding $\sigma : F \to L$ (where L is algebraically closed).

In particular, fix an algebraic closure $\overline{E}$ of E. Then $[E : F]_S = |\{\tau : E \to \overline{E} : \tau \text{ fixes } F\}|$. We could denote this as $|S_1|$ if we were feeling funny. We will show next time that the separable degree is multiplicative.

2.1 Day 3 - August 28

Recall from last class that if E/F is an algebraic extension, we use $[E : F]_S$ to denote the separable degree.

Lemma 2. Let E/F be an algebraic extension, and let $\alpha \in E$. Let $f(x) = Min(\alpha, F)$. Then $[F(\alpha) : F]_S =$ number of distinct roots of f(x) in $\overline{F}$. (In particular, if α is separable over F, then $[F(\alpha) : F]_S = \deg f(x) = [F(\alpha) : F]$.

Proof. We know that $[F(\alpha) : F]_S =$ number of distinct embeddings of $F(\alpha) \to \overline{F}$ which fix F. If $\sigma : F(\alpha) \to \overline{F}$ fixes F, then σ is determined by $\sigma(\alpha)$. Note that $f(\sigma(\alpha) = \sigma(f(\alpha)) = \sigma(0) = 0$.

Thus $\sigma(\alpha)$ is a root of $f(x)$ in $\overline{F}$. So $[F(\alpha) : F]_S \leq \#$ of distinct roots of f(x). If $\beta \in \overline{F}$ is a root of $f(x)$, then there exists $\sigma : F(\alpha) \to \overline{F}$ such that $\sigma(\alpha) = \beta$. Thus, $[(\alpha) : F]_S \geq \#$ of distinct roots of f(x). But $f(x)$ is minimal and separable, so it has $\deg f(x)$ distinct roots. □

Proposition 4. Let $K \subset L \subset E$ be fields such that $[E:K]$ is finite. Then $[E:K]_S = [E:L]_S[L:K]_S$. Moreover, $[E:K]_S \leq [E:K]$.

Proof. (Proof of multiplicativity.) Fix an algebraic closure $\overline{E}$ of E. Then $\overline{E} = \overline{L} = \overline{K}$. Let $S = \{\pi : L \to \overline{E} | \pi \text{ fixes } K\}$. Then $|S| = [L:K]_S$.

Given $\pi \in S$, let $T_\pi = \{\tau : E \to \overline{E} | \tau\Big|_L = \pi\}$. The $|T_\pi| = [E:L]_S$. Note also that if $\pi_1 \neq \pi_2$, then T_{π_1} and T_{π_2} are disjoint.

Let $T = \bigcup_{\pi \in S} T_\pi$. Note that every $\sigma \in T$ is a function mapping E to $\overline{E}$, and also fixes K. Furthermore, if $\sigma : E \to \overline{E}$ fixes K, then $\sigma\Big|_L : L \to \overline{E}$ fixes K, so $\sigma\Big|_L = \pi \in S$. Thus $\sigma \in T_\pi \subset T$. Hence $|T| = [E:K]_S$.

Hence $|T| = [E:K]_S$, but $|T| = \displaystyle\sum_{\pi \in S} |T_\pi| = \sum_{\pi \in S} [E:L]_S = [L:K]_S[E:L]_S$. ☐

Proof. (Proof of "moreover".) Since E/K is finite, $E = K(\alpha_1, ...\alpha_n)$. We use induction on n to show that $[E:K]_S \leq [E:K]$.

If $n = 1$, then by the lemma we have have that the $[E:K]_S$ is the number of roots of the minimal polynomial of α_1, and $[E:K]$ is the degree of the polynomial of α_1. But it is an ultra-classical result that the number of roots is less than or equal to the number of degrees.

If $n > 1$, assume the inductive hypothsis. Then let $L = K(\alpha_1, ...\alpha_{n-1})$. Then $E = L(\alpha_n)$. By induction, $[L:K]_S \leq [L:K]$. By the $n = 1$ case, $[E:L]_S \leq [E:L]$, so $[E:K]_S \leq [E:K]$. ☐

Example 3. Let p be a prime and $\mathbb{F}_p$ be the field of p elements. Let t be an indeterminant. Let $E = \mathbb{F}_p(t)$, and $K = \mathbb{F}_p(t^p)$. Then t is algebraic over K, since t is a root of $f(x) = x^p - t^p \in K[x]$.

We claim that in fact, $f(x) = Min(t, K)$. Let $g(x) = Min(t, K)$. Then $g(x)|f(x)$ in $K[x]$, and hence in $E[x]$. However, in $E[x]$, $x^p - t^p = (x-t)^p$. Thus $g(x) = (x-t)^i$ for some $1 \leq i \leq p$. But then $g(x) = x^i - itx^{i-1} + ... \in K[x]$. Thus $-it \in K$. But if $i < p$, then i is a unit in $\mathbb{F}_p$, so $t \in K$. But this is absurd, since $K = \mathbb{F}_p(t^p)$.

Thus $[E:K] = p$. But there is exactly one root of $x^p - t^p$ (namely, $x = t$), so $[E:K]_S = 1$.

Remark 3. Let E/F be algebraic, and let $\alpha \in E$. Then α is separable over F if and only if $[F(\alpha):F]_S = [F(\alpha:F]$. (The proof of this was hidden in the lemma: $[F(\alpha):F]_S$ is the number of distinct roots, which equals $[F(\alpha:F]$ if and only if all the roots are distinct, aka the polynomial is separable.)

Remark 4. Suppose E/F is algebraic and separable, and suppose L is an intermediate field. (It is directly true from definitions that L/F is separable.) Then E/L is separable.

Proof. Let $\alpha \in E$. Let $f(x) = Min(\alpha, F)$, and let $g(x) = Min(\alpha, L)$. Since $f(x) \in L[x]$, and $f(\alpha) = 0$, so $g(x)|f(x)$. But since $f(x)$ is separable, it has no repeated roots, and thus $g(x)$ has no repeated roots. Hence α is separable over L. ☐

Theorem 3. Let E/F be a finite extension. Then E/F is separable if and only if $[E:F]_S = [E:F]$.

Proof. Suppose E/F is separable. Then we can write $E = F(\alpha_1, ..\alpha_n)$. We will now induct on n.

If $n = 1$, then the theorem follows from remark 3.

If $n > 1$, then suppose the inductive hypothesis. Let $L = F(\alpha_1, ...\alpha_{n-1})$. Then $E = L(\alpha_n)$. As E/L is separable by remark 4, then by the inductive hypothesis, $[L:F]_S = [L:F]$. Furthermore, by the $n = 1$ case, $[E:L]_S = [E:L]$. Thus because both degree and separable degrees are multiplicative, $[E:F]_S = [E:F]$.

Conversely, suppose $[E:F]_S = [E:F]$. Let $\alpha \in E$. Then $[E:F(\alpha)]_S[F(\alpha):F]_S = [E_F]_S = [E:F] = [E:F(\alpha)][F(\alpha):F]$. But since $[E:F(\alpha)]_S \leq [E:F(\alpha)]$ and $[F(\alpha):F]_S \leq [F(\alpha):F]$, the the only way for us to have equality when we multiply these is to have equality in both of these expressions. That is, $[F(\alpha):F]_S = [F(\alpha):F]$. By remark 3, we know that α is separable over F. But α was arbitary, so every element is separable, so E is separable.

Robert's alternate proof of the converse: suppose E/F were not separable. Then there would be some $\alpha \in E$ such that $Min(\alpha, F)$ has repeated roots. Then by remark 3, $[F(\alpha):F]_S < [F(\alpha):F]$. By the "moreover" part of the proposition, $[E:F(\alpha)]_S \leq [E:F(\alpha)]$. Combining these two inequalities, we have $[E:F(\alpha)]_S[F(\alpha):F]_S < [E:F(\alpha)][F(\alpha):F]$. But since both separable degree and regular degree are multiplicative, the left hand side is $[E:F]_S$ and the righthand side is $[E:F]$. ☐

Exercise 1. Let $K \subset L \subset E$ be fields with E/K algebraic. Suppose E/L and L/K are separable. Then prove E/K is separable.

Corollary 2. Let $E = F(\alpha_1, ...\alpha_n)$, where each α_i is separable and algebraic over F. Then E/F is algebraic and separable.

Proof. Induct on n. If $n = 1$, then by remark 3, we have that $[F(\alpha_1) : F]_S = [F(\alpha_1) : F]$. But by the theorem, $F(\alpha_1)/F$ is separable.

(Rest of the proof is a sketch.) In the inductive case, we use multiplicativity. □

2.2 Day 4 - August 31

Definition 7. A field F is called *separably closed* if there does not exist an extension field $E \supsetneq F$ such that E/F is algebraic and separable.

Given a field K, a field L is a *separable closure* of K if $L \subset K$ and if L/K is separable algebraic and L is separably closed.

Proposition 5. Let F be a field, and let $\overline{F}$ be a fixed algebraic closure of F. Let $F^{sep} = \{\alpha \in \overline{F} | \alpha \text{ is separable over } F\}$. Then F^{sep} is a field and is a separable closure of F.

Proof. Certainly, F^{sep} contains F. Then it suffices to show that F^{sep} is closed under the four field operations.

Let $\alpha, \beta \in F^{sep}$. Since α, β are separable, then $F(\alpha, \beta)/F$ is separable. But $\alpha+\beta, \alpha-\beta, \alpha\beta, \frac{\alpha}{\beta}$ if $(\beta \neq 0)$ $\in F(\alpha, \beta) \subset F^{sep}$. Thus F^{sep} is closed under these operations, so it is a field.

Suppose E/F^{sep} is an algebraic and separable extension. Without loss of generality, we can assume $E \subset \overline{F}$ (since we can assume everything is happening within a single algebraic closure). We have that E/F^{sep} is separable, and F^{sep}/F is separable, so by homework problem 2 [edit: see immediately below], E/F is separable. That is, every element of E is an element of $\overline{F}$ which is separable over F, so $E \subset F^{sep}$. Thus $E = F^{sep}$. □

Homework Problem 1. *Claim: Let $K \subset F \subset E$ be a tower of fields such that F/K and E/F are algebraic and separable. Then E/K is algebraic and separable.*

Definition 8. Let E, F be subfields of a field L. Then the *compositum* or *join* of E and F is $EF = \bigcap_{\substack{K \text{ subfield of } L \\ E \cup F \subset K}} K$.

Example 4. Let $E = K(\alpha_1, ...\alpha_m) \subset L$ and let $F = K(\beta_1, ...\beta_n) \subset L$. Then $EF = K(\alpha_1, ...\alpha_m, \beta_1, ...\beta_n)$.

Exercise 2. If E/K and F/K are algebraic then EF/K is algebraic. If E/K and F/K are separable then EF/K is separable.

Theorem 4 (Eisenstein's Criterion). Let D be a Unique Factorization Domain, and let $F = Q(D)$ (ie the field of fractions of D). Let $f(x) = a_n x^n + ...a_1 x + a_0 \in D[x]$, and suppose there exists an irreducible element $\pi \in D$ such that $\pi \nmid a_n$, $\pi | a_i$ for all $i < n$, and $\pi^2 \nmid a_0$. Then $f(x)$ is irreducible in $F[x]$.

Proof. Suppose for the sake of contradiction that $f(x)$ is reducible in $F[x]$. By Gauss's Lemma, $f(x)$ is reducible in $D[x]$, so let $f(x) = g(x)h(x)$ be a non-trivial factorization in $D[x]$.

Let $g(x) = b_m x^m + ... + b_0$, and let $h(x) = c_l x^l + ...c_0$. In $(D/(\pi))[x]$, write $\overline{g}(x) = \overline{b}_m x^m + ...\overline{b}_j x^j$ $(\overline{b}_j \neq 0)$, and similarly write $\overline{h}(x) = \overline{c}_l x^l + ...\overline{c}_i x^i$ $(\overline{c}_i \neq 0)$

In $(D/(\pi))[x]$, we have that

$$\begin{aligned} \overline{a}_n x^n &= \overline{f}(x) \\ &= \overline{g}(x)\overline{h}(x) \\ &= (\overline{b}_m x^m + ... + \overline{b}_i x^i)(\overline{c}_l x^l + ...\overline{c}_j x^j) \\ &= \overline{b}_m \overline{c}_l x^n + ... + \overline{b}_i \overline{c}_j x^{i+j} \end{aligned}$$

If $i < m$ or $j < l$, then $\bar{b}_i\bar{c}_j = \bar{0}$ in $D/(\pi)$. But $D/(\pi)$ is a domain since π is prime, so $\bar{b}_i = \bar{0}$ or $\bar{c}_j = \bar{0}$, which contradicts our assumption. Thus $i = m$ and $j = l$. In particular, $\bar{b}_0 = \bar{c}_0 = \bar{0}$, so $\pi | b_0$ and $\pi | c_0$. But $a_0 = b_0c_0$, and thus $\pi^2 | a_0$, which is a contradiction.

□

Proposition 6. Let K be a field and u be a transcendental element over K. Let $F = K(u)$. Then $x^n - u$ is irreducible in $F[x]$ for all $n \geq 1$.

Proof. Let $F = Q(D)$ where $D = K[u]$. Since u is transcendental over K, then $K[u]$ is a polynomial ring, so it is a UFD. Then u is an irreducible element in D, so by Eisenstein's Irreducibility Criterion (with $\pi = u$), $x^n - u$ is irreducible in $F[x]$. □

Example 5. Let K be a field of characteristic $p > 0$. Let u be transcendental over K, and let v be transcendental over $K(u)$.

Let $E = K(u, v)$ and let $F = K(u^p, v^p)$. What is $[E : F]$?

Let $L = K(u, v^p)$. Consider the tower $F \subset L \subset E$. We can see that $Min(v, L) = x^p - v^p$ is irreducible over $K(u, v^p)$ as v^p is transcendental over $K(u)$.

Also, $Min(u, F) = x^p - u^p$, as u^p is transcendental over $K(v^p)$ (take Professor Marley's word for this). Thus $[E : F] = [E : L][L : F] = p^2$.

Remark 5. In the previous example, note that if $g(u, v) \in E$, then $g(u, v)^p \in K^p(u^p, v^p) \subset K(u^p, v^p) = F$. Thus $Min(g(u, v), F) | x^p - g(u, v)^p$, so $[F(g(u, v)) : F] \leq p$ for all $g \in E$. Thus E/F has no primitive element.

Recall from 818 the following theorems:

Theorem 5 (Primitive Element Theorem 1 (PET 1)). Let E/F be a finite separable extension. Then there exists $\alpha \in E$ such that $E = F(\alpha)$.

Theorem 6. (Primitive Element Theorem 2 (PET 2)) Let E/F be a finite field extension. Then there exists $\alpha \in E$ such that $E = F(\alpha)$ if and only if there exist only finitely many intermediate fields of E/F.

2.3 Day 5 - September 2

We shall prove the following theorem (which was stated last class):

Theorem 7 (Primitive Element Theorem II). Let E/F be a finite extension. Then $E = F(\alpha)$ for some $\alpha \in E$ if and only if there exists only finitely many intermediate fields of E/F (that is, if there exist only finitely many fields L such that $F \subset L \subset E$.

Proof. Let $S = \{$intermediate fields of E/F$\} = \{L \text{ field} | E \subset L \subset F\}$.

Suppose $E = F(\alpha)$. Let $f(x) = Min(\alpha, F)$, and let $\overline{E}$ be a fixed algebraic closure of E.

Let $T = \{$monic polynomial factors of $f(x)$ in $\overline{E}[x]\}$. Note that $f(x) = (x - \alpha_1)...(x - \alpha_n) \in \overline{E}[x]$, so the monic factors of $f(x)$ are of the form $(x - \alpha_{i_1})...(x - \alpha_{i_k})$ for some $i_1...i_k$ distinct elements of $\{1, ...n\}$. Thus T is finite.

Define $\lambda : S \to T$ by $L \mapsto Min(\alpha, L)$. (Since $Min(\alpha, L) | Min(\alpha, F)$, then $Min(\alpha, L) \in T$.)

We wish to show that λ is injective. Suppose $L_1, L_2 \in S$ and $Min(\alpha, L_1) = Min(\alpha, L_2) = x^n + c_{n-1}x^{n-1} + ...c_0 \in L_i[x]$ for $i = 1, 2$. It suffices to show that $L_1 = F(c_0, ..., c_{n-1})$ (since by the exact same argument it would follow that, $L_2 = F(c_0, ..., c_{n-1})$.

Let $K = F(c_0, ...c_{n-1})$. Since the $c_i \in L_1$, then certainly $K \subset L_1$. It then suffices to show that $[E : L_1] = [E : K]$ (since then $[L_1 : K] = 1$).

Let $g(x) = Min(\alpha, L_1)$. Note $g(x) \in K[x]$ and is irreducible in $L_1[x]$, so it is also irreducible in $K[x]$. Thus $g(x) = Min(\alpha, K)$. Note that $E = K(\alpha) = L_1(\alpha)$. Thus

$$\begin{aligned}
[E : K] &= \deg(Min(\alpha, K)) \\
&= deg(g(x)) \\
&= deg(Min(\alpha, L_1)) \\
&= [E : L_1]
\end{aligned}$$

Following this string of implications all the way back, we can conclude that λ is injective. Since λ injects S into T, and T is a finite set, then S is also finite, as desired.

Conversely, suppose there are only finitely many intermediate fields. We have two cases: either F is finite or infinite.

If F is finite, then E is also finite, so $E^\times$ is cyclic (since the unit group of any finite field is cyclic). Thus $E^\times =< \alpha >$ (in the sense of generating a group) for some α, so $E = F(\alpha)$.

If F is infinite, then since the extension is finite, we can write $E = F(\alpha_1, ...\alpha_n)$ for some $\alpha_1, ..., \alpha_n \in E$. We then induct on n.

If $n = 1$, then $E = F(\alpha_1)$, as desired.

If $n > 1$, we can really just show that $n = 2$ case. So suppose $E = F(\alpha, \beta)$. Then let $\Lambda = \{F(\alpha + c\beta) | c \in F\} \subset S$. Since S is finite, then Λ is finite, but $|F| = \infty$, so there exist $c_1 \neq c_2 \in F$ such that $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Let us call this field L. Then $(c_1 - c_2)\beta = (\alpha + c_1\beta) - (\alpha + c_2\beta) \in L$, so $\beta \in L$. Then $\alpha \in L$ as well, so $L = F(\alpha, \beta)$, and thus $F(\alpha, \beta)$ is generated by a single element.

□

3 Inseparable Extensions

Let us turn our attention to inseparability.

Theorem 8. Let F be a field of characteristic $p > 0$, and let $\alpha \in \overline{F}$. Then,

1. α is separable over F if and only if $F(\alpha) = F(\alpha^p)$

2. If α is inseparable over F then $[F(\alpha) : F(\alpha^p)] = p$ and $Min(\alpha, F(\alpha^p)) = x^p - \alpha^p$.

3. For all $n \geq 1$, $[F(\alpha^{p^{n-1}}) : F(\alpha^{p^n})]_S = 1$, so $[F(\alpha) : F]_S = [F(\alpha^{p^n}) : F]_S$

4. There exists $n \in \mathbb{N}$ such that α^{p^i} is separable over F for all $i \geq n$.

5. Let n be the least exponent such that α^{p^n} is separable over F. Then $[F(\alpha) : F] = p^n[F(\alpha) : F]_S$.

Proof. (1) Suppose α is separable over F. Then α is separable over $F(\alpha^p)$, but we know that $Min(\alpha, F(\alpha^p)) | x^p - \alpha^p = (x - \alpha)^p$. Since $Min(\alpha, F(\alpha^p))$ has distinct roots then it must be that $\deg(Min(\alpha, F(\alpha^p))) = 1$, so $\alpha \in F(\alpha^p)$. Thus $F(\alpha) = F(\alpha^p)$.

[Alternative proof of the forward direction: Since α is separable, then $[F(\alpha) : F(\alpha^p)] = [F(\alpha) : F(\alpha^p)]_S =$ # of distinct roots of $Min(\alpha, F(\alpha^p)) = 1$.]

Conversely, suppose $F(\alpha) = F(\alpha^p)$. Suppose for the sake of contradiction that α is not separable over F. Let $f(x) = Min(\alpha, F)$. Then $f(x) = g(x^p)$ for some $g(x) \in F[x]$. Thus $g(\alpha^p) = 0$. Then $[F(\alpha^p) : F] \leq deg(g(x)) < deg(g(x^p)) = [F(\alpha) : F]_S$. This is a contradiction, so $F(\alpha) = F(\alpha^p)$. □

(2) We know that $Min(\alpha, F(\alpha^p)) | x^p - \alpha^p$. By homework problem 5 [edit: see immediately below], either $x^p - \alpha^p$ is irreducible in $F(\alpha^p)[x]$ or it splits completely. If it splits, then $\alpha \in F(\alpha^p)$, which implies that α is separable by part (1) of the theorem. But this is a contradiction, since we assumed α is inseparable. Thus $x^p - \alpha^p$ is irreducible, so it is the minimal polynomial of α as desired. □

(3) We know that $[F(\alpha):F(\alpha^p)]_S = \#$ of distinct roots of $Min(\alpha, F(\alpha^p)) = 1$. From part (2), $Min(\alpha, F(\alpha^p)) = (x-\alpha)^p$, so it only has one distinct root. By applying this argument to $\alpha^{p^{n-1}}$, we get that $[F(\alpha^{p^{n-1}}) : F(\alpha^{p^n})]_S = 1$ for all n. Thus $[F(\alpha) : F(\alpha^{p^n})]_S = [F(\alpha) : F(\alpha^p)]_S ... [F(\alpha^{p^{n-1}}) : F(\alpha^{p^n})]_S = 1$, so $[F(\alpha):F]_S = [F(\alpha):F(\alpha^{p^n})]_S[F(\alpha^{p^n}):F]_S = [F(\alpha^{p^n}):F]_S$ for all n. □

(4) Consider the descending chain of F-vector spaces $F(\alpha) \supset F(\alpha^p) \supset F(\alpha^{p^2}) \supset ....$ Since $\dim_F(F_\alpha) = [F(\alpha):F] < \infty$, then this chain stabilizes. Thus there exists an $n \in \mathbb{N}$ such that $F(\alpha^{p^n}) = F(\alpha^{p^{n+1}})$. But $(\alpha^{p^n})^p = \alpha^{p^{n+1}}$, so by part (1), α^{p^n} is separable over F. Thus $F(\alpha^{p^n})$ is separable over F but since $\alpha^{p^i} \in F(\alpha^{p^n})$ whenever $i \geq n$, then α^{p^i} is separable for all $i \geq n$. □

(5) We have the following tower of fields: $F(\alpha) \supset F(\alpha^p) \supset F(\alpha^{p^2}) ... \supset F(\alpha^{p^n})$. For each of these, the degree of the extension is p by part (2), and the separable degree is 1 by part (3). By assumption, α^{p^n} is separable, so $F(\alpha^{p^n})$ is separable. Thus $[F(\alpha^{p^n}):F] = [F(\alpha^{p^n}):F]_S$.

But

$$\begin{aligned}
[F(\alpha):F] &= [F(\alpha):F(\alpha^p)][F(\alpha^p):F(\alpha^{p^2})]...[F(\alpha^{p^{n-1}}):F(\alpha^{p^n})][F(\alpha^{p^n}):F] \\
&= p^n[F(\alpha^{p^n}):F] \\
&= p^n[F(\alpha^{p^n}):F]_S \\
&= p^n 1^n [F(\alpha^{p^n}):F]_S \\
&= p^n[F(\alpha):F(\alpha^p)]_S[F(\alpha^p):F(\alpha^{p^2})]_S...[F(\alpha^{p^{n-1}}):F(\alpha^{p^n})]_S[F(\alpha^{p^n}):F]_S \\
&= p^n[F(\alpha):F]_S
\end{aligned}$$

□

Homework Problem 2. *Let E/F be an extension, and suppose $charF = p > 0$. Let $\alpha \in E$. Then either $x^p - \alpha$ is either irreducible over F, or it factorizes completely.*

Corollary 3. Let E/F be a finite extension, and let $CharF = p$. Then $[E:F] = p^n[E:F]_S$ for some $n \geq 0$.

Proof. Let $E = F(\alpha_1, ..., \alpha_k)$ for some $\alpha_1, ..., \alpha_k \in E$. We induct on k.

If $k = 1$, we have this from part (5) of the previous theorem.

If $k > 1$, then let $L = F(\alpha_1, ..., \alpha_{k-1})$. By the inductive hypothesis, $[L:F] = p^\ell[L:F]_S$ for some $\ell \in \mathbb{N}$. Also, $E = L(\alpha_k)$. By the $k = 1$ case, $[E:L] = p^t[E:L]_S$ for some $t \in \mathbb{N}$. Then we multiply, and get that $[E:F] = [E:L][L:F] = p^{\ell+t}[E:L]_S[L:F]_S = p^{\ell+t}[E:F]_S$. □

Definition 9. If E/F is a finite extension, with $[E:F] = p^k[E:F]_S$, then the *inseparable degree* of E/K is p^k.

Theorem 9. (Really easy) The inseparable degree is multiplicative.

3.1 Day 6 - September 4

Andrew sez:im helping!

On homework 1 problem 4, we can assume the degrees are finite.

Definition 10. Let F be a field of characteristic $p > 0$, and let $\alpha \in \overline{F}$. Then α is *purely inseparable* (often written p.i.) if $\alpha^{p^n} \in F$ for some $n \geq 0$.

This is equivalent to $Min(\alpha, F) | x^{p^n} - \beta$ in $F[x]$.

We say E/F is *purely inseparable* if each $\alpha \in E$ is p.i. over F.

Lemma 3. Let $\alpha \in \overline{F}$. Then the following are equivalent

1. α is p.i. over F.
2. $[F(\alpha):F]_S = 1$
3. $[F(\alpha):F]_i = [F(\alpha):F]$

Proof. We note that 2 and 3 are equivalent by the definitions of separable and inseparable degrees.

For 1 and 2, note that α is p.i. over F if and only if $\alpha^{p^n} \in F$ for some $n \geq 0$. But this is the case if and only if $[F(\alpha^{p^n}) : F] = 1$ for some $n \geq 0$. But this is the case if and only if $[F(\alpha^{p^n}) : F]_S = 1$ for some $n \geq 0$ (since for some n sufficiently large, α^{p^n} is separable by a theorem from last class). But this is the case if and only if $[F(\alpha) : F]_S = 1$ since $[F(\alpha) : F]_S = [F(\alpha^{p^n}) : F]_S$. □

Theorem 10. Let E/F be a finite extension. Let $E = F(\alpha_1, ...\alpha_n)$ for some $\alpha_i \in E$. Then the following are equivalent.

1. E/F is p.i.
2. Each α_i is p.i. over F
3. $[E : F]_S = 1$
4. $[E : F] = [E : F]_i$

Proof. Note that (3) and (4) are equivalent by the definition of separable and inseparable degree.

Note that (1) implies (2) by definition.

Suppose (2) holds. We induct on i to prove that $[F(\alpha_1, ...\alpha_i) : F]_S = 1$. The $i = 1$ case is the lemma.

If $i > 1$, let $L = F(\alpha_1, ...\alpha_{i-1})$. By the inductive hypothesis, $[L : F]_S = 1$. As α_i is p.i. over F, then $[L(\alpha_i) : L]_S = 1$, so $(L(\alpha_i) : F]_S = 1$, but $L(\alpha_i) = F(\alpha_1, ..., \alpha_i)$. Thus (2) implies (3).

Suppose 3 is true. Then let $\beta \in E$. Then $[F(\beta) : F]_S \leq [E : F]_S = 1$, so by the lemma β is p.i. over F. Thus (3) implies (1), and all are equivalent. □

Definition 11. Let E/F be an algebraic extension, and let $char F = p$. Let $L = \{\alpha \in E | \alpha \text{ is p.i. over } F\}$. Then L is a field (proof omitted, but straightforward). Certainly, L is intermediate between E and F. We call L the *inseparable closure* of F inside E.

4 Normal Extensions

Question 1. If E/F is an algebraic extension, is E generated by the separable closure of F and the inseparable closure of F?

Answer: yes, if E/F is normal.

Lemma 4. Let E/F be an algebraic extension. And let $\sigma : E \to E$ be a field map fixing F. Then σ is an automorphism of E.

Proof. Let $\beta \in E$. Let $f(x) = Min(\beta, F)$, and let $S = \{\text{all roots of } f(x) \text{ in } E\}$. Observe that S is a nonempty finite set. As $f(x)$ has coefficients in F, and σ fixes F, then $\sigma(\beta)$ is a root of $f(x)$. Thus σ maps elements of S to elements of S. But S is finite, and σ is injective (as it is a field map), so in fact σ permutes S. Thus in particular there exists a $\gamma \in S$ such that $\sigma(\gamma) = \beta$. Thus σ is onto, so it is a bijection. □

Proposition 7. Let E/F be an algebraic extension. The following are equivalent.

1. E is a splitting field for some (possibly infinite, but definitely nonempty) set of polynomials in $F[x]$.
2. Any embedding $\sigma : E \to \overline{E}$ which fixes F is an automorphism of E.
3. Any irreducible polynomial in $F[x]$ which has a root in E splits completely in $E[x]$.

Proof. Suppose (1), and let S denote the set of polynomials for which E is the splitting field. Then let $T = \{\alpha \in E : \alpha \text{ is a root of some } f(x) \in S\}$. Certainly, $E = F(T)$.

Let $\sigma : E \to \overline{E}$ and suppose σ fixes F.

By the same argument as in the previous lemma, σ is a permutation of T, so namely $\sigma(T) = T \subset E$. Thus $\sigma(T) \subset E$. But σ fixes F and sends elements of T to elements of T, and E is generated by F and T, so $\sigma\Big|_E$ maps into E. But by the previous lemma, $\sigma(E) = E$, and thus σ is an automorphism.

Thus (1) implies (2).

Suppose (2). Let $f(x) \in F[x]$ be irreducible and let $\alpha \in E$ be a root of $f(x)$. Let $\beta \in \overline{E}$ be a root of $f(x)$. Then there exists an isomorphism between $F(\alpha)$ and $F(\beta)$ which fixes F (since both are isomorphic to $F[x]/(f(x))$) and for which α is mapped to β. Let this automorphism be called τ.

Then τ extends to an embedding σ of E into $\overline{E}$, but by (2), then σ is in fact a field automorphism. Thus $\tau(\alpha) = \beta \in E$, so every root of $f(x)$ is in E, so $f(x)$ factors completely. Thus (2) implies (3).

Suppose (3). Let $S = \{Min(\alpha, F) : \alpha \in E\}$. By (3), all polynomials in S split completely in E, so E is the splitting field for S over F. Thus (3) implies (1), and all three criteria are equivalent.

□

Definition 12. If E/F satisfies any of the equivalent conditions in Proposition 7, then E/F is called a *normal extension*.

Example 6. If $[E : F] = 2$, then E/F is normal.

Remark 6. Let E/F and F/K be field extensions. If E/K is normal, then E/F is normal. This follows directly from the criterion 1 in Proposition 7.

However, F/K may not be normal. For instance, let $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt[3]{2})$, let ω be a primitive third root of unity, and let $E = \mathbb{Q}(\omega, \sqrt[3]{2})$. Then E is the splitting field of $x^3 - 2$, but F/K is not normal since $x^3 - 2$ has a root but does not factor completely.

Remark 7. If E/F and F/K are normal extensions, then it does NOT follow that E/K is normal.

For instance, if $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2})$, and $E = \mathbb{Q}(\sqrt[4]{2})$, then E/F is degree 2, hence normal, and similarly F/K is also degree 2, hence normal.

However, $x^4 - 2$ has a root in E but does not factor completely.

4.1 Day 7 - September 9

Recall from last class that if $K \subset L \subset E$ are field extensions and E/K is normal, then E/L is normal. If E is the splitting field for a set $S \subset K[x]$, then E is also the splitting field for S as a subset of $L[x]$.

Exercise 3. Let $\{E_\alpha\}_{\alpha\in\Lambda}$ be a set of subfields of a field L, and suppose each E_α is normal over a fixed field F. Then $\bigcap_{\alpha\in\Lambda} E_\alpha$ is normal over F.

Definition 13. Let E/F be an algebraic field extension. Then *normal closure* of E/F is $\displaystyle\bigcap_{\substack{E\subset K\subset\overline{E}\\ K/F \text{ normal}}} K$. By the previous exercise, this is normal, and by construction it is the smallest normal extension of F containing E.

Example 7. Let $E = F(\alpha_1, ..., \alpha_n)$. Let $f_i(x) = Min(\alpha_i, F)$, and let $f(x) = f_1(x)...f_n(x)$.

Then the normal closure of E/F is the splitting field for $f(x)$ over F.

Proposition 8. Let E/F be a normal algebraic extension. Suppose E/F is inseparable. Then there exists $\alpha \in E \setminus F$ such that α is purely inseparable over F.

(Remark: This is false if E/F is not assumed to be normal.)

Proof. Let $\alpha \in E$, such that α is inseparable over F. Let $f(x) = Min(\alpha, F)$. Since α is inseparable over F, then its minimal polynomial is of the form $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

In $\overline{E}[x]$, we can factorize $g(x) = (x - \alpha_1)...(x - \alpha_n)$.

So $f(x) = g(x^p) = (x^p - \alpha_1)...(x^p - \alpha_n)$. For each i, let $\beta_i \in \overline{E}$ be a root of $x^p - \alpha_i$. Then $\beta_i^p = \alpha_i$ for all i, so $f(x) = (x^p - \beta_1^p)...(x^p - \beta_n^p) = ((x - \beta_1)...(x - \beta_2))^p$.

But each β_i is a root of $f(x)$, and $f(x) \in F[x]$ is irreducible and has a root $\alpha \in E$. But E/F is normal, so $f(x)$ factors completely in $E[x]$. Thus each $\beta_i \in E$.

Let $\ell(x) = (x - \beta_1)...(x - \beta_n) \in E[x]$. Also, $\ell(x)^p = f(x) \in F[x]$ (and $\ell(x) \notin F[x]$ since $f(x)$ is irreducible). Therefore, there exists a coefficient in $\ell(x)$ which is not in F. Let us call that coefficient c. But the corresponding coefficient in $\ell(x)^p$ is c^p, which is in F. Thus $c \in E \setminus F$, and c is purely inseparable (by the definition). $\square$

Definition 14. If E/F is a field extension, then we say $F^{insep} = \{\alpha \in E | \alpha \text{ is purely inseparable over } F\}$. We call F^{insep} the *inseparable closure* of F (over E).

Time for Galois Theory!

Definition 15. Let E/F be a field extension. Let $Aut(E/F) = \{\phi : E \to E | \phi \text{ fixes } F\}$ ($\subset \{\phi : E \to \overline{E} | \phi \text{ fixes } F\}$. We call $Aut(E/F)$ the *automorphism group* of E/F (and yeah, it is a group).

Remark 8. Let E/F be a finite extension. Then

1. $|Aut(E/F)| \leq [E : F]_S$ with equality if and only if E/F is normal.
2. $|Aut(E/F)| \leq [E : F]$ (this follows immediately from the first part), with equality if and only E/F is normal and separable.

Definition 16. Let E/F be an algebraic extension. If E/F is normal and separable, then we say that E/F is a *Galois extension*. In this case, $Aut(E/F)$ is called the *Galois group*, and we denote it $Gal(E/F)$.

(By the previous remark, note that if E/F is finite, then E/F is Galois if and only if $|Gal(E/F)| = [E : F]$.)

Example 8. Let E be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. The roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, where ω is a primitive third root of unity.

So $E = \mathbb{Q}(\omega, \sqrt[3]{2})$. We can draw a chart of the intermediate fields as $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset E$ and $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset E$ (wow, it would really help if I could draw diagrams in LaTeX... I should probably learn). Note that $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, so $3|[E : \mathbb{Q}]$ and $2|[E : \mathbb{Q}]$. Thus $[E : \mathbb{Q}] \geq 6$. But at the same time it is at most 6 (since it can at most permute the roots, and there are only $3! = 6$ permutations of 3 roots), so $[E : \mathbb{Q}] = 6$.

Then $Gal(E/F) = \{\text{permutations of the roots of } x^3 - 2\}$. Alternatively, if $\sigma : E \to E$ by $\omega \mapsto \omega^2$ and $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, and $\tau : E \to E$ by $\omega \mapsto \omega$ and $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$. Then we can present the group as $< \sigma, \tau | \sigma^2 = 1, \tau^3 = 1, \tau\sigma = \sigma\tau^2 >$.

Remark 9. If you are working over a field of characteristic 0, separability is free. Therefore, Galois-ness is equivalent to normality.

Example 9. Let E be the splitting field for $x^n - 1$ over $\mathbb{Q}$. Then $E = \mathbb{Q}(\omega)$, where $\omega = e^{\frac{2\pi i}{n}}$ (a primitive n-th root of unity).

Furthermore, $Min(\omega, \mathbb{Q}) = \Phi_n(x)$ which has degree $\phi(n)$, so $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$.

Define $\psi_i : E \to E$ by $\omega \mapsto \omega_i$. Then $Gal(E/\mathbb{Q}) = \{\psi_i | \gcd(i, n) = 1\}$ (and one should check that $\psi_i = \psi_j$ if and only if $i \equiv j \mod n$). Then $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_n^\times$, so $|Gal(E/\mathbb{Q})| = |\mathbb{Z}_n^\times| = \phi_n$. Thus the extension is Galois.

(But actually, we already knew this: the extension is separable because it is over fields of characteristic 0, and it is normal since it is a splitting field. Thus it is Galois.)

5 Fundamental Theorem of Galois Theory

5.1 Day 8 - September 11

Special thanks to Matt Mills for letting me use his laptop today!

Example 10. Let E be the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Then $E = \mathbb{Q}(\omega, \sqrt[5]{2})$, where ω is a primitive 5-th root of unity.

Then what is the degree of the extension? Well $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$, so the degree of $\mathbb{Q}(\omega, \sqrt[5]{2}/\mathbb{Q}) = 20$.

What is the Galois group? Let $L_1 = \mathbb{Q}(\omega)$, $L_2 = \mathbb{Q}(\sqrt[5]{2})$, and $E = \mathbb{Q}(\omega, \sqrt[5]{2})$. Then we define $\tau : E \to E$ by $\sqrt[5]{2} \mapsto \sqrt[5]{2}\omega$ (and fixing L_1). Observe that τ has order 5. We also define $\sigma : E \to E$ by $\omega \mapsto \omega^2$ (and fixing L_2). Observe that σ has order 4.

Thus σ and τ generate $Gal(E/\mathbb{Q}) = G$. What is the relation between τ and σ? By Sylow's theorem, $< \tau >$ is normal in G. Thus $\sigma\tau\sigma^{-1} = \tau^i$ for some i between 1 and 4. In particular, $\sigma(\tau(\sqrt[5]{2})) = \sigma(\omega\sqrt[5]{2}) = \omega^2\sqrt[5]{2}$. Also, $\tau^i(\sigma(\sqrt[5]{2})) = \tau^i(\sqrt[5]{2}) = \omega^i\sqrt[5]{2}$. Thus $i = 2$, and we can present G by $G =< \sigma, \tau | \sigma^4 = 1, \tau^5 = 1, \sigma\tau = \tau^2\sigma >$.

Theorem 11 (Fundamental Theorem of Galois Theory). Let E/F be a finite Galois extension, and let $G = Gal(E/F)$. Then we have maps from {intermediate fields of E/F} to {subgroups of G} and vice-versa, given by

- If $H \leq G$, let $E_H = \{\alpha \in E | \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$. We call E_H the *fixed field* of H, and it is indeed an intermediate field between E/F. We say $\phi(H) = E_H$.
- Let L be an intermediate field of E/F. Then E/L is Galois, and $Gal(E/L) \leq G$. We say $\psi(L) = Gal(E/L)$.

Then ϕ and ψ are inverses. That is $L = E_{Gal(E/L)}$, and $H = Gal(E/E_H)$.

Proof. We first show that $L = E_{Gal(E/L)}$. Recall that $E_{Gal(E/L)}$ denotes the set of elements that are fixed by every automorphism which fixes L. Then certainly $L \subset E_{Gal(E/L)}$.

Instead suppose $\alpha \in E_{Gal(E/L)}$. Let $\sigma : L(\alpha) \to \overline{L} = \overline{E}$ be any embedding which fixes L. The number of such σs is $[L(\alpha) : L]_S$, but since E/L is Galois, it is separable, so this equals $[L(\alpha) : L]$.

Let $\tau : E \to \overline{E}$ be any extension of σ. As τ fixes L, and E/L is normal, we have that $\tau : E \to E$, so $\tau \in Aut(E/L) = Gal(E/L)$. Since $\alpha \in E_{Gal(E/L)}$, $\tau(\alpha) = \alpha$. But recall that $\tau\Big|_L = \sigma$, so $\sigma(\alpha) = \alpha$, and since α was arbitrary, then $\sigma = id$. Hence, $1 = [L(\alpha) : L]_S = [L(\alpha) : L]$, so $\alpha \in L$. Thus $L = E_{Gal(E/L)}$.

[Proof that $H = Gal(E/E_H)$ comes later.] □

Lemma 5. Let E/F be a separable algebraic extenion such that there exists n satisfying $[F(\alpha) : F] \leq n$ for all $\alpha \in E$. Then $[E : F] \leq n$.

Proof. Choose $\alpha \in E$ such that $[F(\alpha) : F]$ is as large as possible (we can find such an α because these degrees are bounded above by n).

Suppose for the sake of contradiction that $F(\alpha) \neq E$. Then there exists some $\beta \in E \setminus F(\alpha)$. Then $[F(\alpha, \beta) : F] > [F(\alpha) : F]$. But by the first primitive element theorem (which we did not prove in class), there exists $\gamma \in F(\alpha, \beta)$ such that $F(\alpha, \beta) = F(\gamma)$, so this is a contradiction of the assumption that σ was maximal. Thus $E = F(\alpha)$, and $[E : F] = [F(\alpha) : F] \leq n$. □

Theorem 12 (Artin's Theorem). Let E be a field, and let G be a finite subgroup of $Aut(E)$. Let $E_G = \{\alpha \in E | \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$. Then E/E_G is Galois and finite, and $G = Gal(E/E_G)$.

Note that Artin's Theorem makes it very easy to prove the second part of the Fundamental Theorem of Galois Theory:

Proof. If H is a finite subgroup of $Aut(E) = Gal(E/F)$, then by Artin's Theorem, $H = Gal(E/E_H)$. □

5.2 Day 9 - September 14

We shall begin by proving Artin's Theorem, which will finish our proof of The Fundamental Theorem of Galois Theory.

Theorem 13. Let E be a field, and let G be a finite subgroup of $Aut(E)$. Let $E_G = \{\alpha \in E | \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$. Then E/E_G is Galois, and $Gal(E/E_G) = G$.

Proof. Let $\alpha \in E$. Let $\phi_1(\alpha), ...\phi_r(\alpha)$ be the distinct maps of α under G (where each $\phi_i \in G$).

Let $G = |n|$. Then $r \leq n$.

If $\tau \in G$, as τ is one-to-one, then $\tau\phi_1(\alpha), ..., \tau\phi_r(\alpha)$ are distinct, so τ is merely permutes the set $\{\phi_1(\alpha), ...\phi_r(\alpha)\}$. Let $f(x) = \prod_{i=1}^{r}(x - \phi_i(\alpha))$. Then for all $\tau \in G$, $f^\tau(x) = f(x)$ (where $f^\tau(x)$ denotes the polynomial given by applying τ to the coefficients of $f(x)$). Thus $f(x) \in E_G[x]$.

Also note that $f(\alpha) = 0$.

So, $Min(\alpha, E_G) | f(x)$. Since $f(x)$ has distinct roots, then so does $Min(\alpha, E_G)$. Thus α is separable over E_G for all $\alpha \in E$. Thus E/E_G is separable.

Note that $[E_G(\alpha) : E_G] \leq deg f(x) = r \leq n$ for all $\alpha \in E$. Thus $[E : E_G] \leq n$ by the lemma from last class.

Note that for all $\alpha \in E$, $Min(\alpha, E_G)$ splits in $E[x]$ (since $f(x)$ does). But if $f(x) \in E[x]$ has a root α, then $f(x) = kMin(\alpha, E_G)$, so $f(x)$ splits completely. Thus the extension is normal. Thus E/E_G is Galois.

Certainly, $G \leq Gal(E/E_G)$. Then $|Gal(E/E_G)| \geq |G| = n$. But $|Gal(E/E_G)| = [E : E_G]$ since this is a Galois extension, but $[E : E_G] \leq n$, so $G = Gal(E/E_G)$. $\square$

Remark 10. Let E/F be a finite Galois Extension, and let $G = Gal(E/F)$. Then,

1. If L is an intermediate field, then $|Gal(E/L)| = [E : L]$ (since E/L is Galois).
2. If $H \leq G$, then $|G| = [E : E_H]$. This follows from part 2 of the FTGT since $H = Gal(E/E_H)$.
3. If L_1 and L_2 are intermediate fields, then $L_1 \supset L_2 \iff Gal(E/L_1) \subset Gal(E/L_2)$, and if H_1 and H_2 are subgroups of G, then $H_1 \leq H_2 \iff E_{H_1} \supset E_{H_2}$. The forward directions are easy, and the backwards directions follow from the forward directions plus the Fundamental Theorem.

Example 11. Let $E = \mathbb{Q}(\omega, \sqrt[3]{2})$, the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Let's find generators of all the intermediate fields of $E/\mathbb{Q}$.

Let $G = Gal(E/\mathbb{Q}) =< \sigma, \tau >$ where σ fixes ω and sends $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$, and τ fixes $\sqrt[3]{2}$ and sends $\omega \mapsto \omega^2$.

Since this group is isomorphic to S_3, then every proper subgroup is of order 2 or 3, and is hence cyclic. In fact, the subgroups are $< \sigma >, < \tau >, < \sigma\tau >, < \sigma^2\tau >$. Then the subfield lattice is the subgroup lattice but order-reversed.

Since all of our extensions in this case are prime, then we can merely check that we adjoin a single things fixed by our generator and which is not rational.

Then the subfields are $E_{<\sigma>} = \mathbb{Q}(\omega)$, $E_{<\tau>} = \mathbb{Q}(\sqrt[3]{2})$, $E_{<\sigma\tau>} = \mathbb{Q}(\omega^2 \sqrt[2]{3})$, and $E_{<\sigma^2\tau>} = \mathbb{Q}(\omega\sqrt[3]{2})$.

Proposition 9. Let E/F be a finite Galois extension. Then E/F is separable, so by the first Primitive Element Theorem, $E = F(\alpha)$ for some $\alpha \in E$. Let $H \leq Gal(E/F) = G$. Then

1. $Min(\alpha, E_H) = \prod_{h \in H}(x - h(\alpha))$.
2. If $Min(\alpha, E_H) = x^m + c_{m-1}x^{m-1} + ...c_0$, then $E_H = F(c_{m-1}, ..., c_0)$.

Proof. Let E/F be a finite Galois extension, and suppose $E = F(\alpha)$, and let $H \leq Gal(E/F)$. Furthermore, let $f(x) = \prod_{h \in H}(x - h(\alpha))$.

For all $\tau \in H$, we have that $f^\tau(x) = f(x)$ since $\tau H = H$ (where $f^\tau(x)$ denotes τ applied to all the coefficients of f). Thus $f(x) \in E_H[x]$.

Note that $deg f(x) = |H| = [E : E_H] = [E_H(\alpha) : E_H]$. Since $f(\alpha) = 0$, then $Min(\alpha, E_H)|f(x)$. But since $f(x)$ and $Min(\alpha, E_H)$ have the same degree (and are monic), then $f(x) = Min(\alpha, E_H)$, as desired.

Let $L = F(c_0, ..., c_{m-1})$, and note that $E = L(\alpha)$. Since $f^\tau(x) = f(x)$, then each c_i is fixed by each element in H, so $L \subset E_H$. But $f(x) \in L[x]$, so $f(x)$ is irreducible in $L[x]$ (since it is irreducible in $E_H[x]$). Thus $f(x) = Min(\alpha, L)$, so $[E : L] = [L(\alpha) : L] = deg f(x) = [E : E_H]$, so $L = E_H$. $\square$

Example 12. Let ω be a primative 19th root of unity. Let $E = \mathbb{Q}(\omega)$, a splitting field for $x^{19} - 1$ over $\mathbb{Q}[x]$. Then $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_{19}^\times \cong C_{18}$ (where C_{18} is the cyclic group of 18 elements).

Note that $Gal(E/\mathbb{Q})$ is generated by $\phi_2 : \omega \mapsto \omega^2$. Thus the subgroups of G are generated by $\phi_{18} = \phi_2^9$, $\phi_7 = \phi_2^6$, $\phi_8 = \phi_2^3$, and $\phi_4 = \phi_2^2$.

Let E_i denote the subfield of E fixed by ϕ_i. Then the subfield orders are given by $\mathbb{Q} \subset E_8 \subset E_{18} \subset E$, $\mathbb{Q} \subset E_4 \subset E_7 \subset E$, and $E_8 \subset E_7$.

How do we write these nicely? Let's do E_7, for which $H_7 =< \omega_7 >$. Then the corresponding polynomial is $(x - \omega)(x - \omega^7)(x - \omega^{11}) = x^3 - (\omega + \omega^7 + \omega^{11})x^2 + (\omega^8 + \omega^{12} + \omega^{18})x - 1$. Thus $E_7 = \mathbb{Q}(\omega^8 + \omega^{12} + \omega^{18}, \omega + \omega^7 + \omega^{11})$.

5.3 Day 10 - September 16

Recall Artin's Theorem from last class:

Theorem 14. Let E be a field, and let G be a finite subgroup of $Aut(E)$. Let $E_G = \{\alpha \in E | \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$. Then E/E_G is Galois, and $Gal(E/E_G) = G$.

Here's an application of it:

Let K be a field and let $x_1, ..., x_n$ be indeterminants over K. Let $E = K(x_1, ..., x_n) = \{\frac{f(x_1,...,x_n)}{g(x_1,...,x_n)} | f, g \in K[x_1, ...x_n]\}$. Given $\sigma \in S_n$, define $\tilde{\sigma} : E \to E$ by sending x_i to $x_{\sigma(i)}$.

For example, if $\sigma = (13)(24)$, then $\tilde{\sigma}(\frac{3x_2x_3^3 - x_4^2}{x_1^2x_2 + x_3 + x_2^4}) = \frac{3x_4x_1^3 - x_2^2}{x_3^2x_4 + x_1 + x_4^4}$.

Observe that some polynomials are fixed by all $\tilde{\sigma}$. For instance, $x_1 + ... + x_n$ and $x_1x_2...x_n$ are fixed by all $\tilde{\sigma}$.

Let $L = E_{S_n}$ (the fixed field under S_n). We call L the field of symmetric rational functions.

What are field generators for L/K?

By Artin's theorem, since S_n is a finite subgroup of the automorphism group of E, then E/L is Galois and $Gal(E/L) = S_n$. Also, $[E : L] = |S_n| = n!$.

Let t be another indeterminant over E. Consider $f(t) = \prod_{i=1}^{n}(t - x_i) \in E[t]$. Note that $f^\sigma(t) = f(t)$. Thus all coefficients of $f(t)$ are in L. That is, $f(t) \in L[t]$. Let s_i be the coefficients in L such that $f(t) = t^n - s_1t^{n-1} + s_2t^{n-2} + ... + (-1)^n s_n$. Then, for instance, $s_1 = x_1 + ... + x_n$ and $s_n = x_1x_2...x_n$.

Theorem 15. If K, L, E, and s_i are as before, then $L = K(s_1, ..., s_n)$.

Proof. We've already shown that $s_i \in L$ for all i, so $K(s_1, ..., s_n) \subset L$.

But observe that $f(t)$ splits in $E = K(s_1, ..., s_n)(x_1, ..., x_n)$, and in fact E is the smallest field that $f(t)$ splits in (since if it splits, each x_i must be in the splitting field). Thus E is actually the splitting field of $f(t)$ over $K(s_1, ..., s_n)$.

Since $deg f(t) = n$ then $[E : K(s_1, ..., s_n)] \leq n!$ (by elementary abstract algebra). However, $[E : L] = n!$ by Artin's theorem. Then

$$\begin{aligned} n! \cdot [L : K(s_1, ..., s_n)] &= [E : L][L : K(s_1, ..., s_n)] \\ &= [E : K(s_1, ..., s_n)] \\ &\leq n! \end{aligned}$$

Thus $[L : K(s_1, ..., s_n)] = 1$, and $L = K(s_1, ..., s_n)$ $\square$

Theorem 16 (Fundamental Theorem of Galois Theory, Part 3). Let E/F be a finite Galois extension, let $G = Gal(E/F)$ and let L be an intermediate field. Let $H = Gal(E/L)$. Then L/F is normal if and only if $H \lhd G$. Furthermore, if L/F is normal, $Gal(L/F) \cong G/H$.

Proof. Suppose L/F is normal. Define $\phi : G \to Gal(L/F)$ by $\sigma \mapsto \sigma\Big|_L$. It is easy to see ϕ is a group homomorphism.

What is the kernel of ϕ? Well, $\sigma \in \ker\phi$ if and only if $\sigma\Big|_L = 1_L$ if and only if σ fixes L, which is the case if and only if $\sigma \in H$. Thus $H = ker\phi$. But every kernel is normal in the group, so $H \lhd G$, as desired.

Furthermore, since every $\tau \in Gal(L/F)$ can be extended to some $\sigma \in Gal(E, F)$, then ϕ is onto.

Then we can apply an Isomorphism Theorem (of groups): that $G/ker(\phi) \cong im(\phi) = Gal(L/F)$. Since $ker(\phi) = H$, then $G/H \cong Gal(L/F)$, as desired.

Conversely, suppose $H \lhd G$. We wish to show that L/F is normal using the definition that every embedding of L into $\overline{L} = \overline{F}$ which fixes F in fact is an automorphism of L. To that end, let $\sigma : L \to \overline{F}$ be an embedding which fixes F. Let $\alpha \in L$, and let $h \in H$. We can extend σ to $\tau : E \to \overline{E}$. But since E/F is Galois, it is normal, so since τ fixes F, then in fact τ maps into E. Thus $\tau \in Aut(E/F) = Gal(E/F) = G$. Since $H \lhd G$, then there exists some $h' \in H$ such that $\tau^{-1}h\tau = h'$. Thus $\tau^{-1}h\tau(\alpha) = h'(\alpha)$. But $H = Gal(E/L)$, and $\alpha \in L$, so $h'(\alpha) = \alpha$. Thus by transitivity, $\tau^{-1}h\tau(\alpha) = \alpha$, so $h(\tau(\alpha)) = \tau(\alpha)$.

But h was arbitrary, so $\tau(\alpha)$ is fixed by every element of $H = Gal(E/L)$. Thus $\tau(\alpha) \in L$. Recall that $\sigma(\alpha) = \tau(\alpha)$, so $\sigma(\alpha) \in L$. But α was an arbitrary element of L, so σ maps every element of L to an element of L. That is, σ is an automorphism of L/F, as desired. $\square$

6 Norm and Trace

Definition 17. Let E/F be a finite extension. Let $\sigma_1, ..., \sigma_r$ be the distinct embeddings of $E \to \overline{F}$ fixing F. (So $r = [E : F]_S$ by the definition of separable degree.)

Define the *norm* of E/F as $N_F^E : E \to E$ by $\alpha \mapsto \left(\prod_{i=1}^{r} \sigma_i(\alpha)\right)^{[E:F]_{insep}}$.

Similarly, we define the *trace* of E/F as $\mathrm{Tr}_F^E : E \to E$ by $\alpha \mapsto [E : F]_{insep}\left(\sum_{i=1}^{r} \sigma_i(\alpha)\right)$.

Example 13. Let $E = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ (and $F = \mathbb{Q}$, of course). Then there are only two σ_i: the identity, and $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Then $N(a + b\sqrt{2}) = a^2 - 2b^2$ and $\mathrm{Tr}(a + b\sqrt{2}) = 2a$.

Example 14. Let $E = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\}$ (and $F = \mathbb{Q}$, of course). Then there are now three σ_i: the identity; σ, which is generated by $\sigma : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ (where ω is a primitive 3rd root of unity); and σ^2. Then $N(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a+b\sqrt[3]{2}+c\sqrt[3]{4}+\sigma(a+b\sqrt[3]{2}+c\sqrt[3]{4})+\sigma^2(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a^3+2b^3+4c^3-6abc \in \mathbb{Q}$. Also, $\mathrm{Tr}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 3a$ (since $1 + \omega + \omega^2 = 0$, and a few steps of algebra).

Example 15. (An inseparable example) Let $E = \mathbb{F}_p(t)$, and $F = \mathbb{F}_p(t^p)$ (where t is some indeterminant). Then we have seen that E/F is purely inseparable, with $[E : F]_{insep} = p$, and $[E : F]_S = 1$. Since the separable degree is only 1, there is only the identity map, so for all $\beta \in E$, $N(\beta) = \beta^p \in F$. Also, $\mathrm{Tr}(\beta) = p \cdot \beta = 0$.

Remark 11. The trace always "degenerates" whenever E/F fails to be separable. That is, if $[E : F]_{insep} > 1$, then $\mathrm{Tr}(\beta) = 0$ for all $\beta \in E$.

6.1 Day 11 - September 18

Recall from last class the norm and trace: if E/F is a finite extension, and $\sigma_1, ...\sigma_r$ are the distinct embeddings of F into E, then we say $N_F^E(\alpha) = \left(\prod_{i=1}^{r} \sigma_i(\alpha)\right)^{[E:F]_{insep}}$, and $\mathrm{Tr}_E^F(\alpha)$ is the additive version for all $\alpha \in E$.

Lemma 6. Let E/F be a finite separable extension. Then for all $\alpha \in E$, $N_F^E(\alpha) \in F$ and $\mathrm{Tr}_F^E(\alpha) \in F$.

Proof. Let $\sigma_1, ...\sigma_r : E \to \overline{F}$ be the distinct embeddings of E into $\overline{F}$ which fix F. Let L be the normal closure of E/F. In particular, by the primitive element theorem, E/F is generated by as single element, so $E = F(\alpha)$ for some $\alpha \in E$, and then L is the splitting field of $Min(\alpha, F)$ over F.

As proved on the homework [edit: see immediately below], L/F is separable, and since it is normal, then L/F is Galois (and also finite). Let $G = Gal(L/F)$. For each $\phi \in G$, $\phi\sigma_1, ...\phi\sigma_r$ are distinct embeddings from $E \to \overline{F}$ fixing $\overline{F}$. (We can do this because $Im(\sigma_i) \subset L$ for all i as L/F is normal.)

Thus each $\phi \in G$ permutes $\sigma_1, ...\sigma_r$.

Let $\alpha \in E$. Then

$$\begin{aligned}
\phi(N_F^E(\alpha)) &= \phi(\sigma_1(\alpha), ..., \sigma_r(\alpha)) \\
&= (\phi\sigma_1)(\alpha)...(\phi\sigma_r)(\alpha) \\
&= \sigma_1(\alpha)...\sigma_r(\alpha) \\
&= N_E^F(\alpha)
\end{aligned}$$

Thus N_E^F is fixed by all $\phi \in G$. Thus $N_F^E(\alpha) \in L_G = F$, as desired.

The proof for trace is identical. □

Homework Problem 3. *Let E/F be a separable algebraic field extension, and let L be the normal closure of E/F. Then L/F is separable.*

Remark 12. Recall that if $[F(\alpha) : F]_{insep} = p^n$, then α^{p^n} is separable over F.

Theorem 17. Let E/F be a finite extension. Then for all $\alpha \in E$, $N_F^E(\alpha) \in F$ and $\mathrm{Tr}_F^E(\alpha) \in F$.

Proof. We know that $[E : F]_{insep} = p^n$. By the lemma, it suffices to consider the case $n > 0$.

The claim for trace is boring: $\mathrm{Tr}_F^E(\alpha) = p^n(\text{blah}) = 0 \in F$ for all $\alpha \in E$.

It then suffices to check $N_F^E(\alpha) \in F$. Let L be the separable closure of F in E. By a homework problem [edit: see immediately below], E/L is purely inseparable. That is, $[E : L]_S = 1$. Let $r = [E : F]_S = [L : F]_S = [L : F]$.

Then there are r embeddings of L into $\overline{F}$ which fix F (by the definition of separable degree). Let us call them $\sigma_1, ..., \sigma_r$.

Extend each σ_i to $\tau_i : E \to \overline{F}$. But each embedding of $E \to \overline{F}$ which fixes F can be restricted back down to some σ_i, so $\tau_1, ...\tau_r$ are the distinct embeddings of $E \to \overline{F}$ which fix F.

Let $\alpha \in E$. Then $[L(\alpha) : L]_{insep} \leq [E : F]_{insep} = p^n$, so α^{p^n} is separable over L. Thus α^{p^n} is separable over F since L/F is also separable. Therefore $\alpha^{p^n} \in L$.

Then

$$\begin{aligned}
N_F^E(\alpha) &= \left(\prod_{i=1}^{r} \tau_i(\alpha)\right)^{[E:F]_{insep}} \\
&= \left(\prod_{i=1}^{r} \tau_i(\alpha)\right)^{p^n} \\
&= \prod_{i=1}^{r} \tau_i(\alpha^{p^n}) \\
&= \prod_{i=1}^{r} \sigma_i(\alpha^{p^n}) \\
&= N_F^L(\alpha^{p^n})
\end{aligned}$$

Since L/F is separable and $\alpha^{p^n} \in L$, then by the lemma, $N_F^L(\alpha^{p^n}) \in F$. Thus $N_F^E(\alpha) \in F$ as desired. $\square$

Homework Problem 4. *Let E/F be an algebraic field extension and let $K = F^{sep}$, the separable closure of F in E. Then E/K is purely inseparable.*

Proposition 10. Let E/F be a finite extension. Then

1. For all $\alpha, \beta \in E$, $N(\alpha\beta) = N(\alpha)N(\beta)$. In particular, $N_F^E : E^\times \to F^\times$ is a group homomorphism.
2. For all $\alpha, \beta \in E$, and $c \in F$, $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ and $\mathrm{Tr}(c\alpha) = cTr(\alpha)$. Thus $\mathrm{Tr}_F^E : E \to F$ is an F-linear transformation (a "linear functional").
3. For $\alpha \in F$, $N_F^E(\alpha) = \alpha^{[E:F]}$.
4. For $\alpha \in F$, $\mathrm{Tr}_F^E(\alpha) = [E : F]\alpha$.
5. If K is an intermediate field, then $N_F^E = N_F^K \circ F_K^E$ and $\mathrm{Tr}_F^E = \mathrm{Tr}_F^K \circ \mathrm{Tr}_K^E$.

Proof. Observe that (1) and (2) follow from the fact that the σ_is are automorphisms, so they respect addition and multiplication.

Observe that (3) and (4) follow from the fact that the number of σ_i is the separable degree, and that if $\alpha \in F$, then $\sigma_i(\alpha) = \alpha$ for all i.

We will now prove (5). Let $\phi_1, ..., \phi_s$ be the distinct embeddings $E \to \overline{F}$ fixing K. (So $s = [E : K]_S$).

Let $\sigma_1, ..., \sigma_t : K \to \overline{F}$ be the distinct embeddings fixing F.

Extend each σ_i to $\tau_i : E \to \overline{F}$.

We claim that the $\{\tau_i\phi_j\}$ are distinct embeddings of $E \to \overline{F}$ fixing F.

Suppose $\tau_i\phi_j = \tau_k\phi_l$. Then restrict these both to K. But the ϕs fix K, so they are the identity when restricted to K, and thus $\tau_i\Big|_K = \tau_k\Big|_K$. But $\tau_i\Big|_K = \sigma_i$ and $\tau_k\Big|_K = \sigma_k$. Thus $i = k$, and by applying τ_i^{-1}, we get that $\phi_j = \phi_l$ so $j = l$. Thus the $\tau_i\phi_j$ are distinct.

Note that $\#\{\tau_i\phi_j\} = st = [E : K]_S[K : F]_S = [E : F]_S$. But then we have found the right number of distinct embeddings of $E \to \overline{F}$ fixing F, so this is the correct list of all embeddings.

Then,

$$\begin{aligned}
N_F^K N_K^E(\alpha) &= N_F^K\left(\prod_j \phi_j(\alpha)^{[E:K]_{insep}}\right) \\
&= \left(\prod_i \tau_i \left(\prod_j \phi_j(\alpha)\right)^{[E:K]_{insep}}\right)^{[K:F]_{insep}} \\
&= \left(\prod_{i,j} \tau_i\phi_j(\alpha)\right)^{[E:F]_{insep}} \\
&= N_F^E(\alpha)
\end{aligned}$$

The proof of trace is similar but with sums instead of products. $\square$

Lemma 7. Let $\sigma_1, ...\sigma_r : E \to L$ be distinct nonzero field homomorphisms. Then $\{\sigma_1, ...\sigma_r\}$ is a linearly independent set over L, in the sense that if $c_1\sigma_1 + ... + c_r\sigma_r = 0$ as a linear transformation, where each $c_i \in L$, then $c_i = 0$ for all i.

Proof. We induct on r. If $r = 1$, then if $c_1\sigma_1 = 0$, then $c_1 = c_1\sigma(1) = 0$, so $c_1 = 0$.

In the inductive case, suppose $r > 1$, and assume for the sake of contradiction that $c_1\sigma_1 + ...c_r\sigma_r = 0$, where $c_i \neq 0$ for some i. By the inductive hypothesis, we can in fact assume that $c_i \neq 0$ for all i. Our inductive hypothesis also lets us assume that there is no shorter linear dependence among the σ_is.

As $\sigma_1 \neq \sigma_2$, there exists some $\beta \in E$ such that $\sigma_1(\beta) \neq 0$ and $\sigma_1(\beta) \neq \sigma_2(\beta)$.

Then for all $\alpha \in E$, we have that

$$\begin{aligned}\sum_{i=1}^{r} c_i\sigma_i(\alpha) &= 0 \\ &= \sum_{i=1}^{r} c_i\sigma_i(\alpha\beta) \\ &= \sum_{i=1}^{r} c_i\sigma_i(\alpha)\sigma_i(\beta)\end{aligned}$$

Thus we can divide by $\sigma_1(\beta)$ to get that $c_1\sigma(\alpha_1) + \sum_{i=2}^{r}\left(\frac{c_i\sigma_i(\beta)}{\sigma_1(\beta)}\right)\sigma_i(\alpha) = 0$ and subtracting from a previous equation, we get that a non-zero linear combination of $\sigma_2, ...\sigma_r$ is 0. Thus we have found a linear dependence among $r-1$ of the σs, which contradicts the inductive hypothesis. Thus $\sigma_1, ..., \sigma_r$ are linearly independent. $\square$

6.2 Day 12 - September 21

The first exam will be coming soon: probably either Wednesday October 7 or Wednesday October 14. But maybe we won't have class on Friday October 16.

Recall the following theorem from character theory:

Theorem 18 (Linearly Independent Characters). Let $\sigma_1, ...\sigma_r$ be distinct field embeddings from E into L. Then $\sigma_1, ...\sigma_r$ are linearly independent (as linear transformations) over L.

Corollary 4. If E/F is finite separable, then $\mathrm{Tr}_F^E \neq 0$. If E/F is inseparable, then $\mathrm{Tr}_F^E = 0$.

Proof. If E/F is separable and finite, $\mathrm{Tr}_F^E = \sigma_1 + ... + \sigma_r$. This is a non-zero linear combination, so it is non-zero.

If E/F is inseparable, then recall that the trace is multiplied by the inseparable degree. The inseparable degree is p^n for some $n > 1$, but p is the characteristic, so Tr_F^E is always zero. $\square$

Definition 18. Let E/F be a finite extension. The extension is called *cyclic (respectively abelian, solvable, nilpotent, etc.)* if E/F is Galois, and $Gal(E/F)$ is cyclic (respectively abelian, solvable, nilpotent, etc.).

Theorem 19 (Hilbert's Satz 90). Let E/F be a finite cyclic extension, let σ be a generator for $Gal(E/F)$, and let $\beta \in E$. Then $N(\beta) = 1$ if and only if $\beta = \frac{\alpha}{\sigma(\alpha)}$ for some $\alpha \in E$.

Proof. Suppose $\beta = \frac{\alpha}{\sigma(\alpha)}$. Let n be the order of σ. Then $N_F^E(\beta) = \prod_{i=1}^{n-1}\sigma^i(\beta) = \sigma^i(\frac{\alpha}{\sigma(\alpha)}) = \frac{\sigma(\alpha)...\sigma^n(\alpha)}{\sigma^2(\alpha)...\sigma^{n+1}(\alpha)} = 1$ since $\sigma^n = id$.

Suppose instead that $N(\beta) = 1$. Then by Theorem 18, $\{1, \sigma, ...\sigma^{n-1}\}$ is linearly independent.

Let $\phi : E \to E$ by $\phi(x) = \beta \cdot \sigma(x)$. Note that $\phi^n(x) = \left(\prod_{i=0}^{n-1}\sigma(\beta)\right)(\sigma^n(x)) = N(\beta)\sigma^n(x) = 1 \cdot x = x$ for all $x \in E$.

Let $g : E \to E$ be given by $g(x) = \sum_{i=0}^{n-1}\phi^i(x)$. By gathering up all of the σ terms in ϕ^i, we can see that g is a linear combination of σ^is. But one of its coefficients (namely the one on the 1 term) is nonzero, so since the σ^is are linearly independent, then $g \neq 0$. Let $u \in E$ such that $g(u) \neq 0$. Let $\alpha = g(u)$. Then

$$\begin{aligned}
\phi(\alpha) &= \phi(g(u)) \\
&= \phi(\sum_{i=0}^{n-1}\phi^i(u)) \\
&= \sum_{i=1}^{n}\phi^i(u) \\
&= \sum_{i=0}^{n-1}\phi(u) \\
&= g(u) \\
&= \alpha
\end{aligned}$$

Thus $\beta\sigma(\alpha) = \alpha$, so $\beta = \frac{\alpha}{\sigma(\alpha)}$ as desired.

□

Remark 13. Let F be a field and let $n \geq 1$ such that $Char\ F \nmid n$. Then $x^n - 1$ has n distinct roots on $\overline{F}$. The set of roots, called U_n is a subgroup of $\overline{F}^{\times}$. Furthermore, U_n is cyclic. Any cyclic generator of U_n is caled a *primitive n-th root of 1*.

Theorem 20. Let E/F be a finite extension. Assume F contains a primitive n-th root of 1. Also assume $Char\ F \nmid n$. Then E/F is cyclic of degree dividing n if and only if there exists some $\alpha \in E$ such that $E = F(\alpha)$ and $\alpha^n \in F$.

Proof. Suppose E/F is cyclic of degree dividing n. Let $[E:F] = d$ (so $n|d$). Let $\zeta \in F$ be a primitive n-th root of 1. Then $\omega = \zeta^{\frac{n}{d}}$ is a primitive d-th root of unity.

Note that $N_F^E(\omega^{-1}) = (\omega^{-1})^{[E:F]} = 1$. By Hilbert's Satz 90, there exists $\alpha \in E$ such that $\omega^{-1} = \frac{\alpha}{\sigma(\alpha)}$, where $Gal(E/F) =< \sigma >$.

Then $\sigma(\alpha) = \omega\alpha$, so $\sigma^i(\alpha) = \omega^i\alpha$ for $i = 0, ..., d-1$.

Since $Char\ F \nmid d$, we can say that $\alpha, \omega\alpha, ..., \omega^{d-1}\alpha$ are all distinct, so $[F(\alpha):F]_S \geq d$, since $\alpha \mapsto \omega^i\alpha$ are d distinct embeddings of $F(\alpha)$ into $\overline{E}$. But $d \leq [F(\alpha):F]_S \leq [F(\alpha):F] \leq [E:F] = d$, so all of these equal d. Thus $E = F(\alpha)$.

It then suffices to check that $\alpha^n \in F$. Since E/F is Galois, it suffices to check that α^n is fixed by all elements of $Gal(E/F)$. Note that $\sigma(\alpha^n) = (\sigma(\alpha))^n = \omega^n\alpha^n = \alpha^n$, so α^n is fixed by σ. But $Gal(E/F)$ is generated by σ, so α^n is fixed by all automorphisms, and thus $\alpha^n \in F$, as desired.

Conversely, suppose there exists an $\alpha \in E$ such that $E = F(\alpha)$, and $\beta = \alpha^n \in F$.

Then α is a root of $x^n - \beta \in F[x]$. By hypothesis, F contains a primitive n-th root of unity. Let ω be such a root of unity. Then $\omega^i\alpha$ (for $i = 0, ..., n-1$) are all of the roots of $x^n - \beta$. Thus $F(\alpha)$ is the splitting field of $x^n - \beta$.

So $F(\alpha)/F$ is normal. Also, $Min(\alpha, F)|x^n - \beta$, so $Min(\alpha, F)$ has distinct roots. Thus α is separable over F, so $F(\alpha)/F$ is separable. Since it is separable and normal, $F(\alpha)/F$ is Galois.

Let $G = Gal(E/F)$. If $\sigma \in G$, then $\sigma(\alpha) = \omega^{i_\sigma}(\alpha)$ for some $i_\sigma = 0, ..., n-1$. Define $\psi : G \to < \omega >$ by $\sigma \to \frac{\sigma(\alpha)}{\alpha}$.

We claim ψ is a group homomorphism. Let $\sigma, \pi \in G$. Say $\sigma(\alpha) = \omega^i\alpha$ and $\pi(\alpha) = \omega^j\alpha$. Then $\sigma\pi(\alpha) = (\omega^{i+j})\alpha$. Thus $\psi(\sigma)\psi(\pi) = i + j = \psi(\sigma\pi)$, so ψ is a homomorphism.

Furthermore, note that $\sigma \in \ker\psi$ if and only if $\psi(\alpha) = 1$ if and only if $\sigma(\alpha) = \alpha$, which is the case precisely when $\sigma = id$. Thus ψ is injective, so G is isomorphic to a subgroup of a cyclic group of order n. Thus G is cyclic of order $d|n$.

□

Remark 14. This is the key step to showing that not all equations are solvable by radicals.

6.3 Day 13 - September 23

The first Exam will be Monday, October 12, from 3-6. The actual exam will be only 2 hours, and we get to choose when we start.

Recall the following foreshadowing theorem from the last class:

Theorem 21. *Let E/F be a finite extension. Assume F contains a primitive n-th root of 1. Also assume $Char\ F \nmid n$. Then E/F is cyclic of degree dividing n if and only if there exists some $\alpha \in E$ such that $E = F(\alpha)$ and $\alpha^n \in F$.*

But now let's ignore it and look at something else:

7 Solvable Groups and Radical Extensions

Definition 19. Let G be a group. A *commutator* is an element of the form $xyx^{-1}y^{-1}$ for some $x, y \in G$. The *commutator subgroup* G' of G is the subgroup of G generated its commuators.

Definition 20. A subgroup $H \leq G$ is a *characteristic subgroup* if $\phi(H) = H$ for all $Y \in Aut(G)$. We use the notation $H\ Char\ G$.

Remark 15. We have the following results:

1. $H\ Char\ G \iff \phi(H) \subset H$ for all $\phi \in Aut(G)$.
2. $H\ Char\ G$ implies $H \lhd G$.
3. $G'\ Char\ G$

Let us prove the last part:

Proof. It suffices to show that if $\phi \in Aut(G)$, then $\phi(G') \subset G'$. It suffices to show that each commutator is sent into G'. But $\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1}$, so $G'\ Char\ G$. □

Remark 16. Since $G'\ Char\ G$, then $G' \lhd G$.

Proposition 11. *Let G be a group and let $H \leq G$. Then*

1. *G/G' is abelian.*
2. *If $H \lhd G$ and G/H is abelian, then $G' \leq H$.*
3. *If $G' \leq H$, then $H \lhd G$ and G/H is abelian.*

Proof. (Part 1) In G/G', for all $x, y \in G$, $\overline{xyx}^{-1}\overline{y}^{-1} = \overline{1}$, so $\overline{xy} = \overline{yx}$. □

(Part 2) Let $x, y \in G$. Then in G/H, $\overline{xy} = \overline{yx}$, so $\overline{xyx^{-1}y^{-1}} = \overline{1}$, so $xyx^{-1}y^{-1} \in H$, so $G' \subset H$. □

(Part 3) Note H/G' is a subgroup of G/G'. Then $H/G' \lhd G/G'$, as G/G' is abelian. Thus $H \lhd G$ because normality lifts.

□

Definition 21. Let $G^{(0)} = G$, and for all i, let $G^{(i+1)} = (G^{(i)})'$.

The *derived normal series* of G is $... \lhd G^{(2)} \lhd G^{(1)} \lhd G^{(0)} = G$.

A group G is called *solvable* if $G^{(n)} = 1$ for some $n \geq 0$.

Remark 17. If G is a group, then $G^{(1)} = 1$ if and only if G is abelian.

Example 16. Let's compute the derived normal series of S_3. Let $H =< (123) > \lhd S_3$. Then S_3/H is abelian, so $S_3^{(1)} \subset H$. Since $S_3^{(1)} \neq 1$, then $H = S_3^{(1)}$.

Then $S_3^{(2)} = H' = 1$ since H is abelian. So S_3 is solvable.

Lemma 8. Let $\phi : A \to B$ be a surjective group homomorphism. Then $\phi(A^{(i)}) = B^{(i)}$ for all $i \geq 0$.

Proof. We induct on i. If $i = 0$, then $A^{(i)} = A$ and $B^{(i)} = B$. But since ϕ is surjective, then $\phi(A) = B$, as desired.

If $i = 1$, then for all $x, y \in A$, $\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1}$, so $\phi(A^{(1)}) \leq B^{(1)}$. If $aba^{-1}b^{-1} \in B^{(1)}$, then there exist $x, y \in A$ such that $\phi(x) = a$ and $\phi(y) = b$, so then $\phi(xyx^{-1}y^{-1}) = aba^{-1}b^{-1}$. Thus $\phi(A^{(1)}) = B^{(1)}$

Suppose $i > 1$, and assume $\phi(A^{(i-1)}) = B^{(i-1)}$. Then $\phi\Big|_{A^{(i-1)}}$ is a surjective homomorphism, so we can apply the $i = 1$ case to this, proving the inductive case. □

Corollary 5. Suppose $H \lhd G$ and $\phi : G \to G/H$ is the natural map. Then $\phi(G^{(i)}) = (G/H)^{(i)}$. Also, $\phi(G^{(i)}) = \overline{G^{(i)}} = \frac{G^{(i)}H}{H}$.

Theorem 22. Let G be a group, and let $H \leq G$. Then

1. If G is solvable, so is H. If, in addition, $H \lhd G$, then G/H is solvable.
2. Conversely, if $H \lhd G$, and both H and G/H are solvable, then so is G.

Proof. If G is solvable, then $G^{(n)} = 1$ for some n. Since $H^{(i)} \subset G^{(i)}$ for all i, then $H^{(n)} = 1$, so H is solvable.

If $H \lhd G$, then by the corollary, $(G/H)^{(n)} = \overline{G^{(n)}} = \overline{1}$, so G/H is solvable. □

Conversely, suppose we have $\frac{G^{(n)}H}{H} = (G/H)^{(n)} = \overline{1}$ for some n. Hence $G^{(n)} \subset H$, so we have $H^{(m)} = 1$ for some m, and thus $G^{(m+n)} = 1$. Thus G is solvable. □

Proposition 12. Any p-group is solvable.

Proof. Let G be a p-group, and let $|G| = p^n$. We induct on n. We use the fact that any p-group has a non-trivial center: If $n = 1$, then G is cyclic, hence abelian, hence solvable. If $n > 1$, then consider the center $Z(G)$. This is certainly normal, and it is abelian, hence solvable. Furthermore, $G/Z(G)$ is smaller, so by the inductive hypothesis it is solvable. Thus by the previous theorem, G is solvable by the previous theorem. □

Exercise 4. Any group of order pq is solvable.

Why? If $p = q$, then we are done. If $p < q$, then the Sylow q-subgroup Q is normal and solvable. Thus $|G/Q| = p$, so G/Q is a Ap-group, hence solvable. Thus G is solvable.

Exercise 5. Any group of order pqr (where p, q, r are primes) is solvable. I should prove this by extensive application of Sylow's Theorem.

7.1 Day 14 - September 25

Definition 22. A *solvable series* for a group G is a normal series $\{1\} = G_t \lhd ... \lhd G_0 = G$ such that G_i/G_{i+1} is abelian for all i.

Proposition 13. If G is a group, then G is solvable if and only if G has a solvable series.

Proof. Suppose G is solvable. Then its derived series is a solvable series.

Suppose instead that G has a solvable series $\{1\} = G_t \lhd ... \lhd G_0 = G$. We claim that $G^{(i)} \leq G_i$ for all i. We prove this by induction on i. If $i = 0$, this is easy, since $G_0 = G$. Suppose $G^{(i-1)} \leq G_{i-1}$. Then $G^{(i)} = (G^{(i-1)})' \leq G'_{i-1} \leq G_i$ (the last containment is because G_{i-1}/G_i is abelian). Thus $G^{(t)} \leq G_t = \{1\}$, so G is solvable. □

This proof also implies that the derived series is the shortest possible normal series.

Corollary 6. If G is a group, then G is solvable if and only if G has a normal series where the factor groups are cyclic of prime order.

Proof. Suppose G has a normal series where the factor groups are cyclic of prime order. Then it has a normal series, so it is solvable by the previous proposition.

Suppose instead that G is solvable. We wish to consider the "longest possible" solvable series of G. First, note that any time a quotient in a solvable series is the identity, we can remove it. But then in each step, the group gets strictly smaller, so the lengths of solvable series are bounded by $|G|$. Thus there is a solvable series of maximal length. Let $\{1\} = G_t \lhd ... \lhd G_0 = G$ be such a series.

Then suppose for the sake of contradiction that some G_i/G_{i+1} is not cyclic of prime order. Since $|G_i/G_{i+1}|$ is a natural number greater than 1, it must be composite. But G_i/G_{i+1} is abelian, so there exists some intermediate group H such that $G_{i+1} \leq H \leq G_i$ and such that H/G_{i+1} is a subgroup of order p. Then $H/G_{i+1} \lhd G_i/G_{i+1}$ as G_i/G_{i+1} is abelian. Then $H \lhd G_i$, and $G_{i+1} \lhd H \lhd G_i$. Furthermore, this containments are proper, so we have that this can be inserted into the solvable series. This contradicts the maximality of the solvable series, so G_i/G_{i+1} is cyclic of prime order for all i. $\square$

We will use this exercise for the next theorem:

Exercise 6. Let A_n denote the alternating group on n elements. Then A_n is generated by the 3-cycles.

Theorem 23. Let A_n denote the alternating group on n elements. Then A_n is not simple (i.e. it contains no proper, nontrivial normal subgroups) for all $n \geq 5$.

Proof. Suppose $K \lhd A_n$, and suppose $K \neq \{1\}$.

We will show that K contains a 3-cycle. Choose $\sigma \in K \setminus \{1\}$ such that σ fixes a maximal number of elements of $\{1, 2, ..., n\}$. Assume for the sake of contradiction that σ is not a 3-cycle. Write σ as a product of disjoint cycles. Then there are two possible forms (much WLOGing is going on):

1. $\sigma = (123...)...$ (i.e. there exists a 3-cycle or longer)
2. $\sigma = (12)(34)...$ (i.e. there are no 3-cycles, i.e. σ is the product of disjoint transpositions)

If we are in case (1), then note that since σ is not a 3-cycle, then σ must move at least two more elements. Without loss of generality, let those elements be called 4 and 5. Also let $\beta = (354)$, and let $\pi = \beta\sigma\beta^{-1}$. Then in case (1), $\pi = (124...)$. In case (2), $\pi = (12)(35)....$ Note that $\pi \neq \sigma$.

Now let $\tau = \pi\sigma^{-1} = \beta\sigma\beta^{-1}\sigma^{-1}$. Since $\pi \neq \sigma$, then $\tau \in K \setminus \{1\}$.

We now wish to show that τ fixes more elements than σ, which will contradict our choice of σ. Note that if $i > 5$, and $\sigma(i) = i$, then $\tau(i) = i$.

Also note that in case (1), $\tau(2) = 2$, but σ moves 1,2,3,4, and 5. Thus τ fixes more elements than σ.

In case (2), $\tau(1) = 1$ and $\tau(2) = 2$, but σ moves 1,2,3, and 4, so τ fixes more elements than σ.

Thus in either case, we have a contradiction. Thus σ is a 3-cycle, so K contains at least one 3-cycle.

We will now show that σ contains every other 3-cycle. Without loss of generality, let the 3-cycle in K be (123). Let (ijk) be any other 3-cycle. We construct $\gamma \in S_n$ by $\gamma(1) = i$, $\gamma(2) = j$, $\gamma(3) = k$. Furthermore, we choose two other elements l, m such that $\gamma(4) = l$ and $\gamma(5) = m$, and we fill out the rest of γ any other way. If γ is even, then $\gamma \in A_n$, so $\gamma(123)\gamma^{-1} = (ijk) \in K$ since K is normal. If γ is odd, then let $\pi = (lm)\gamma$. Then $\pi \in A_n$, so $\pi(123)\pi^{-1} = (ijk) \in K$. Thus K contains every 3-cycle.

Then by the exercise, since A_n is generated by 3-cycles, $K = A_n$. Thus the only normal subgroups of A_n are $\{1\}$ and A_n.

$\square$

Corollary 7. If $n \geq 5$, then A_n is not solvable.

Proof. Since A_n is not abelian, $A_n' \neq \{1\}$. However, $A_n' \lhd A_n$, so since A_n is simple, $A_n' = A_n$. Thus $A_n^{(i)} = A_n \neq \{1\}$ for all i, so it not solvable. $\square$

Remark 18. The quadratic formula says that if F is a field with characteristic not equal to 2, and $f(x) = ax^2 + bx + c \in F[x]$ (for $a \neq 0$), then the roots of f are $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$.

Remark 19. Suppose F is a field, and $x^3 + bx^2 + cx + d \in F[x]$. If $Char F \neq 2, 3$, then by replacing x by $x - \frac{b}{3}$, we get a polynomial of the form $f(x) = x^3 + px + q$.

The following result of Cardano (in the 1500s) found that the roots of $f(x)$ can be found in the field $E = F(\omega, \delta, y_1, y_2)$ where $\omega^3 \in F$, $\delta^2 \in F(\omega)$, $y_1^2 \in F(\omega, \delta)$, $y_2^3 \in F(\omega, \delta, y_1)$. This is called a *root tower*.

7.2 Day 15 - September 28

Recall the following theorem from last class:

Theorem 24. Let E/F be a finite extension, and suppose $Char\ F \nmid n$. Suppose also that F contains a primitive nth root of unity. Then E/F is cyclic of degree $n_i|n$ if and only if $E = F(\alpha)$ for some α such that $\alpha^{n_i} \in F$.

Recall also the remark on the cubic formula from last class:

Remark 20. Suppose F is a field, and $x^3 + bx^2 + cx + d \in F[x]$. If $CharF \neq 2, 3$, then by replacing x by $x - \frac{b}{3}$, we get a polynomial of the form $f(x) = x^3 + px + q$.

The following result of Cardano (in the 1500s) found that the roots of $f(x)$ can be found in the field $E = F(\omega, \delta, y_1, y_2)$ where $\omega^3 \in F$, $\delta^2 \in F(\omega)$, $y_1^2 \in F(\omega, \delta)$, $y_2^3 \in F(\omega, \delta, y_1)$. This is called a *root tower*.

Namely,

$$\begin{aligned} \omega^3 &= 1 \\ \delta^2 &= 12p^3 - 81q^2 \\ y_1^2 &= \frac{27}{2}q + \frac{3}{2}\delta \\ y_2^3 &= \frac{27}{2}q - \frac{3}{2}\delta \end{aligned}$$

Definition 23. A field extension E/F is called *radical* if there exists a sequence of fields $F = E_0 \subset E_1 \subset ... \subset E_t = E$ where for each i, $E_i = E_{i-1}(u_i)$ and $u_i^{m_i} \in E_{i-1}$ for some $m_i \in \mathbb{N}$.

Definition 24. A polynomial $f(x) \in F[x]$ is called *solvable by radicals* over F if $f(x)$ splits completely in some radical extension of F.

Theorem 25. Let $f(x) \in F[x]$ be a separable polynomial, and let E be its splitting field. Suppose also that $Char\ F \nmid [E : F]$. Then if $Gal(E/F)$ is solvable, then $f(x)$ is solvable by radicals (over F).

Proof. Let $n = [E : F]$. We wish to reduce to the case where F contains a primitive n-th root of unity.

To this end, let ω be a primitive nth root of unity, and let $L = F(\omega)$. Note that since $Char\ F \nmid [E : F]$, then there are indeed $\phi(n)$ distinct nth roots of unity.

Note also that $f(x)$ is solvable by radicals over L if and only if its splitting field lies inside a radical extension R. This is the case if and only if $L = E_0 \subset ... \subset E_t = R$ for some appropriately chosen E_i. Let $E_{-1} = F$. Then $E_0 \subset ... \subset E_t$ is a radical tower if and only if $E_{-1} \subset E_0 \subset ... \subset E_t = R$ is a radical tower. This is the case if and only if $f(x)$ is solvable by radicals over $E_{-1} = F$.

Thus it suffices to show $f(x)$ is solvable by radicals over L.

By a homework problem [edit: see immediately below], EL/L is Galois and $G = Gal(EL/L)$ is isomorphic to a subgroup of $Gal(E/F)$. By assumption $Gal(E/F)$ is solvable, and a subgroup of a solvable group is solvable. Thus $G = Gal(EL/L)$ is solvable.

That is, there exists a normal series $\{1\} = G_t \lhd ... \lhd G_1 \lhd G_0 = G$. Recall that by a previous result, we can assume G_i/G_{i+1} is cyclic. If $n_i = \#G_i/G_{i+1}$, then certainly, $n_i|\#G = n$.

Let E_i be the subfield of EL fixed by G_i. (So $E_t = EL$ and $E_0 = F$). Then $Gal(E_t/E_i) = G_i \lhd G_{i-1} = Gal(E_t/E_{i-1})$. Since the one Galois group is normal in the other, then E_i/E_{i-1} is a normal extension, and $Gal(E_i/E_{i-1}) \cong G_{i-1}/G_i$, which is cyclic.

Thus by Theorem 24 $E_i = E_{i-1}(u_i)$, where $u_i^{n_i} \in E_i$. Thus EL/L is a radical extension, so $f(x)$ is solvable by radicals over L. Therefore it is solvable by radicals over F. ☐

Homework Problem 5. *Let $K \subset E \subset L$ and let $K \subset F \subset L$ be fields. Suppose E/K is finite and Galois. Then EF/F is Galois, and $Gal(EF/F)$ is isomorphic to a subgroup of $Gal(E/K)$.*

We now want to prove some form of the converse of this theorem.

Lemma 9. Let E/F be a radical extension, and let L be the normal closure of E/F. Then L/F is a radical extension.

Proof. Since E/F is radical, $E = F(u_1, ..., u_\ell)$, where there exists some $m \in \mathbb{N}$ such that $u_i^m \in F(u_1, ...u_{i-1})$ for all i.

Let $\sigma_1, ...\sigma_r$ be the distinct embeddings of $E \to \overline{F}$ fixing F.

Let $K = F(\{\sigma_j(u_i)\}_{i,j}\}$, and recall that L denotes the normal closure of F in E. We claim that $L = K$.

For each j, let τ_j be an extension of σ_j to $L \to L$. Then $\tau_j(u_i) = \sigma_j(u_i) \in L$ for all i, j (since L is the normal closure), so $K \subset L$.

Let $\pi : K \to \overline{F}$ be an embedding fixing F. It suffices to show that this sends elements of K to elements of K. In other words, it suffices to show that $\pi(\sigma_j(u_i)) \in K$ for all i, j. Extend π and σ_j to τ and $\tau_j \in Aut(L/F)$. Then $(\pi\sigma_j)(u_i) = (\tau\tau_j)(u_i)$. But $\tau\tau_j\Big|_E : E \to \overline{F}$ and fixes E, so $\tau\tau_j\Big|_E = \sigma_k$ for some k. Thus $(\pi\sigma_j)(u_i) = (\tau\tau_j)(u_i) = \sigma_k(u_i) \in K$. Thus K/F is normal, so $K \subset L$. Thus $K = L$.

It then suffices to show that K/F is radical. To do this, you adjoin the roots in a moderately clever way. First you adjoin $\sigma_i(u_1)$ for all i, since for all i, $\sigma_i(u_1)^{n_1} = \sigma_i(u_1^{n_1})$, and since E/F is radical, $u_1^{n_1} \in F$. Also, σ_i fixes F, so $\sigma_i(u_1)^{n_1} \in F$.

Then you adjoin $\sigma_i(u_2)$ for all i, and then continue through all the u_js. Finally, you have adjoined all $\sigma_j(u_i)$, so K/F is radical. Thus L/F is radical.

□

7.3 Day 16 - September 30

Recall from last class the following lemma (which we proved):

Lemma 10. Let E/F be a radical extension, and let L be the normal closure of E/F. Then L/F is a radical extension.

We will now prove another lemma:

Lemma 11. Let L/K be a Galois radical extension. Then the Galois group is solvable.

Proof. Since L/K is radical, there is a root tower $K = K_0 \subset K_1 \subset ... \subset K_t = K$, where $K_i = K_{i-1}(u_i)$ where $u_i^{m_i} \in K_{i-1}$ for all i.

We wish to show that we can in fact choose m_i such that $Char\ K \nmid m_i$ for all i. Suppose for the sake of contradiction that this is not the case. Then $Char\ K = p$, a prime, and let $m_i = lp^t$ where $p \nmid l$. Then $(u_i^l)^{p^t} \in K_{i-1}$, so u_i^l is purely inseparable over K_{i-1}. But L/K_{i-1} is separable, so $u_i^l \in K_{i-1}$. Thus we can replace m_i with l, and $p \nmid l$.

Let $m = m_1...m_t$. Then $Char\ K \nmid m$, and $u_i^m \in K_{i-1}$ for all i.

Let ω be a primitive mth root of unity. We will now show that, without loss of generality, we can assume $\omega \in K$. That is, we will show that $Gal(L/K)$ is solvable if $Gal(L(\omega)/K(\omega))$ is solvable.

Consider the five extensions in $K \subset K(\omega) \subset L(\omega)$ and $K \subset L \subset L(\omega)$ (namely $K(\omega)/K$), $L(\omega)/K(\omega)$, L/K, $L(\omega)/L$, and $L(\omega)/K$). We claim that all of these extensions are Galois and radical.

In no particular order, we can see that $K(\omega)/K$ and $L(\omega)/L$ are the splitting fields of $x^m - 1$, so they are Galois and radical. Also, L/K is radical and Galois by our hypothesis. Then since $L(\omega)/L$ and L/K are radical and Galois, then $L(\omega)/K$ is radical and Galois since "radicalness" and "radicalness" are transitive. It then suffices to show that $L(\omega)/K(\omega)$ is radical and Galois. This extension must be radical because L/K is radical, and you can take the same radical tower with the same exponents. Furthermore, $L(\omega) = LK(\omega)$, and by Homework Problem 5, $LK(\omega)/K(\omega)$ is Galois.

Therefore all of these extensions are radical and Galois.

Let $L' = L(\omega)$ and $K' = K(\omega)$. Let $K_i' = K_i(\omega)$.

Then, let $H_i = Gal(L'/K_i')$. By the theorem on m-cyclic extensions, K_i'/K_{i-1}' is cyclic. Thus $H_i \lhd H_{i-1}$ and H_{i-1}/H_i is cyclic. Then $H_0 = Gal(L'/K')$ and $H_t = Gal(L'/L') = \{1\}$, so $Gal(L'/K')$ is solvable. That is, $Gal(L(\omega)/K(\omega))$ is solvable.

Also, $Gal(K(\omega)/K)$ is isomorphic to a subgroup of $\mathbb{Z}_n^\times$, which is abelian. Thus $Gal(K(\omega)/K)$ is solvable.

But $Gal(K(\omega)/K) \cong Gal(L(\omega)/K)/Gal(L(\omega)/K(\omega))$, and by a previous theorem, since $Gal(K(\omega)/K)$ and $Gal(L(\omega)/K(\omega))$ are both solvable, then so is $Gal(L(\omega)/K)$.

But $Gal(L/K) \cong Gal(L(\omega)/K)/Gal(L(\omega)/L)$, and the quotient of a solvable group is solvable. Thus L/K is solvable.

□

Theorem 26. Let F be a field, and let $f(x) \in F[x]$ be a separable polynomial which is solvable by radicals over F. Let E be the splitting field of $f(x)$ over F. Then $Gal(E/F)$ is solvable.

Proof. Since $f(x)$ is solvable by radicals, there exists some radical extension L/F such that $E \subset L$.

By the first lemma (Lemma 10), we can assume L/F is normal (if not, replace it by its normal closure). Let $G = Aut(L/F)$. Note that $|G| = [L : F]_S \leq [L : F] < \infty$. Define $\phi : G \to Gal(E/F)$ by $\sigma \mapsto \sigma\Big|_E$. Note that ϕ does indeed map into $Gal(E/F)$ since E/F is normal.

Furthermore, any $\tau \in Gal(E/F)$ can be extended to some $\sigma \in Aut(L/F)$ since L/E is algebraic, and L/F is normal. Thus ϕ is surjective.

Thus to show that $Gal(E/F)$ is solvable, it suffices to show that $G = Aut(L/F)$ is solvable.

Let L_G be the fixed field of G. By Artin's Theorem, we know that L/L_G is Galois, and $G = Gal(L/L_G)$. Also, L/L_G is radical as $F \subset L_G$ and L/F is radical.

But by the second lemma (Lemma 11), G is solvable, as desired.

□

Recall that if $u_1, ..., u_n, x$ are indeterminants over F, then let $g(x) = \displaystyle\prod_{i=1}^{n}(x - u_i) \in F[u_1, ..., u_n, x] \subset F(u_1, ...u_n)[x]$. Let s_i be the correct polynomial in the u_is such that $g(x) = x^n - s_1x^{n-1} + ... + (-1)^n s_n$. Then the s_i are elements of $F[u_1, ..., u_n]$.

We showed that $F(u_1, ..., u_n)/F(s_1, ..., s_n)$ is a Galois extension, and the Galois group is S_n. Furthermore, we showed that $F(u_1, ..., u_n)$ is the splitting field for $g(x)$ over $F(s_1, ..., s_n)$.

Definition 25. Let F be a field. The *general equation of degree* n over F is $x^n - t_1x^{n-1} + ... + (-1)^n t_n$ where $t_1, ..., t_n$ are indeterminants over F.

Theorem 27. Let F be a field and let $t_1, ..., t_n$ be indeterminants. Furthermore, let $L = F(t_1, ..., t_n)$, and let $f(x) = x^n - t_1x^{n-1} + ... + (-1)^n t_n \in L[x]$. Let E be the splitting field of $f(x)$ over L. Then E/L is Galois and $Gal(E/L) \cong S_n$.

(A proof will be given next class.)

Remark 21. For $n \leq 4$, S_n is solvable. Therefore the general equation of degree $n \leq 4$ is solvable by radicals, so there exists a single formula for all functions of degree n. That is, there exists a quadratic, cubic, and quartic formula.

7.4 Day 17 - October 2

We will now prove this statement, which we said last class:

Theorem 28. Let F be a field and let $t_1, ..., t_n$ be indeterminants. Furthermore, let $L = F(t_1, ..., t_n)$, and let $f(x) = x^n - t_1x^{n-1} + ... + (-1)^n t_n \in L[x]$. Let E be the splitting field of $f(x)$ over L. Then E/L is Galois and $Gal(E/L) \cong S_n$.

Proof. Let $E = L(y_1, ..., y_n)$ where $y_1, ..., y_n$ are the n roots of $f(x)$ in $\overline{L}$. Then $f(x) = \displaystyle\prod_{i=1}^{n}(x - y_i)$ in $E[x]$. Then by definition of the elementary symmetric functions, $t_i = s_i(y_1, ..., y_n)$ for each i.

Then $E = L(y_1, ..., y_n) = F(y_1, ...y_n)$ since $L = F(t_1, ..., t_n)$ and each $t_i \in F(y_1, ..y_n)$.

Consider the diagram [which I can't draw lol] of $F[y_1, ...y_n] \leftarrow F[u_1, ..., u_n]$, where this arrow is ϕ given by plugging in y_i for u_i. Below this should be $F[t_1, ..., t_n] \to F[s_1, ..., s_n]$ with containment arrows going up. Here the function is ψ given by sending t_i to s_i. Since the t_is and u_is are indeterminants, these are surjections.

Note that $\phi\psi(t_i) = \phi(s_i) = \phi(s_i(u_1, ..., u_n)) = s_i(y_1, ..., s_n) = t_i$. Thus $\phi\psi$ is the identity on $F[t_1, ..., t_n]$. Thus ψ is injective and thus is an isomorphism.

Now consider a diagram of the field of fractions:

We have $L = F(t_1, ..., t_n) \subset F(y_1, ..., y_n) = E$, and $B = F(s_1, ..., s_n) \subset F(u_1, ..., u_n) = A$ (and these are the respective splitting fields). But we also have $\sigma : F(t_1, ..., t_n) \to F(s_1, ..., s_n)$ by $\sigma : \frac{a(t)}{b(t)} \mapsto \frac{a(s)}{b(s)}$.

But $f(x) \in L[x]$ and $f^\sigma(x) = x^n - s_1 x^{n-1} + ... + (-1)^n s_n = \prod_{i=1}^{n}(x - u_i)$. Thus A is the splitting field for f^σ over B. As E is the splitting field for $f(x)$ over L, we get an isomorphism $\tau : E \to A$ such that $\tau\Big|_L = \sigma$. Thus we've proven A/B is Galois, and $Gal(A/B) \cong S_n$. But because we have isomorphisms, E/L is Galois and $Gal(E/L) \cong S_n$. $\square$

Corollary 8. If $n \leq 4$, and $Char\ F \nmid n!$, then the general equation of degree n over F is solvable by radicals.

Proof. This follows from the fact that S_n is solvable for $n \leq 4$. $\square$

Corollary 9. (Abel's Theorem)

If $n \geq 5$, the general equation of degree n is not solvable by radicals (over any field).

Proof. This follows from the fact that S_n is not solvable for $n \geq 5$. $\square$

Exercise 7. Let p be prime. Then S_n is generated by any p-cycle and any transposition.

Proposition 14. Let $f(x) \in \mathbb{Q}[x]$ be any irreducible polynomial of prime degree with precisely two non-real roots. Let E be the splitting field of $f(x)$. Then $G = Gal(E/\mathbb{Q}) \cong S_p$.

Proof. As $deg f(x) = p$, and is separable, then every element of G is a permutation of the roots of $f(x)$. Thus $G \leq S_p$.

Let $\alpha \in E$ be a root of $f(x)$. Then $[F(\alpha) : F] = p$, since $f(x)$ is the minimal polynomial (assuming, without loss of generality, that $f(x)$ is monic). Thus $p\Big||G|$, so G contains an element of order p. But the only elements of order p in S_p are p-cycles, so G contains a p-cycle. Also, if τ denotes complex conjugaction restricted to E, then $\tau \in Gal(E/F)$, but τ is a transposition. Thus by the exercise, $G = S_p$. $\square$

Example 17. Let $f(x) = x^5 - 2x^3 - 8x - 2 \in \mathbb{Q}[x]$. By Eisenstein, $f(x)$ is irreducible.

We now use calculus to show that there are exactly three real roots. Observe that $f'(x) = 5x^4 - 6x^2 - 8 = (5x^2 + 4)(x^2 - 2)$. The only zeroes of $f'(x)$ are $\pm\sqrt{2}$, so it has at most 3 real roots (recall from calculus that between any two zeroes of a function is a zero of its derivative).

Note also that $f(-3) = -167$, $f(-1) = 7$, $f(0) = -2$, and $f(3) = 163$, so by the intermediate value theorem, $f(x)$ has three real roots. Thus by the proposition, this is a polynomial whose roots do not live in root towers!

Remark 22. RIP Quintic Formula

Question 2. (Inverse Galois Problem) Is every finite group the Galois group of a finite extension of $\mathbb{Q}$?

This is an open problem.

7.5 Day 18 - October 2

Lemma 12. Let m, n be distinct positive integers, such that $m|n$. Let p be a prime such that $p \nmid n$. Then $\Phi_n(x)$ and $x^m - 1$ have no common root mod p.

Proof. We know that $x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \left(\prod_{\substack{d|n \\ d<n}} \Phi_d(x) \right)$. Let $f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$. Then $x^n - 1 = \Phi_n(x) \cdot f(x)$. Note that $x^m - 1$ divides $f(x)$.

Suppose for the sake of contradiction that $a \in \mathbb{Z}$ is a common root of $x^m - 1$ and $\Phi_n(x)$ mod p. Then a is a double root of $x^n - 1$. But $p \nmid n$, so $x^n - 1$ has distinct roots mod p. This is a contradiction. $\square$

Theorem 29. Let $n > 1$ be an integer. Then there exists infinitely many primes congruent to 1 mod n.

Proof. Suppose for the sake of contradiction that there were only finitely many primes congruent to 1 mod n. Let $p_1, ..., p_k$ be the complete list of them.

We know that $\Phi_n(x)$ is monic, so $\Phi_n(s) > 1$ for all s sufficiently large.

Choose l sufficiently large such that $\Phi_n(lnp_1...p_k) \geq 2$. Note that the constant term of $\Phi_n(x) = \pm 1$. Let $a = lnp_1...p_k$.

As l, n, and each p_i divides each term of $\Phi(a)$ except the constant term, then we can see that $n \nmid \Phi(a)$ and $p_i \nmid \Phi(a)$.

Since $\Phi(a) \geq 2$, there exists a prime p dividing it. Then $\Phi_n(a) \equiv 0 \pmod p$, and since $\Phi_n(x)|x^n - 1$, then $a^n - 1 \equiv 0 \pmod p$. Thus $a^n \equiv 1 \pmod p$.

Also, $p \nmid n$, (since if $p|n$, then $p|a$, so $p \nmid \Phi_n(a)$, a contradiction). By the lemma, $a^m \not\equiv 1 \pmod p$ for all $m|n$ and $m < n$, so the order of a in $\mathbb{Z}_p^\times$ is n.

But by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p$, so $n|p-1$ so $p \equiv 1 \pmod n$. But p is not any p_i since no p_i divides $\Phi(a)$. This is a contradiction of our assumption that $p_1, ...p_k$ is a complete list of primes congruent to 1 mod n.

$\square$

Theorem 30. Let G be a finite abelian group. Then there exists a root of unity $\omega \in \mathbb{C}$ and a field $E \subset \mathbb{Q}(\omega)$ such that $F/\mathbb{Q}$ is Galois and $Gal(F/\mathbb{Q}) \cong G$.

Proof. Recall that by the classification of finite abelian groups, $G \cong C_{n_1} \times ... \times C_{n_k}$ where each C_{n_i} is a cyclic group of order n_i.

Let $p_1, ...p_k$ be distinct primes such that $p_i \cong 1 \bmod n_i$. (Remark: in order to do the pathological case $n_1 = n_2 = ... = n_k$, we need the fact that there are infinitely many primes congruent to 1 mod n_i.)

Let $m = p_1...p_k$. Then $\mathbb{Z}_m \cong \mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_k}$ (as rings).

So, $\mathbb{Z}_m^\times \cong \mathbb{Z}_{p_1}^\times \times ... \times \mathbb{Z}_{p_k}^\times$ as abelian groups.

But for all primes p_i, $\mathbb{Z}_{p_i}^\times$ is cyclic, and has $p_i - 1$ elements, so $\mathbb{Z}_m^\times \cong C_{p_1-1} \times ... \times C_{p_k-1}$. As $n_i|p_i - 1$, there exists $H_i \leq C_{p_i-1}$ of order $\frac{p_i-1}{n_i}$. Let $H = H_i \times ... \times H_k$. Then $Z_m^\times/H \cong C_{n_1} \times ... \times C_{n_k}$.

Let ω be a primitive mth root of unity, and let $E = \mathbb{Q}(\omega)$. We've seen $Gal(E/\mathbb{Q}) = \mathbb{Z}_m^\times$. Let $F = E_H$. As $\mathbb{Z}_m^\times$ is abelian, $F/\mathbb{Q}$ is Galois and $Gal(F/\mathbb{Q}) \cong \mathbb{Z}_m^\times/H \cong G$. $\square$

Stuff before this point: · will be on the exam. Stuff after it will not!

8 Algebraic Independence and Transcendental Extensions

Now let's start on algebraically independent things.

Definition 26. Let E/F be a field extension, and let $S \subset E$. We say S is *algebraically dependent over* F if there exist $s_1, ..., s_n \in S$ and $f(x_1, ..., x_n) \in F[x_1, ..., x_n]$ such that f is nonzero, but $f(s_1, ..., s_n) = 0$.

We say S is *algebraically independent over* F if it is not algebraically dependent.

Proposition 15. If S is the singleton $\{s\}$, then S is algebraically dependent over F if and only if s is algebraic. (Equivalently, S is algebraically independent over F if and only if s is transcendental.)

Example 18. Let $E = F(x, y)$ (the field of rational functions in x and y). Let $S = \{x^2, xy, y^2\}$. Then if $f(u, v, w) = uw - v^2$, then $f(x^2, xy, y^2) = 0$ and f is not the zero polynomial, so S is algebraically dependent over F.

Remark 23. Recall the concept from linear algebra that if S is linearly independent and $v \notin S$, then $S \cup \{v\}$ is linearly independent if and only if $v \notin Span(S)$.

We now write a version of this for algebraically independent sets over fields.

Lemma 13. Let E/F be a field extension, and let $S \subset E$ be an algebraically independent set over F. Let $u \in E$. Then $S \cup \{u\}$ is algebraically independent if and only if u is transcendental over $F(S)$.

Proof. Suppose u is not transcendental over $F(S)$.Then it is algebraic. That is, there exist $f(x) \in F(S)[x]$ such that $f(u) = 0$. Since $f(x)$ has coefficients in $F(S)$, there exists $s_1, ..., s_n \in S$ such that each coefficient is a polynomial in the s_i. Then f can be thought of as a root of the nonzero polynomial in $n + 1$ variables. □

Suppose instead that u is transcendental over $F(S)$. Suppose that g is a polynomial in $x_1, ..., x_n$ such that $g(s_1, ..., s_{n-1}, u) = 0$. Then this can be interpreted as a polynomial in one variable and $s_1, ..., s_{n-1}$, so it is a polynomial in $F(S)[x]$ with u as a root. Thus it is the zero polynomial.

8.1 Day 19 - October 7

Exam will be next week. The room was decided, but will be announced via email. We need to answer $4 - 5$ problems, but there will be more questions than that on the exam. Also, one of the problems will be a homework problem. Also, Friday will be review.

Recall the following Lemma

Lemma 14. Let E/F be a field extension and $S \subset E$ an algebraically independent set over F, and let $u \in E$. Then $U \cup \{u\}$ is algebraically independent if and only if u is transcendental over $F(S)$.

Proof. We proved the "only if" direction last time, so we will prove the "if" direction now.

By way of contradiction, suppose u is algebraic over $F(S)$. Then there exist $s_1, ..., s_n) \in S$ such that u is algebraic over $F(s_1, ..., s_n)$. That is, there exists a nonzero polynomial $f(x) \in F(s_1, ..., s_n)[x]$ such that $f(u) = 0$. The coefficients of $f(x)$ are of the form $\frac{a_i(s_1,...,s_n)}{b_i(s_1,...,s_n)}$. If we clear all denominators, we can find $f_1(x)$ with coefficients in $F[s_1, ..., s_n]$. But all denominators are non-zero, so the leading coefficient is non-zero. Also, $f_1(u) = 0$ still. Then, thinking of this as a polnyomial in $x_1, ..., x_n, x$, we have found u as a root. But $\{s_1, ..., s_n, u\}$ is algebraically independent over F, so this polynomial cannot evaluate to 0. This is a contradiction, and we are done. □

Definition 27. Let E/F be a field extension. A set $S \subset E$ is called a *transcendence base* for E/F if S is algebraically independent over F and $E/F(S)$ is algebraic.

Example 19. Let X and Y be indeterminants over F, and let $E = F(X, Y)$. Then $\{x, y\}$ is a transcendence base for E/F. But so is $\{X^2, Y^5\}$.

Theorem 31. Let E/F be a field extension. Then if L is an algebraically independent set, there exists a transcendence base of E/F containing L. Since $\emptyset$ is algebraically independent, it can be extended to a transcendence base, so there always exists a transcendence base.

Proof. We use Zorn's Lemma. Let $\Lambda = \{T |\ L \subset T \subset E,\ T \text{ is alg. ind. over} F\}$. This is partially ordered by containment. Also, $L \in \Lambda$, so Λ is nonempty.

Suppose C is a chain of Λ. Let $_C = \bigcup_{T \in C} T$. Then T_C is algebraically independent, since any finite subset of T_C is contained in some $T \in C$.

Thus T_C is an upper bound for C.

Thus by Zorn's Lemma, Λ has a maximal element, say S. Since $S \in \Lambda$, then S is algebraically independent. If $E/F(S)$ is not algebraic, it has a nonalgebraic element u. Then $S \cup \{u\}$ is algebrically independent, which contradicts the maximality of S. Thus S is a transcendence base for E/F. □

Theorem 32. Let E/F be a field extension, and let S, T be two transcendence bases for E/F. If $|S| < \infty$, then $|S| = |T|$.

Proof. Let $S = \{s_1, ...s_n\}$. Suppose for the sake of contradiction that for all $t \in T$, $\{t, s_2, ..., s_n\}$ is not algebraically independent. Then $F(T)$ is algebraic over $F(s_2, ..., s_n)$. Since $E/F(T)$ is algebraic, then $E/F(s_2, ..., s_n)$ is algebraic. Thus s_1 is algebraic over $F(s_2, ..., s_n)$, so S was not algebraically independent. This is a contradiction, so there exists some $t_1 \in T$ such that $\{t_1, s_2, ..., s_n\}$ is algebraically independent.

Suppose for the sake of contradiction that $E/F(t_1, s_2, ..., s_n)$ were not algebraic. Since $E/F(s_1, ..., s_n)$ is algebraic, then $E/F(s_1, ..., s_n, t)$ is algebraic. Thus $F(s_1, ..., s_n, t)/F(s_2, ..., s_n, t)$ is not algebraic, so s_1 is transcendental over $F(s_2, ..., s_n, t)$, so $\{s_1, ..., s_n, t\}$ is algebraically independent by the lemma. But t_1 is algebraic over $F(s_1, ..., s_n)$, and this contradicts the lemma. Thus $E/F(t_1, s_2, .., s_n)$ is algebraic, so $\{t_1, s_2, ..., s_n\}$ is a transcendence base.

By repeated application of this, we can replace all the elements of S with elements of T. But the elements of a transcendence base are always distinct, so in particular these elements of T must be distinct, so $|S| \leq |T|$. One could also do this process going the other way, giving that $|T| \leq |S|$, so $|T| = |S|$ as desired.

□

Definition 28. The *transcendence degree* of E/F is the number of elements in any transcendence base for E/F.

Proposition 16. If E/F is a field extension, then E/F is algebraic if and only if $\operatorname{Tr}.deg(E/F) = 0$.

Theorem 33. Let $E/F/L$ be a tower of fields. Then $\operatorname{Tr}.deg(E/L) = \operatorname{Tr}.deg(E/F) + \operatorname{Tr}.deg(F/L)$.

Proof. Let $S \subset E$ be a transcendence base for E/F and let $T \subset F$ be a transcendence base for F/L. Note that $S \cap F = \emptyset$, so $S \cap T = \emptyset$. Thus $|S \cup T| = |S| + |T| = \operatorname{Tr}.deg(E/F) + \operatorname{Tr}.deg(F/L)$.

Thus it suffices to show that $S \cup T$ is a transcendence base of E/L.

We first show that $E/L(S \cup T)$ is algebraic. We know that F is algebraic over $L(T)$, so $F(S)$ is algebraic over $L(T)(S) = L(S \cup T)$. As $E/F(S)$ is algebraic, $E/L(S \cup T)$ is algebraic.

We now need to show $S \cup T$ is algebraically independent over L¿ Let $f(x_1, ..., x_m, y_1, ...y_n) \in L[x_1, ..., x_m, y_1, ...y_n]$ and suppose $f(s_1, ..., s_m, t_1, ...t_n) = 0$ for some $s_i \in S$ and $t_i \in T$. We need to show $f = 0$.

Write $f = \sum_j g_j(y_1, ..., y_n)h_j(x_1, ..., x_m)$. Then the h_js are distinct monomials in $x_1, ..., x_m$. Let $l(x_1, ..., x_m) = f(x_1, ..., x_m, t_1, ..., t_n) \in L(T)[x_1, ..., x_m] \subset F[x_1, ..., x_m]$. But $l(s_1, ..., s_m) = 0$, and S is algebraically independent over F. Thus $l(x_1, ..., x_m) = 0$. Then $\sum g_j(t_1, ...t_n)h_j(x_1, ..., x_m) = 0$. As the h_js are linearly independent over F, then $g_j(t_1, ..., t_n) = 0$ for all i. As $\{t_1, ..., t_n\}$ is algebraically independent over L, $g_j(y_1, ..., y_n) = 0$ for all i. Thus $f = 0$, so $S \cup T$is algebraically independent.

Thus $S \cup T$ is a transcendence base, so $\operatorname{Tr}.deg(E/L) = |S \cup T| = \operatorname{Tr}.deg(E/F) + \operatorname{Tr}.deg(F/L)$ as desired. □

9 Introduction to Rings and Modules

9.1 Day 20 - October 9

Definition 29. A *ring* has a multiplicative identity, but may not be commutative. You know the rest.

Example 20. (Matrix Rings) If R is a ring, then let $\mathcal{M}_n(R)$ denote the set of $n \times n$ matrices with entries from R. Then $\mathcal{M}_n(R)$ is also a ring. Furthermore, if $n \geq 2$, this ring is noncommutative (except maybe for $R = 0$).

Example 21. (Group Rings) Let R be a ring (usually commutative), and let G be a group. Let $R[G]$ be a free R-module with basis G (i.e. it is the set of R-linear combinations of elements of G). Then $R[G] = \bigoplus_{g \in G} Rg$. We also give $R[G]$ a multiplication operation by defining $(r_1g_1)(r_2g_2) = r_1r_2(g_1g_2)$.

For a particular example, consider $R = \mathbb{Z}$ and $G = C_3$, the cyclic group of 3 elements. Then $R[G] = \mathbb{Z}(C_3)$. If a is a generator of C_3, then $(2 + 3a)(1 - a^2) = 2 - 2a^2 + 3a - 3 = -1 + 3a - 2a^2$.

In general, $R[G]$ is commutative if and only if G is abelian.

Example 22. (Skew Polynomial Rings) Let R be a commutative ring, and $\sigma : R \to R$ be a ring homomorphism. Let $R[x, \sigma] = R[x]$ as a left R-module, but define multiplication in $R[x, \sigma]$ by $(ax^m)(bx^n) = a\sigma^n(b)x^{m+n}$.

In particular, if $Char\ R = p$, then $f : R \to r^p$ is a ring homomorphism. Then $R[x, f]$ is given by $ax^mb^n = ab^{p^m}x^{m+n}$.

Example 23. (Real Quaternions) Considering the following matrices in $\mathcal{M}_2(\mathbb{C})$: $1 = id$, $\bar{i} = [i, 0, 0, -i]$, $\bar{j} = [0, 1, -1, 0]$, and $\bar{k} = [0, i, i, 0]$. We let $\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}\bar{i} \oplus \mathbb{R}\bar{j} \oplus \mathbb{R}\bar{k}$. In fact, $\mathbb{H}$ is a ring with the usual multiplication (it suffices to check that multiplication works out). One can check that $\overline{i}^2 = \overline{j}^2 = \overline{k}^2 = \overline{ijk} = -1$, so it is a ring.

In fact, $\mathbb{H}$ is a division ring. Since if $\alpha = r_0 1 + r_1 i + r_2 j + r_3 k$, set $\overline{\alpha} = r_0 1 - r_1 i - r_2 j - r_3 k$. Then $\alpha\overline{\alpha} = (r_0^2 + r_1^2 + r_2^2 + r_3^2)1$, so $\alpha^{-1} = \frac{\overline{\alpha}}{|\alpha|^2}$.

Definition 30. Let R be a ring. A *left R-module* is an abelian group $(M, +)$ and an operation $\cdot : R \times M \to M$ such that the usual axioms hold. That is,

1. $(r + s)m = rm + sm$

2. $r(m + n) = rm + rn$

3. $r(s(m)) = (rs)m$

4. $1 \cdot m = m$

[Remark: some people do without the fourth property. To make it clear that we have the fourth property, one might say it is a *unital* module.]

A *right R-module* is the same, but the operation is on $M \times R$ and obeys $(m(s))r = m(sr)$ instead of the third property.

Definition 31. If R is a ring, a *left* (respectively, *right*) *ideal* of R is just a left (respectively, right) R-submodule of R. An *ideal* of R is a left ideal which is also a right ideal (a "2-sided ideal").

Definition 32. Let R be a ring, and let M be a left R-module. M is called (left) *Noetherian* or (respectively, (left) *Artinian*) if M satisfies the Ascending Chain Condition (respectively, the Descending Chain Condition) on (left) submodules.

Recall that the ascending chain condition is that if $N_1 \subset N_2, ...,$ is a chain of submodules of M, then there exists n such that $N_n = N_{n+1} = ...$ (i.e. the chain stabilizes). [Remark: the notation implies that the chain is countable, but countable chains stabilizing is equivalent to any chain stabilizing.] The decreasing chain condition is the same but for decreasing chains of submodules.

A ring R is left or right Noetherian or Artinian if and only if it is that adjective as an R-module.

Definition 33. Let R and S be rings. We say M is an $R - S$ bimodule if M is a left R-module, a right S-module, and $(rm)s = r(ms)$ for all $r \in R$, $m \in M$, and $s \in S$.

Example 24. Let R and S be rings, and let M be an $R - S$ bimodule. Let A denote the set of upper triangular matrices $(r, m, 0, s)$ where $r \in R$, $m \in M$, and $s \in S$. Then this is indeed a ring and all of the stuff holds.

Exercise 8. Show that A is left Noetherian if and only if R and S are left noetherian and M is left Noetherian.

Also show that the same statement holds if "left" is replaced with right, and/or "Noetherian" is replaced by "Artinian".

Example 25. Let $A = (\mathbb{Q}, \mathbb{Q}, 0, \mathbb{Z})$. Recall that $\mathbb{Q}$ is a field, so it is Noetherian (as a ring), and $\mathbb{Z}$ is a Principal Ideal Domain, so it is Noetherian (as a ring). But $\mathbb{Q}$ is not Noetherian as a (right) $\mathbb{Z}$-module. Thus A is left Noetherian, but not right Noetherian.

If instead $A = (\mathbb{R}, \mathbb{R}, 0, \mathbb{Q})$, then this is left Artinian but not right Artinian.

9.2 Day 21 - October 12

Review day!

This was a theorem from 818:

Theorem 34. Let E/F be algebraic, and let $\sigma : E \to E$ be a field embedding which fixes F. Then σ is in fact onto. That is, σ is an automorphism.

Proof. One proof uses vector space dimension: E is an F-vector space, so if E/F is finite, then σ is an F-linear transformation, so since σ is injective, it is also surjective. The infinite dimensional case can be reduced to the finite dimensional case since $E/F$is algebraic.

Alternatively, let $\alpha \in E$, and let $f_\alpha(x) = Min(\alpha, F)$. Let $\beta_1, ..., \beta_n$ be the roots of $f_\alpha \in E$. For each i, $\sigma(\beta_i) = \beta_j$ for some j, so if you restrict σ to $\{\beta_1, ..., \beta_n\}$, then it is still injective. Therefore it is a permutation of the β_is, so it is surjective. Since α is some β_i, and α was arbitrary, then σ is surjective. ☐

10 Exact Sequences

10.1 Day 22 - October 14

Back to rings:

Exact sequences!

Definition 34. A sequence of R-linear maps of left R-modules N_i with $f_i : N_i \to N_{i+1}$ (where N_i is called "degree i") is said to be *exact in degree* $i+1$ if $imf_i = kerf_{i+1}$. We say the entire sequence is *exact* if it is exact at in all of its degrees.

We often write our exact sequence as

$$... \to N_i \xrightarrow{f_i} N_{i+1} \xrightarrow{f_i+1} N_{i+1} \to ...$$

Example 26. We have that $0 \to A \xrightarrow{f} B$ is exact if and only if $kerf = 0$ if and only if f is injective.

Example 27. Similarly, $A\overline{g} \to B \to 0$ is exact if and only if g is surjective.

Example 28. By combining these, $0 \to A \to 0$ is exact if and only if $A = 0$.

Example 29. Lastly, $0 \to A \xrightarrow{f} B \to 0$ is exact if and only if f is an isomorphism.

Definition 35. An exact sequence of the form $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is called a *short exact sequence*. A short exact sequence has the property that f is injective, $im\ f = ker\ g$, and g is onto.

Example 30. Let N be a submodule of M. Then $0 \to N \overset{inclusion}{\to} M \overset{projection}{\to} M/N \to 0$ is a short exact sequence.

Example 31. Let M_1 and M_2 be modules. Then $0 \to M_1 \xrightarrow{f} M_1 \oplus M_2 \xrightarrow{g} M_2 \to 0$ is a short exact sequence when $f : u \mapsto (u, 0)$ and $g : (u, v) \mapsto v$. This short exact sequence is called a *split short exact sequence* since there are maps $f' : M_1 \oplus M_2 \to M_1$ and $g' : M_2 \to M_1 \oplus M_2$ such that $f \circ f' = id_{M_1}$ and $g' \circ g = im_{M_2}$.

Example 32. The following short exact sequence is not a split exact sequence: $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \to 0$, where $f(n) = 2n$ and $g(m) = \overline{m}$.

Remark 24. We have been leaving off the word "left" a lot, but it should probably be around. Also, most theorems give another theorem if you find/replace the word "left" with the work "right".

Theorem 35. [Two theorems in one!] Let R be a ring and let $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ be a short exact sequence of left R-modules. Then M is Noetherian (respectively, Artinian) if and only if both L and N are Noetherian (respectively, Artinian).

Proof. We know that $L \cong f(L)$, and $N \cong M/ker\ g = M/f(L)$. Thus without loss of generality, we can assume $L \subset M$ and $N \subset M/L$.

If M is Noetherian (respectively, Artinian), ideals in L are ideals in M, so any descending (respectively, ascending) chain stabilizes in L. Thus L is Noetherian (respectively, Artinian). Also, a chain in $N = M/L$ can be lifted to a chain in M, which must stabilize, and when we project back down, the result must stabilize. Thus $N = M/L$ is Noetherian (respectively, Artinian), as desired.

Conversely, suppose both L and N are Noetherian (Artinian case will be identical, but not proven). Let $A \supset A_2 \supset ...$ be a descending chain of left R-submodule of M. Then $A \cap L_1 \supset A \cap L_2 \subset ...$ is a descending chain of L-modules. Since L is Noetherian, this chain stabilizes. Thus there exists a k such that $A_k \cap L = A_{k+1} \cap L$ for all $i \geq 0$.

Also, $A_1 + L \supset A_2 + L \supset ...$, so $\frac{A_1+L}{L} \supset \frac{A_2+L}{L} \supset ...$ is a descending chain in $N = M/L$. As M/L has the descending chain condition, there exists an l such that $\frac{A_l+L}{L} = \frac{A_{l+1}+L}{L}$ for all $i \geq 0$. But this is the case if and only if $A_l + L = A_{l+i} + L$.

Let $j = \max(k, l)$. We wish to show that $A_j = A_{j+i}$ for all $i \geq 0$. Fix some $i \geq 0$. Let $u \in A_j \subset A_j + L = A_{j+i} + L$. Then $u = a_{j+i} + l_{j+i}$ for some $a_{j+i} \in A_{j+i}$ and $l \in L$. Then $u - a_{j+i} = l_{j+i} \in A_j \cap L = A_{j+i} \cap L \subset A_{j+i}$. Thus $u \in A_{j+i}$, so $A_j \subset A_{j+i}$, so $A_j = A_{j+i}$. Thus the chain has stabilized.

As remarked, the Artinian proof is similar. □

Corollary 10. If M, N R-modules, then both M and N are Noetherian (respectively, Artinian) if and only if $M \oplus N$ is Noetherian (respectively, Artinian).

Proof. Apply the previous theorem to $0 \to M \to M \oplus N \to N \to 0$, which is a short exact sequence. □

Corollary 11. A module M is Noetherian (respectively, Artinian) if and only if $M^n = \bigoplus_{i=1}^n M$ is Noetherian (respectively, Artinian).

Proof. Apply the previous corollary over and over, and induct on n. □

Corollary 12. Let R be a left Noethereian (respectively, Artinian) ring, and let M be a finitely generated left R-module. Then M is left Noetherian (respectively, Artinian).

Proof. Since M is finitely generated, then $M = Rx_1 + ... + Rx_n$ for some $x_1, ..., x_n \in M$. Then define and R-linear map $\phi : R^n \to M$ by $(r_1, ..., r_n) \mapsto \sum r_i x_i$. Note that ϕ is onto.

Since R is left Noetherian (respectively, left Artinian), then R^n is left Noetherian (respectively, left Artinian), so $M = R^n / ker\ \phi$ is Noetherian.

□

Remark 25. Let $\phi : R \to S$ be a ring homomorphism (including the restriction that $\phi(1) = 1$). Then ϕ defines a left- and right-R-module structure on S. In particular, for $r \in R$ and $s \in S$, define $r \cdot s = \phi(r)s$ and $s \cdot r = s\phi(r)$. If $im\ \phi \subset Z(S) = \{t \in S | at = ta \text{ for all } a \in S\}$ (the so-called "center" of S), then S is called an *R-algebra*.

Remark 26. Let $\phi : R \to S$ be a ring homomorphism. Suppose R is left Noetherian (respectively, Artinian) and suppose S is finitely generated as a left R-module. Then S is left Noetherian (respectively, Artinian), as a ring.

Proof. By Corollary 12, S is left Noetherian (respectively, Artinian) as an R-module. But every left S module is a left R-module because of ϕ. Thus S satisfies the ascending chain condition on left ideals, since such left ideals are left R-modules. □

Example 33 (Don't got time for this!).

Remember, no class on Friday!

11 Notherian Rings

11.1 Day 23 - October 21

More rings!

Example 34. Recall that if R is a commutative ring, and G is a finite group, then $R[G]$ is the group ring generated by R and G. As a module, it is a free module over R with basis G. We define multiplication the logical way to make it a ring.

Define $\phi : R \to R[G]$ by $r \mapsto r \cdot 1$. Then ϕ is a ring homomorphism and $im\phi \subset Z(R[G])$.

Therefore, $R[G]$ is an R-algebra. Note that $R[G]$ is a finitely generated left and right R-module.

Therefore, if R is Noetherian, $R[G]$ is (left and right) Noetherian as a ring. Similarly, if R is Artinian, $R[G]$ is left and right Artinian.

Proposition 17. Let R be a ring, and let M be a left R-module. Then the following are equivalent

1. M is (left) Noetherian.

2. Every (left) R-submodule of M is finitely generated.

3. Every nonempty subset of (left) R-submodules of M has a maximal element. (I.e. there exists an $A \in \Lambda$ such that if $A \leq B$ and $B \in \Lambda$, then $A = B$.

Proof. (1 implies 2) Let N be a submodule of N. Choose $x_1 \in N$, and let $L_1 = Rx_1 \subset N$. If $N \neq L_1$, choose an $x_2 \in N \setminus L_1$, and let $L_2 = L_1 + Rx_2$. Note $L_1 \subsetneq L_2 \subset N$.

We repeat this process: if $L_n \neq N$, then take some $x_{n+1} \in N \setminus L_n$, and let $L_{n+1} = L_n + Rx_{n+1}$. This gives us $L_1 \subsetneq L_2 \subsetneq L_3 \subsetneq ....$ If for all n, $L_n \neq N$, this would give us an infinite strictly increasing chain, contradicting Noetherian-ness. Thus $N = L_n$ for some n, but $N = Rx_1 + ... + Rx_n$, so N is finitely generated. Thus every submodule is finitely generated, as desired.

(2 implies 3; actually, not 3 implies not 2) Suppose Λ is a nonempty collection of submodules with no maximal element. Then there exists an infinite an infinite ascending chain of submodules $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq ...$

For all $i \geq 2$, choose some $x_i \in N_i \setminus N_{i-1}$, and let N denote the module generated by x_2, x_3,... Note that $N \subset \bigcup_{i=1}^{\infty} N_i$. If N were finitely generated, then all of its generators would come from some N_k. Thus $x_i \in N_k$ for all i, so in particular $x_{k+1} \in N_k$, which is a contradiction. Thus N is not finitely generated, as desired.

(3 implies 1) If $L_1 \subset L_2 \subset ...$, then let $\Lambda = \{L_i | i \in \mathbb{N}\}$. Then Λ has a maximal element L_k. That is, the chain stabilizes at L_k.

□

Remark 27. If a ring is Noetherian, condition (3) from this proposition means we don't have to worry about citing Zorn's lemma! Condition (3) is really powerful!

Example 35. Let F be a field, and let $\sigma : F \to F$ be a nonzero field homomorphism which is not surjective. (For example, it might be that $F = \mathbb{Q}(t)$, where t is an indeterminant, and we define $\sigma : F \to F$ by $\frac{f(t)}{g(t)} \mapsto \frac{f(t^2)}{g(t^2)}$.)

Then we have $F[x;\sigma]$ is left Noetherian, but not right Noetherian. (We will prove this.)

(Hold up, what the heck is $F[x;\sigma]$? As an F-vector space, $F[x;\sigma] = F[x]$. We give it a different multiplication though: $(a_n x^n)(b_m x^m) = a_n \sigma^n(b_m) x^{n+m}$.)

Before we prove the claim from the example, we prove a lemma.

Lemma 15. Let $f(x)$, $g(x) \in F[x;\sigma]$, with $g(x) \neq 0$. Then there exists $q(x)$, $r(x) \in F[x;\sigma]$ such that $f = qg + r$, and deg $r <$ deg g.

Proof. Let $f(x) = a_m x^m + ... + a_0$, and let $g(x) = b_n x^n + ... b_0$. If $m < n$, we are already done, since we can let $q = 0$, and $r = f$.

But if $m \geq n$, then consider $f - a_m(\sigma^{m-n}(b_n))^{-1} x^{m-n}$. Observe that this has no degree m term, so its degree is strictly less than m. Then proceed by induction to strip away all the degrees. □

Proof. (Of the claim in the example)

Let $R = F[x;\sigma]$.

We first show that every left ideal of $F[x;\sigma]$ is principal. Let $I \neq 0$ be a left ideal of $F[x;\sigma]$. Choose $g \in I \setminus \{0\}$ of minimal degree. Then certainly $Rg \subset I$. If $f \in I$, then by the lemma, there exists a quotient and remainder such that $f = qg + r$, so $r = f - qg$. Since I is a left ideal, then $r \in I$, but r has degree strictly less than the degree of g, so $r = 0$. Thus $f = qg$, so $f \in Rg$. Thus $Rg = I$, so all left ideals are principal.

Thus in particular, all left ideals are finitely generated, so $F[x;\sigma]$ is left Noetherian.

We now wish to show that R is not right Noetherian. We shall do so by constructing an infinite ascending chain of right ideals. Since σ is no surjective, choose some $b \in F \setminus \sigma(F)$. Let $M_0 = bxR$, and for all For all $i > 0$, let $M_i = x^i bxR + M_{i-1}$. Certainly, $x^i bx \in M_i$. We wish to show that $x^n bx \notin M_{n-1}$.

Suppose for the sake of contradiction that $x^n bx \in M_{n-1}$. Then $x^n bx = x^{n-1}bxf_{n-1}(x) + ... + bxf_0(x)$ for some $f_{n-1}, ..., f_0 \in R$. Then $bxf_0(x) = xg(x)$ for some $g(x) \in R$. Let $r = \deg\ f_0 = \deg\ g$.

If $f_0 = a_r x^r + ... + a_0$, and $g_1 = c_r x^r + ... + c_0$, then $b\sigma(a_r) = \sigma(c_r)$. Thus $b = \sigma(\frac{c_r}{a_r}) \in \sigma(F)$, which is a contradiction. Thus $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq ...$ is a strictly ascending chain of right modules, so R is not right Noetherian. □

Recall the Hilbert Basis Theorem, in all of its glorious generality:

Theorem 36 (Hilbert Basis Theorem). Let R be a left Notherian ring, and let X be a variable. Then $R[x]$ is left Noetherian.

By induction, $R[x_1, ..., x_n]$ is left Noetherian for commuting variables $x_1, ..., x_n$.

Remark 28. Subrings of Noetherian (or Artinian) rings are not necessarily Noetherian or Artinian.

Example 36. Note $\mathbb{Z} \subset \mathbb{Q}$, and since $\mathbb{Q}$ is a field, it is Artinian. But $\mathbb{Z}$ is not Artinian.

12 Simple Rings and Modules

12.1 Day 24 - October 23

Definition 36. Let R be a ring. An *ideal* in R is a left ideal that happens to be a right ideal as well. That is, I is an ideal if $(I, +)$ is a subgroup of $(R, +)$, and $rI \subset I$ and $Ir \subset I$ for all $r \in \mathbb{R}$.

Definition 37. The two *trivial ideals* of a ring R are (0) and R.

A ring R is *simple* if it has no nontrivial ideals.

Example 37. Let $R = M_2(\mathbb{Q})$. Then $I = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \Big| a, b \in \mathbb{Q}\}$ is a left ideal but not a right ideal.

Another example is $R = M_2(\mathbb{Z})$. Let $I = \{2A | A \in R\} = M_2(2\mathbb{Z})$. Then I is a nontrivial ideal.

Remark 29. Any division ring is simple. By a homework problem [edit: see immediately below], $M_n(D)$ is simple whenever $n \geq 1$ and D is a division ring.

Homework Problem 6. *Let $n \in \mathbb{N}$, let R be a ring, and let $S = M_n(R)$. Then there is a natural bijection between the two-sided ideals in R and the two-sided ideals in S given by $I \leftrightarrow M_n(I)$.*

Example 38. If $\phi : R \to S$ is a ring homomorphism, then $\ker\ \phi$ is an ideal of R.

If R is simple, every such $\phi : R \to S$ is either 0 or injective.

Example 39. Let M be a (left) R-module, and let $\mathrm{Ann}_R\ M = \{r \in R | rM = 0\}$. Then $\mathrm{Ann}_R\ M$ is a (two-sided) ideal of R. This is the case because if $r \in \mathrm{Ann}_R\ M$, and $s \in R$, then $(sr)M = s(rM) = s \cdot 0 = 0$, and $(rs)M = r(sM) \subset rM = 0$.

Aside 1. Let $x \in M$. Then $\mathrm{Ann}_R\ x = \{r \in R | rx = 0\}$. Then $\mathrm{Ann}_R\ x$ is a left ideal, but not necessarily a right ideal. However, $\mathrm{Ann}_R\ Rx$ is an ideal.

Definition 38. Let R be a ring. An R-module M is called *simple* if $M \neq 0$, and M has no non-trivial submodules.

Remark 30. A simple ring is not necessarily simple as a left R-module. For instance, take $M_2(\mathbb{Q})$. We showed that this is simple, but it had a nontrivial left ideal. Therefore it is not simple as a left R-module.

Proposition 18. An R-module M is simple if and only if $M \cong R/I$ for some maximal left ideal I.

Proof. ($\Leftarrow$) Suppose $M \cong R/I$ for some maximal ideal I. Recall that the submodules of R/I are in one-to-one correspondence with the submodules of R containing I. As I is maximal, the only submodules containing I are R and I. So the only submodules of R/I are R/I and $I/I = 0$. Thus $M = R/I$ is simple (as a R-module), as desired.

($\Rightarrow$) Let $x \in M$, $x \neq 0$. Then Rx is a submodule of M, but it is nonzero, so $Rx = M$ since M is simple. Define an R-homomorphism $\phi : R \to Rx = M$ by $r \mapsto rx$. Then by an isomorphism theorem, $M \cong R/I$, where $I = \ker\ \phi$. Since R/I is simple, I is maximal as a left ideal. $\square$

Remark 31. If R is commutative, then left ideals are precisely two-sided ideals, so M is simple if and only if $M = R/m$ where m is a maximal ideal. But R/m is a field, so the only simple R-modules are fields.

If R is a local ring (i.e. there is a unique maximal ideal), then this implies that for all simple R-modules are isomorphic.

Example 40. For the complex numbers, things are nicely behaved by Hilbert's Nullstellensatz.

For a not-algebraically-closed field, things need not be very nice. For instance, let $R = \mathbb{R}[x]$. Let $m_1 = (x)$. Then $R/m_1 \cong R$. Let $m_2 = (x^2 + 1)$. Then $R/m^2 \cong \mathbb{R}(i) = \mathbb{C}$. Thus two simple modules have led to different fields.

Example 41. Let D be a division ring, and let $R = M_n(D)$, where $n \geq 1$. Consider $M = D^n = \{\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \Big| a_i \in D\}$. Then M is a left R-module by matrix multiplication.

We claim that D^n is a simple R-module. It suffices to show that $Ru = D^n$ for all $u \in D^n \setminus \{0\}$. Note that D^n is generated by the vector $(1, 0, 0, ..., 0)$. This vector is generated by any vector of the form $(a_1, 0, ..., 0)$ (where $a_1 \neq 0$) since we can divide by a_1. But this is generated by any nonzero vector by multiplying by the right matrix which kills all-but-one term, and also the right row swapping matrix.

Example 42. Let $R = S_3$, let $R = \mathbb{C}[S_3]$ (or any algebraically closed field of characteristic not equal to 2 or 3). Recall that $R = \mathbb{C}1 \oplus \mathbb{C}(12) \oplus ... \oplus \mathbb{C}(132)$.

Let $I_1 = \mathbb{C}(1 + (12) + (13) + (23) + (123) + (132)$. This is a $\mathbb{C}$-vector space, at least. But also, multiplying by any element of S_3 will only permute the terms, so it is a left R-module.

Also, as a vector space it is dimension 1, so there are no nontrivial submodules (which would be subspaces). Thus I_1 is a simple left R-module.

Let $u_1 = (1) + (12)$ and let $u_2 = (23) + (132)$ and let $u_3 = (13) + (123)$. Let $v_1 = u_1 - u_2$ and let $v_2 = u_1 - u_3$.

Let $I_2 = \mathbb{C}v_1 + \mathbb{C}v_2$. We can check that v_1 and v_2 are linearly independent, so this has dimension 2, as a $\mathbb{C}$-vector space. Also, by checking left multiplication, I_2 is a left ideal.

Finally, by a complicated argument that will remain a secret, but apparently involving character theory, I_2 has no nontrivial submodules. Thus I_2 is is simple as a left module.

13 Semisimple Rings and Modules

13.1 Day 25 - October 26

No homework was posted yet, since Tom was at a conference!

(Recall that an ring is simple if it only has two (two-sided) ideals. A module is called simple if it is nonzero and has no proper submodules.)

Definition 39. An R-module M is called *semisimple* if every submodule N of M is a direct summand of M (i.e. there exists $N' \subset M$ such that $M = N \oplus N'$ (i.e.i.e. $M = N + N'$ and $N \cap N' = 0$)).

Aside 2. Let $\{N_\lambda\}_{\lambda \in I}$ be a collection of submodules of M. Then $\sum_{\lambda \in I} N_\lambda = \{\text{finite sums of elements of } N_\lambda s\}$. This is a submodule of M, and is the smallest such submodule containing all of the N_λs.

We write $\sum_{\lambda \in I} N_\lambda = \bigoplus_{\lambda \in I} N_\lambda$ if for all $x \in N$, there exist unique $a_\lambda \in N_\lambda$ for each $\lambda \in I$ such that $x = \sum_{\lambda \in I} a_\lambda$ (that is, each element can be written uniquely as a sum). This is called the *internal direct sum*.

The *external direct sum* is the set of ordered I-tuples such that all but finitely many entries are nonzero, with termwise addition.

Exercise: The sum is direct if and only if the sum is isomorphic to the external direct product.

Exercise: The sum is direct if and only if for all $\lambda \in I$, $N_\lambda \cap (\sum_{\delta \neq \lambda} N_\delta) = (0)$.

Remark 32. A simple module is always semisimple. A simple ring is not always semisimple (as a module).

Claim 1. Let D be a division ring. Then any D-module is semisimple.

Proof. Let M be a D-module, and let N be a submodule. Let β be a basis for N, and extend to a basis β' of M. Let $N' = Span_D(\beta' \setminus \beta)$. hen $M = N \oplus N'$. □

Lemma 16. Any submodule of a semisimple module is semisimple.

Proof. Let M be semisimple and let A be a submodule of M. Let B be a submodule of A. As B is a submodule of M, $M = B \oplus N$ for some N.

We wish to show that $A = B \oplus (N \cap A)$. Certainly, $B + (N \cap A) \subset A$. Let $a \in A$. Then $a \in X$, so $a = b + n$, for some $b \in B$, $n \in N$. But $n = a - b \in A$. Thus $n \in N \cap A$. Thus $A \subset B + (N \cap A)$, so $A = B + (N \cap A)$.

Finally, we wish to show that this sum is direct. Note that $B \cap (N \cap A) \subset B \cap N = (0)$, so B and $(N \cap A)$ are disjoint. Thus the sum is direct, from the second criterion in the aside. □

Remark 33. If M is semisimple, then so is M/N. This is the case because $M/N = (N + N')/N \cong N'$, a submodule of M. Thus M/N is isomorphic to a submodule of M, so it is semisimple by the previous lemma.

Proposition 19. Every nonzero semisimple module contains a simple submodule.

Proof. Let M be a nonzero semisimple R-module. Let $x \in M$ be a nonzero element. Then Rx is semisimple since it is a submodule of a semisimple module. We then wish to show that Rx contains a simple submodule.

Let $\Lambda = \{A | A \subset Rx, x \notin A\}$. Note that $\Lambda \neq \emptyset$ since $(0) \in \Lambda$. Also, for any chain $C \subset \Lambda$, by taking the union of the elements of C, we get a new submodule of Rx, and since each term in C does not contain x, the union does not contain x. Thus the union is in Λ, so every chain in Λ has an upper bound in Λ.

Thus by Zorn's Lemma, there exists a maximal element of Λ, which we shall call B. Since Rx is semisimple, $Rx = B \oplus B'$.

Suppose for the sake of contradiction that B' is not simple. Then there exists $L \subsetneq B'$ such that $L \neq 0$. Note $x \notin B + L$, or else $B + L = Rx$. Let $b' \in B'$. Then $b' = b + l$, for some $b \in B$, $l \in L$. Then $b = b' - l \in B' \cap B$. Thus $b' = l$, so $B' = L$. Thus $B + L \in \Lambda$, so $B \subsetneq B + L$, since $L \neq 0$. This contradicts the maximality of B, so this is a contradiction.

(Alternatively: If B' is not simple, it is still semisimple, so $B' = L \oplus L'$. Thus $R = B \oplus (L \oplus L') = (B \oplus L) \oplus L'$. Then $B \oplus L$ is strictly larger, contradicting maximality of B.)

Thus $B' \subset Rx \subset M$ is simple.

□

Theorem 37. Let M be an R-module. The following are equivalent:

1. M is semisimple.
2. M is the sum of a simple submodule.
3. M is the direct sum of simple submodules.

(Proof is long, and will be done on Wednesday.)

Definition 40. A ring R is called *left semisimple* if R is semisimple as a left R-module.

Similarly, it is called *right semisimple* if R is semisimple as a right R-module.

Remark 34. Much later on, we will see that a ring is left semisimple if and only if it is right semisimple. In this case, we just call the ring semisimple.

Claim 2. A ring R is left semisimple if and only if it is the (direct, or not direct) sum of finitely many simple left ideals.

There is an analogous statement for right semisimple.

Proof. ($\Leftarrow$) If R is the sum or direct sum of finitely many simple left modules, then by the theorem, R is semisimple.

($\Rightarrow$) By the theorem, $R = \sum_{\lambda \in J} I_\lambda$ where I_λ are simple left ideals. Write $1 = a_{\lambda_1} + ... + a_{\lambda_k}$ for $\lambda_1, ..., \lambda_k \in J$, $a_{\lambda_j} \in I_{\lambda_j}$. Since $R = R \cdot 1$, then $R = Ra_{\lambda_1} + ... + Ra_{\lambda_k} \subset I_{\lambda_1} + ... + I_{\lambda_k} \subset R$.

Thus $R = I_{\lambda_1} + ... + I_{\lambda_k}$. $\square$

Exercise 9. Generalize the previous claim to finitely generated modules.

Show that any division ring is semisimple.

Let D be a division ring, and let $R = M_n(D)$. For $k = 1, ..., n$, let I_k denote the set of matrices which are zero except in the k-th column. Then each $I_k \cong D^n$, which is a simple left R-module. Also, $R = I_1 \oplus ... \oplus I_n$, so R is left semisimple.

13.2 Day 26 - October 28

Recall the following theorem from last class. We will prove it now:

Theorem 38. Let M be an R-module. The following are equivalent:

1. M is semisimple.
2. M is the direct sum of a simple submodule.
3. M is the direct sum of simple submodules.

Proof. If $M = 0$, these are all true. Suppose for the rest of the proof that M is nonzero.

($1 \Rightarrow 2$) Suppose M is semisimple. Let $T = \{E | E \subset M, E \text{ is simple}\}$. Since $M \neq 0$, then by a theorem from the previous class, M contains a simple submodule. Thus $T \neq \emptyset$.

Let $\Lambda = \{J \subset T | \sum_{E \in J} E = \oplus_{E \in J}\}$. Certainly, for each $t \in T$, $\{t\} \in \Lambda$, so $\Lambda \neq 0$. Note that the union of a chain is still in Λ for the following reason: the union would fail to be a direct sum if some element could be written two different ways. But this would only involve finitely many elements, so some element of the chain would not be in Λ, a contradiction.

Thus we can apply Zorn's Lemma. Let J be a maximal element of Λ. Then $\sum_{E \in J} E = \bigoplus_{E \in J} E$. Let $N = \sum_{E \in J} E$.We wish to show that $M = N$. Certainly, $N \subset M$, so since M is semisimple, $M = N \oplus N'$ for some submodule N' of M. Since N' is a submodule of a semisimple module, it is semisimple.

Therefore, if N' is nonzero it contains a simple submodule E'. Note that since $E' \cap N = (0)$, then $E' \notin J$. But $J \cup \{E'\} \in \Lambda$ for the same reason. This contradicts the maximality of of J.

Thus $N' = 0$, so $M = N$. $\square$

($2 \Rightarrow 3$) Suppose M is the direct sum of simple submodules. Certainly, every direct sum is a sum, so M is the sum of simple submodules. $\square$

(3 $\Rightarrow$ 1) Suppose M is the sum of simple submodules. We have $M = \sum_{E \in T} E$ for some collection T of simple submodules.

Let A be a submodule of M. We wish to find a submodule A' such that $M = A \oplus A'$.

Let $\Lambda = \{J \subset T | (\sum_{E \in J} E) \cap A = 0\}$. Note that $\emptyset \in \Lambda$, so $\Lambda \neq \emptyset$. Also, the union of chains in Λ are in Λ for the following reason: a union would fail to be in Λ if some nonzero finite sum of elements were in A. Then this finite sum would be in some element of the chain, a contradiction.

Thus we can apply Zorn's Lemma. Let J be maximal in Λ, and let $A' = \sum_{E \in J} E$. Certainly, $A' \cap A = (0)$. Thus the sum $A + A'$ is direct. Let $N = A + A'$. We wish to show that $N = M$.

If $N \neq M$, then there exists a simple submodule E' of M such that $E' \not\subset N$. Since E' is simple, then $E' \cap N = (0)$, so $E' + N$ is direct. Suppose $a = e + e'$ for some $a \in A$, $e \in N$, and $e' \in E'$. Then $e' = a - e \in N \cap E' = (0)$. Thus $e' = 0$, so $a = e \in A \cap A' = (0)$, so $a = e = 0$. Thus $J \cup \{E'\} \in \Lambda$. since $E' \notin J$, then this contradicts the maximality of J. Thus $N = M$, so $M = A \oplus A'$. Thus M is semisimple, as desired. $\square$

14 Filtrations and Length of Modules

Let's move on to a new topic!

Definition 41. Let M be an R-module. A *series* for M is a finite chain (also known as a filtration) of submodules of M such that $0 = M_n \subset M_{n-1} \subset ... \subset M_0 = M$.

The *factor modules* of this series are $M_i/M_{i+1} | i = 0, ..., n-1\}$ and we count them with multiplicity.

The *length* of a series is the number of non-zero factor modules (which is equal to the number of strict inequalities).

A *refinement* of a series for M is another series for M which "contains" the original series as a subseries. That is, if the original series is $0 = M_n \subset .... \subset M_0 = M$, and $0 = M'_k \subset ... \subset M'_0 = M$ is another series, then the new series is a refinement of the original one if for each i there exists a j such that $M_i = M'_j$.

A *proper refinement* is a refinement which strictly increases the length.

We say two series for a module are *equivalent* if there exists a bijection between the two sets of nonzero factor modules, such that the corresponding factor modules are isomorphic.

Example 43. Let $R = \mathbb{Z}$ and let $M = \mathbb{Z}$. Then $(0) \subset 18\mathbb{Z} \subset 18\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$. Then the factor modules are $18\mathbb{Z}, 0, \mathbb{Z}_6, \mathbb{Z}_3$.

A refinement of this series might be $(0) \subset 72\mathbb{Z} \subset 18\mathbb{Z} \subset 18\mathbb{Z} \subset 9\mathbb{Z} \subset 3\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$. Then the factor modules are $72\mathbb{Z}, \mathbb{Z}_4, 0, \mathbb{Z}_2, \mathbb{Z}_3, 0, \mathbb{Z}_3$.

Another series might be $0 \subset 72\mathbb{Z} \subset 24\mathbb{Z} \subset 12\mathbb{Z} \subset 4\mathbb{Z} \subset \mathbb{Z}$. Then the factor modules are $72\mathbb{Z}, \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$. Thus the third series is equivalent to the second. Note that the third series is not a refinement of the first.

Theorem 39. (Schreier Refinement Theorem) Let M be an R-module. Then any two series for M have refinements which are equivalent.

We will prove this next class. For now, we prove a lemma.

Lemma 17 (Zassenhaus Lemma). Let M be an R-module, and let $A \subset A'$ and $B \subset B'$ be R-submodules of M. Then $\dfrac{A + (A' \cap B')}{A + (A' \cap B)} \cong \dfrac{B + (A' \cap B')}{B + (A \cap B')}$.

Proof. We will first show both modules are isomorphic to $\dfrac{A' \cap B'}{A' \cap B + A \cap B'}$. By symmetry, it suffices to show this is true for just one of the modules. That is, it suffices to show that $\dfrac{A + (A' \cap B')}{A + (A' \cap B)} \cong \dfrac{A' \cap B'}{A' \cap B + A \cap B'}$.

Let $\dfrac{A' \cap B'}{A' \cap B + A \cap B'} = L$

Define $\phi : A+(A'\cap B') \to L$ by $a+u \mapsto \overline{u}$. We need to show this is well-defined. Suppose $a_1+u_1 = a_2+u_2$. Then $u_1 - u_2 = a_2 - a_1 \in A \cap A' \cap B' \subset A \cap B'$. Thus $\overline{u}_1 = \overline{u}_2$, so the function is well-defined.

We then need to check two things: first, that this function is surjective. This is straightforward.

Also, we need to check that $\ker \phi = A + (A' \cap B)$. This is left as an exercise. □

14.1 Day 27 - October 30

Homework will be due next Monday (November 9) instead of Friday!

Recall the following lemma from last class:

Lemma 18. (Zassenhaus Lemma) Let M be an R-module, and let $A \subset A'$ and $B \subset B'$ be R-submodules of M. Then $\dfrac{A+(A'\cap B')}{A+(A'\cap B)} \cong \dfrac{B+(A'\cap B')}{B+(A\cap B')}$.

We will use it to prove this important theorem:

Theorem 40 (Schreier Refinement Theorem). Let M be an R-module. Then any two series for M have refinements which are equivalent.

Proof. Let $0 = M_n \subset ... \subset M_0 = M$ and $0 = N_t \subset ... \subset N_0 = M$ be two series for M.

Fix $i \in \{0, 1, ..., n\}$. Let $M_{i,j} = M_{i+1} + M_i \cap N_j$ for $j = 0, ..., t$.

(What does this look like? Well, $M_{i,0} = M_{i+1} + M_i \cap N_0 = M_{i+1} + M_i = M_i$. Also, $M_{i,t} = M_{i+1}$. Also, $M_{i,j} \subset M_{i,j+1}$ so we have "series" such that $M_{i+1} = M_{i,t} \subset M_{i,t-1} \subset ... \subset M_{i,0} = M_i$.)

Then we get a refinement of the first series by taking $0 = M_{n,t} \subset M_{n,t-1} \subset ... \subset M_{0,1} \subset M_{0,0} = M$.

Similarly, we define $N_{i,j} = N_{i+1} + M_j \cap N_i$ for $j \in \{0, ..., n\}$. Thus we get a refinement of the second series by taking $0 = N_{t,n} \subset ...N_{0,1} \subset N_{0,0} = M$.

We now wish to show that these series are equivalent.

First we will show that that $N_{i,j}/N_{i,j+1} \cong M_{j,i}/M_{j,i+1}$. This follows from the Zassenhaus Lemma by setting $N_{i+1} = A$, $N_i = A'$, $M_j = B$, and $M_{j+1} = B'$.

There are also a few other links in the refined series, where something like $M_{i+1,t} \subset M_{i,t}$ but this is in fact equivalence, since these both equal M_{i+1}, so the factor modules are 0, so we don't need to pay attention to them.

Thus the two series are equivalent, as desired. □

Definition 42. Let M be an R module. A *composition series* for M is a series in which all the nonzero factor modules are simple modules.

Remark 35. A series is a composition series if and only if it has no proper refinement. (Proper, in this case, means that we have inserted a strictly contained module).

A series is a composition series if and only if the series is equivalent to all of its refinements.

Proposition 20. Let M be an R-module. Then any two composition series of M are equivalent.

Proof. Take any two composition series of M. By the Schreier Refinement Theorem, these can be refined to equivalent series. But they are composition series, so they are equivalent to their own refinements. Thus by transitivity they are equivalent.

□

Definition 43. Let M be an R-module. If M has a composition series, the *length* of M, denoted $\lambda_R(M)$, is the length of any composition series for M. (Note that this is well defined by the previous proposition.) If M does not have a composition series, then we define $\lambda_R(M) = \infty$.

If $\lambda_R(M) < \infty$, then we say M is a *finite length module*.

Example 44. Let $R = \mathbb{Z}$, and let $M = \mathbb{Z}_{24}$. Then recall that simple $\mathbb{Z}$-modules are simple abelian groups, i.e. cyclic groups of order p. Then a composition series for $\mathbb{Z}_24$ could be

$$0 \subsetneq \frac{(12)}{(24)} \subsetneq \frac{(6)}{(24)} \subsetneq \frac{(2)}{(24)} \subsetneq \frac{\mathbb{Z}}{(24)}$$

Then the factor groups are $\mathbb{Z}_2$, $\mathbb{Z}_2$, $\mathbb{Z}_2$, and $\mathbb{Z}_3$. Thus $\lambda_R(M) = 4$.

Example 45. Let D be a division ring. Then every D-module M has a basis β, so $M \cong \bigoplus_{\alpha \in \beta} D$.

Then D is a simple (left) D-module. Suppose $M = D^n$ (i.e. $dim_D(M) = n$, i.e. $|\beta| = n$).

Then let $M_i = D \oplus D \oplus ... \oplus D \oplus 0 \oplus 0 \oplus ... \oplus 0 \subset D^n$, where there are $n - i$ copes of D, and i copies of 0. Then $0 = M_n \subsetneq ... \subsetneq M_0 = M$, and $M_i/M_{i+1} \cong D$ (which is simple as a left D-module). Thus $\lambda_D(M) = n = dim_D(M)$.

Remark 36. We use ${}_RM$ to denote M thought of a left R-module, and we use M_R to denote M thought of as a right R-module.

Example 46. Let D be a division ring, and let $R = M_n(D)$. For $k =\in \{1, ..., n\}$, we let I_k be the subset with zero entries off of the kth column. Then recall that each I_k is a simple left ideal of R, and $R = I_1 \oplus ... \oplus I_n$. By doing the same thing as before, we can see that $\lambda_R({}_RR) = n$.

By symmetry (exchanging rows with columns), $\lambda_R(R_R) = n$ as well. And since it is a D-vector space, $\lambda_D({}_DR) = n^2$.

Proposition 21. Let M be an R module. Then $\lambda_R(M) < \infty$ if and only if M is both Noetherian and Artinian.

Proof. ($\Rightarrow$) Suppose $\lambda_R(M) < \infty$. Then there is a composition series of length $\lambda_R(M) = r$. Consider any finite chain of submodules of M: $0 = M_n \subset ... \subset M_0 = M$.

By the Schreier Refinement Theorem, we can refine this chain of submodules into a composition series. The refined chain will have r proper containments.

Note that a refinement can introduce new proper containments, but can't destroy them. Thus every chain of submodules has at most r proper containments. That is, any ascending and descending chain of submodules of M stabilizes after at most r proper containments. □

($\Leftarrow$) Suppose M is both Noetherian and Artinian. If $M = 0$, then we are done. If $M \neq 0$, then because M is Artinian, we can choose a minimal nonzero submodule of M, which we shall denote N_1. Note that N_1 is simple, since if it had a proper submodule, it would not be minimal.

Now we repeat this process: if $N_1 \neq M$, choose a submodule that is minimal among all submodules properly containing N_1, which we shall denote N_2. Then N_2/N_1 is simple as before.

Thus by repitition, we get $0 = N_0 \subsetneq N_1 \subsetneq N_2 \subsetneq ...$

Since M is Noetherian, this chain cannot go on forever. The only way it can stop is if some $N_k = M$. Thus we have a composition series $0 = N_0 \subset N_1 \subset ... \subset N_k = M$. Thus M has a composition series. □

14.2 Day 28 - November 2

Recall that homework will be due next Monday (November 9) instead of Friday!

Proposition 22. Claim: Let R be a ring, and let $0 \to A \to B \to C \to 0$ be a short exact sequence of R-modules. Then, $\lambda_R(B) = \lambda_R(A) + \lambda_R(C)$.

Proof. Without loss of generality, we can assume A is a submodule of B and $C = B/A$.

First we consider the case where there are infinite lengths. Recall that a module has finite length if and only if it is Noetherian and Artinian. But also, we have proven that a quotient B is Noetherian (respectively, Artinian) if and only if both its submodule A and its "supermodule" C are Noetherian (respectively, Artinian). Thus $\lambda_R(B) = \infty$ if and only $\lambda_R(A) = \infty$ or $\lambda_R(C) = \infty$. Thus if one of $\lambda_R(A)$,$\lambda_R(B)$, or $\lambda_R(C)$ is infinite, then the claim holds.

Suppose instead that all the lengths are finite. Let $n = \lambda_R(A)$ and let $m = \lambda_R(C)$. Then there exists composition series $0 = A_n \subsetneq ... \subsetneq A_0 = A$ and $0 = B_m/A \subsetneq ... \subsetneq B_0/A = B/A = C$ for A and C, respectively. Since these are composition series, A_j/A_{j+1} and B_i/B_{i+1} is simple for all appropriate j and i.

Then $0 = A_n \subsetneq ... \subsetneq A_0 = B_m \subsetneq ... \subsetneq B_0 = B$ is a series for B. Note that $B_i/B_{i+1} \cong \frac{B_i/A}{B_{i+1}/A}$ is simple for all i. Thus this series is in fact a composition series. Thus $\lambda_R(B) = m + n = \lambda_R(A) + \lambda_R(C)$, as desired.

Thus in all cases, $\lambda_R(B) = \lambda_R(A) + \lambda_R(C)$.

□

Remark 37. Recall that if A_1 and A_2 are modules, then $0 \to A_1 \to A_1 \oplus A_2 \to A_2 \to 0$ is a short exact sequence. Thus $\lambda(A_1 \oplus A_2) = \lambda(A_1) + \lambda(A_2)$.

By induction, we have that $\lambda(\bigoplus_{i=1}^{n} A_i) = \sum_{i=1}^{n} \lambda(A_i)$.

Example 47. Let K be a field, let $R = K[x]$, and let $M = R/(x^2)$. We wish to show that $0 \subsetneq R\overline{x} \subsetneq M$ is a composition series for M. Note that $M/R\overline{x} = \frac{R/(x^2)}{(x)/(x^2)} \cong R/(x) \cong K$, which is simple.

We can also define $f : R \to R\overline{x}$ by $r \to r\overline{x}$, which is a module homomorphism. Note that $r\overline{x} = \overline{0}$ if and only if $\overline{rx} = \overline{0}$ which is the case if and only if $rx \in (x^2)$ which is the case if and only if $r \in (x)$. Thus $\ker f = (x)$, so $R\overline{x}/(0) \cong R\overline{x} \cong R/(x)$ which is simple. Thus $\lambda_R(M) = 2$.

Also, R is a K-algebra, and $\lambda_K(M) = \dim_K(M) = 2$, since $\{\overline{1}, \overline{x}\}$ is a K-basis for M.

Example 48. Let $R = \mathbb{R}[x]$. Let $M = R/(x^2 + 1)$. Note that $x^2 + 1$ is irreducible as a polynomial, so $(x^2 + 1)$ is maximal as an ideal. Thus this quotient is a simple R-module. Thus $\lambda_R(M) = 1$, but $\lambda_{\mathbb{R}}(M) = \dim_{\mathbb{R}}(M) = 2$.

In general, length does not have to equal vector space dimension.

15 Classification of Semisimple Modules

Proposition 23. Let R be a ring. The following are equivalent

1. R is semisimple.
2. ${}_RR$ is a direct sum of finitely many simple left ideals.
3. ${}_RR$ is a sum of finitely many simple left ideals.

Proof. $(1 \Rightarrow 2)$ Suppose R is semisimple. We know from the previous characterization of semisimple modules that R is the direct sum of simple submodules, i.e. ideals. That $R = \bigoplus_{\alpha \in \Lambda} I_\alpha$ for some simple left ideals I_α.

Then we can write the multiplicative identity as $1 = i_{\alpha_1} + ... + i_{\alpha_n}$ where each $i_{\alpha_j} \in I_{\alpha_j}$. Then for all $r \in R$, $r = ri_{\alpha_1} + ... + ri_{\alpha_n} \in I_{\alpha_1} + ... + I_{\alpha_n}$. Thus $R = I_{\alpha_1} + ... + I_{\alpha_n}$. But R was the direct sum of the I_αs, so $R = \bigoplus_{i=1}^{n} I_{\alpha_n}$. Thus R is the direct sum of finitely many simple left ideals, as desired. □

$(2 \to 3)$ Suppose ${}_RR$ is the direct sum of finitely many simple left ideals. Then since every direct sum is a sum, ${}_RR$ is the sum of finitely many simple left ideals. □

$(3 \to 1)$ Suppose ${}_RR$ is the sum of finitely many simple left ideals. Then by the previous characterization of semisimple modules, we know that ${}_RR$ is semisimple. That is, R is semisimple.

□

Remark 38. If R is left semisimple, then ${}_RR = I_1 \oplus ... \oplus I_n$, where each I_j is simple. Thus for each j, $\lambda_R(I_j) = 1$, so $\lambda_R(R) = \sum_{j=1}^{n} \lambda_R(I_j) = n$. Thus R is both left Noetherian and left Artinian.

Exercise 10. Generalize the previous proposition to any finitely generated module. Use this to show that any finitely generated semisimple module has finite length.

Proposition 24. Suppose R is left semisimple. Then every (left) R-module is semisimple.

Proof. Let M be an R-module. Let $\{x_\alpha\}\alpha \in \Lambda$ be a generating set. Then $M = \sum_{\alpha \in \Lambda} Rx_\alpha$. Let $F = \bigoplus_{\alpha \in \Lambda} R$, which is semisimple, since R is semisimple.

Define $\phi : F \to M$ by $\sum r_\alpha e_\alpha \mapsto \sum r_\alpha x_\alpha$. Note that ϕ is surjective homomorphism. Thus $M \cong F/\ker\phi$. That is, M is the quotient of a semisimple module. By a previous theorem, the quotient of semisimple modules is semisimple, so M is semisimple. □

Remark 39. (Prelude to the Artin-Wedderburn Theorem)
Recall that if D is a division ring and n is a positive integer, then $M_n(D)$ is left (and right) semisimple.
Recall also that $R_1, ..., R_l$ are left semisimple, then so is $R_1 \times .. \times R_l$.
From these two facts, it follows that $M_{n_1}(D_1) \times ... \times M_{n_l}(D_l)$ is semisimple for division rings $D_1, ...D_l$.

Next time, we will prove the Artin-Wedderburn Theorem!

15.1 Day 29 - November 4

Let R be a ring, let I be a left ideal, and let M be a left R-module. Then $IM = \{\sum_{finite} a_i u_i | a_i \in I, u_i \in M\}$.
Then IM is a left submodule of M.
In this case $IR = I$ and $RI = I$. Also, for $x \in M$, $IRx = Ix = \{ix | i \in I\}$, and this is a submodule of M.

Lemma 19. Let R be a ring, and I be a simple left ideal and M a simple module. If $I \ncong M$ then, $IM = 0$.

Proof. We prove the contrapositive. Suppose $IM \neq 0$. Then there exists some $i \in I$ and $u \in M$ such that $iu \neq 0$.
Define $\phi : I \to M$ by $a \mapsto au$. Then we can check that ϕ is an R-module homomorphism. Note that $im\phi \neq 0$ since $\phi(i) = iu \neq 0$. Also, $\phi(I)$ is a submodule of M, so since M is simple, $im\phi = M$. That is, ϕ is surjecive.
Also, $\ker\phi \neq I$ since $\phi(i) \neq 0$. But $\ker\phi$ is a subideal of I, and since I is simple then $\ker\phi = 0$. Thus ϕ is injective, so ϕ is an R-module isomorphism. □

Proposition 25. Let R be a left semisimple ring. Then

1. Every simple R module is isomorphic to a simple left ideal.
2. There are only finitely many (up to isomorphism) simple R-modules.

Proof. (Proof of 1) Let M be a simple R-module. Choose $u \in M \setminus \{0\}$. Define $\phi : R \to M$ by $r \mapsto ru$. Note that $Ru \neq 0$, and Ru is a submodule of M, so since M is simple, then $Ru = M$. Thus ϕ is surjective. As R is left semisimple, $R = \ker\phi \oplus I$ for some ideal I. Then for $r \in R$, there exist unique $a \in \ker\phi$ and $b \in I$ such that $r = a + b$. But $\phi(r) = \phi(a+b) = (a+b)u = bu$. Then $\phi\Big|_I : I \to M$ is an isomorphism. Thus $M \cong I$.
Since M is isomorphic to I, and M is simple, then I is simple, as desired. □
(Proof of 2) Since R is semisimple, we can write it as the finite sum of simple left ideals. That is, $R = I_1 + ... + I_k$ for some simple left ideals I_js. Let J be a simple left ideal of R. It suffices to show that J is isomorphic to some I_j.
Suppose J were not isomorphic to any I_j. Then by the lemma, $JI_j = 0$ for all j. But $J = JR = J(I_1 + ...I_k) = JI_1 + ...JI_k = 0$. This is a contradiction, so J must be isomorphic to some I_j. □

Theorem 41. Let R be a left semisimple ring. Let $I_1, ..., I_k$ be representatives of the distinct isomorphism classes of simple left ideals (that is, every simple left ideal of R is isomorphic to exactly one I_j). For each i, let $R_i = \sum_{\substack{L \text{ left ideal} \\ L \cong I_i}} L$. Then

1. For all i, R_i is a ring with identity.
2. For all i, R_i is a left semisimple with a unique (up to isomorphism) simple left ideal.
3. For all i, R_i is simple.

4. Finally, $R \cong R_1 \times ... \times R_k$ (as rings).

Proof. (Proof of 1) As R is semisimple, $R = \sum_{L \text{ simple left ideal}} L = R_1 + ... + R_k$.

Each R_i is a left ideal of R, so R_i is closed under $+$ and $\cdot$. We can write $1 = e_1 + ... + e_k$ for some $e_i \in R_i$. We wish to show that e_i is the multiplicative identity for R_i.

First observe that for $i \neq j$, $R_iR_j = (\sum_{L_\alpha \cong I_i} L_\alpha)(\sum_{L_\beta \cong I_j} L_\beta) = \sum_{\alpha,\beta} L_\alpha L_\beta = \sum 0 = 0$ (since non-isomorphic simple ideals multiply to 0).

Let $x \in R$. We can write $x = x_1 + ... + x_k$ for some $x_i \in R_i$. Then $x_i = x_i \times 1 = x_i(e_1 + ... + e_k) = x_ie_i = (x_i + ...x_k)e_i = xe_i$. Thus the x_is are uniquely determined for all i. Thus $R = R_1 \oplus ... \oplus R_k$ (as left R-modules).

Observe that $x_i = x_i \cdot 1 = x_i(e_1 + ... + e_k) = x_ie_i$, and similarly $x_i = 1 \cdot x_i = (e_1 + ... + e_k)x_i = e_ix_i$. Thus e_i is a multiplicative identity for R_i. Thus each R_i is a ring with identity. □

(Proof of 4) Define $\psi : R \to R_1 \times ... \times R_k$ by $x \mapsto (xe_1, ...xe_k) = x(e_1, ..., e_k)$. Certainly, ψ is R-linear. Note also that $\psi(xy) = (xye_1, ..., xye_k) = x(e_1, ..., e_k)y(e_1, ..., e_k) = \psi(x)\psi(y)$. Thus ψ is a ring homomorphism.

Also, suppose $\psi(x) = 0$. Then $xe_1 = 0$ for all i, and $x = x(e_1 + ... + e_k) = 0$. Thus ψ is injective.

Finally, suppose $(y_1, ..., y_k \in R_1 \times ... \times R_k$. Then let $x = y_1 + ... + y_k$. Then $\psi(x) = (xe_1, ..., xe_k) = (y_1, ..., y_k)$, so ψ is surjective. Thus ψ is a ring isomorphism. Thus $R \cong R_1 \times ... \times R_k$.

(Proof of 2) Fix an i. Then R_i is a sum of left ideals, so R_i is semisimple. Then by something Zorn-ish, it contains a simple left ideal.

Suppose J is a simple left ideal of R_i. We wish to show that $J \cong I_i$.

Let K be a left ideal of R_i. Note that $RK = (R_1 + ... + R_k)K = R_iK \subset J$. Hence K is a left ideal of R. Also, if K is a left ideal of R contained in R_i, then certainly K is a left ideal of R_i. Therefore the left ideals of R_i are precisely the left ideals of R contained in R_i.

Thus since J is a simple left ideal of R_i, then J is a simple left ideal of R_i. Therefore $J \cong I_j$ for some j. But $J = R_iJ \cong R_iI_j = 0$ for all $i \neq j$, so $i = j$ and $J \cong I_i$. Thus there is a unique simple left ideal of R_i, up to isomorphism. □

(Proof of 3) Let $J \neq 0$ be a two-sided ideal of R_i. Then J contains some simple left ideal of R_i, which we can denote L. Since R_i is semisimple, $R_i = L \oplus L'$ where L' is another left ideal of R_i. Then $1 = e + e'$, where $e \in L$ and $e' \in L'$. Thus $e = e^2e + ee'$, so $ee' = e - e^2 \in L' \cap L = (0)$. Thus $e = e^2$.

Hence $e^2 = e \in Le \neq 0$ (as $e \neq 0$). Since L is simple $Le = L$. Let K be a simple left ideal of R_i. Thus $K \cong I_i \cong L$. Let $\psi : L \to K$ be an isomorphism. Then $K = \psi(L) = \psi(Le) = L\psi(e) \subset J\psi(e) \subset J$ (since J is a right ideal). Thus $J = R_i = \sum_{K \cong I_i} K$.

□

Next time, we will prove the Artin-Wedderburn Theorem!

15.2 Day 30 - November 6

Next exam will be take-home.

Recall from last class the following powerful theorem:

Theorem 42. Let R be a left semisimple ring. Let $I_1, ..., I_k$ be representatives of the distinct isomorphism classes of simple left ideals (that is, every simple left ideal of R is isomorphic to exactly one I_j). For each i, let $R_i = \sum_{\substack{L \text{ left ideal} \\ L \cong I_i}} L$. Then

1. For all i, R_i is a ring with identity.

2. For all i, R_i is a left semisimple with a unique (up to isomorphism) simple left ideal.

3. For all i, R_i is simple.

4. Finally, $R \cong R_1 \times ... \times R_k$ (as rings).

This leads to the following corollary:

Corollary 13. Let R be a left semisimple ring. Then R is simple if and only if R has a unique (up to isomorphism) simple left ideal.

Proof. We write $R = R_1 \times \cdots \times R_k$ by the previous theorem.

Suppose R has a unique (up to isomorphism) simple left ideal. Then $k = 1$, so $R = R_1$, and by the previous theorem, R_1 is simple. Thus R is simple.

Suppose instead that R is simple. Recall that each R_i can be interpreted as residing inside R, and that they are ideals in R (since $R_i R_j = 0$ for $i \neq j$). In particular, R_1 is a two-sided ideal in R. Since R is simple, and $R_1 \neq 0$, then $R = R_1$. Thus R has a unique simple left ideal. $\square$

Definition 44. Let R be a ring, and let $R^o = \{r^o | r \in R\}$. We define $+$ on R^o by $r^o + s^o = (r+s)^o$, We define $\cdot$ on R^o by $r^o s^o = (sr)^o$. We say that R^o with these operations is the *opposite ring* of R.

Remark 40. Observe that R is commutative if and only if the map $r \mapsto r^o$ is a ring isomorphism of R and R^o.

Note that I is a left ideal in R if and only if $I^o = \{i^o | i \in I\}$ is a right ideal in R^o. Because of this, R is left Noetherian (respectively, Artinian, semisimple, etc) if and only if R^o is right Noetherian (respectively, Artinian, semisimple, etc).

Finally, $(R^o)^o \cong R$.

Definition 45. Let M be an R-module. Define $\operatorname{End}_R(M) = \{\phi : M \to M | \ \phi \text{ is a } R\text{−module homomorphism}\}$. Then $\operatorname{End}_R M$ is a ring under $+$ and $\cdot$ (which in this case is composition). It has a multiplicative identity element (namely, the identity function). We can also verify distributivity (but I won't).

Proposition 26. Let R be a ring. Then $\operatorname{End}_R(R)$ (where we think of R as a left R-module) is isomorphic to R^o.

Proof. Define $f : \operatorname{End}_R(R) \to R^o$ by $\phi \mapsto \phi(1)^o$. Let us now check that this is an R-module homomorphism. It is easy to verify that $f(\phi + \psi) = f(\phi) + f(\psi)$. Also,

$$\begin{aligned} f(\psi\phi) &= (\psi\phi)(1)^o \\ &= (\psi(\phi(1)))^o \\ &= (\psi(\phi(1) \cdot 1))^o \\ &= (\phi(1)\psi(1))^o \\ &= \phi(1)^o \psi(1)^o \\ &= f(\psi) f(\phi) \end{aligned}$$

Note that the fourth equality is because ψ is R-linear. Thus f is an R-module homomorphism. It is easy to check that f is injective. For surjectivity, we can see that for $r^o \in R^o$, we can define $g : R \to R$ by $x \mapsto xr$. Then $g \in \operatorname{End}_R(R)$, and $f(g) = r^o$. Thus f is surjective, so it is bijective. Thus f is isomorphic to R^o. $\square$

Exercise 11. Let M be an R-module. Then M is simple if and only if $\operatorname{End}_R(M)$ is a division ring.

Remark 41. Let M be an R-module, and let $M^n = M \oplus \cdots \oplus M$ (where we have n copies).

For $i = 1, ..., n$, let $f_i : M \to M^n$ by $u \mapsto (0, \ldots, u, \ldots, 0)$ where the u is in the ith component. Also define $\pi_i : M^n \mapsto M$ by $(u_1, ..., u_n) \mapsto u_i$. Note that $\pi_i f_i = 1_M$ for all i, and $\pi_j f_i = 0$ for all $i \neq 0$.

Let $\psi \in \operatorname{End}_R(M^n)$. Define $\psi_{i,j} = \pi_j \psi f_i$. Note that this is a function $M \to M^n \to M^n \to M$. Thus $\psi_{i,j} \in \operatorname{End}_R(M)$ for all i, j. Define $[\psi] := [\psi_{i,j}] \in M_n(\operatorname{End}_R(M))$.

Claim 3. Let $f : \mathrm{End}_R(M^n) \to M_n(\mathrm{End}_R(M))$ by $\psi \mapsto [\psi]$. Then f is a ring isomorphism.

Proof. This is left as an exercise for the reader. $\square$

Corollary 14. If R is a ring, then $\mathrm{End}_R(R^n) \cong M_n(\mathrm{End}_R(R)) \cong M_n(R^o)$.

Remark 42. Let M be an R module. We use R' or $R'(M)$ to denote $\mathrm{End}_R(M)$. Then M is an R'-module, by the action $\phi u = \phi(u)$ for $\phi \in R'$ and $u \in M$ (one can verify that this is indeed an R'-module).

Also, $R'' = R''(M) = \mathrm{End}'_R(M)$. For $a \in R$, let $r_a^M : M \to M$ by $u \mapsto ua$. Then $r_a^M \in R'(M)$. Let $l_a^M : M \to M$ by $u \mapsto au$. Then $l_a^M \notin R'(M)$ in general.

However, we can show that $l_a^M \in R''(M)$. Let us do so. Note that $l_a^M(u+v) = a(u+v) = au+av = l_a(u)+l_a(v)$. Thus l_a^M is additive. Also, for $\phi \in R'$, we can see that $l_a^M(\phi u) = l_a^M(\phi(u)) = a\phi(u) = \phi(au) = \phi \cdot l_a^M(u)$.

Let M be an R-module. Then there is a ring homomorphism $\lambda : R \to R''(M)$ by $a \mapsto l_a^M$. One can again verify additivity, and it is boring. Also, $(l_a^M l_b^M)(u) = l_a(bu) = abu = l_{ab}^M u$.

Next time, we will prove the following theorem due to Rieffel:

Theorem 43. Let R be a simple ring and let I be a left ideal. Then $\lambda : R \to R''(I)$ is an isomorphism.

Note that we still have not proven the Artin-Wedderburn Theorem.

Theorem 44 (Artin-Wedderburn Theorem). Let R be a left semisimple ring. Then there exists unique positive integers $l, n_1, ..., n_l$ and unique division rings $D_1, \ldots, D_l$ such that $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_l}(D_l)$.

15.3 Day 31 - November 9

Definition 46. Let R be a ring, and let S, T be nonempty subsets of R. Define $ST = \{ \sum_{finite} s_i t_i | s_i \in S, t_i \in T\}$. This is the product of S and T.

Remark 43. We have two elementary properties of these products: first, that $(ST)U = S(TU)$, and that if $f : R \to R'$ is a ring homomorphism, then $f(ST) = f(S)f(T)$. These are easy to prove, but we will skip that.

Last time, we stated the following theorem:

Theorem 45 (Rieffel's Theorem). Let R be a simple ring and let I be a nonzero left ideal of R. Then $\lambda : R \to R''(I)$ given by $a \mapsto l_1$ is an isomorphism.

Let's prove it now!

Proof. Since λ is R-linear (on both sides), then $\ker \lambda$ is a two-sided ideal of R. Then $\lambda(1) = l_1 \neq 0$ since $I \neq 0$. Thus $\ker \lambda \neq R$, so since R is simple, then $\ker \lambda = 0$. That is, λ is injective.

Note that IR is a two-sided ideal of R. Therefore $IR = R$.

We now wish to show that $\lambda(I)$ is a left ideal of R''. Certainly, it is an additive subgroup. It then suffices to show that if $f \in R''$ and $l_a \in \lambda(I)$, then $fl_a \in \lambda(I)$. Fix some $x \in I$, let r_x denote the operation of right multiplying by x. Then $r_x \in R' = \mathrm{End}_R(I)$. Therefore

$$\begin{aligned} (fl_a)(x) &= f(l_a(x)) \\ &= f(ax) \\ &= f(r_x(a)) \\ &= r_x(f(a)) \\ &= f(a)x \\ &= l_{f(a)}(x) \end{aligned}$$

Therefore, $\lambda(I)$ is a left ideal of R'', so $R''\lambda(I) = \lambda(I)$. Then we have that

$$\begin{aligned} R'' &= R''\lambda(R) \\ &= R''\lambda(IR) \\ &= (R''\lambda(I))\lambda(R) \\ &= \lambda(I)\lambda(R) \\ &= \lambda(IR) \\ &= \lambda(R) \end{aligned}$$

Therefore λ is surjective, so λ is a bijection. Thus λ is an isomorphism.

$\square$

Theorem 46. Let R be a simple ring. Then the following are equivalent:

1. R is left semisimple.
2. R is left Artinian.
3. $R \cong M_N(D)$ for some $n \geq 1$ and some division ring D.

Proof. We have already show that (3) implies (1), and that (1) implies (2).

It then suffices to show that (2) implies (3). To that end, suppose R is left Artinian. Then R contains a simple left ideal I. By Rieffel's Theorem, $R \cong R''(I) = \mathrm{End}_{R'}(I)$. Since I is simple, then $R' = \mathrm{End}_R(I) = D$ is a division ring.

Hence, $R \cong \mathrm{End}_D(I)$.

We now wish to show that I is a finite dimensional D-vector space. Suppose for the sake of contradiction that it is not. Then it would be infinite dimensional, so let $\{e_1, e_2, ...\}$ be a countably infinite linearly independent set in I. For each $n \geq 1$, let $J_n = \{f \in \mathrm{End}_R(I) | f(e_i) = 0 \text{whenever} 1 \leq i \leq n\}$. Observe that each J_n is a left ideal of $\mathrm{End}_D(I)$. Additionally, note that $J_1 \supset J_2 \supset ....$

Finally, for each n, we can construct $g_n : I \to I$ with $g_n \in \mathrm{End}_D(I)$ such that $g(e_n) \neq 0$ but $g(e_i) = 0$ for $i \neq n$ (you can do this since we are working in a D-vector space). Then $g_n \in J_{n-1} \setminus J_n$, so we have that $J_1 \supsetneq J_2 \subsetneq ....$ Therefore $\mathrm{End}_D(I)$ is not left Artinian.

But $R \cong \mathrm{End}_D(I)$ is left Artinian, so this is a contradiction. Thus $\dim_D(I) = l < \infty$. That is, $I \cong D^l$. Therefore $R \cong \mathrm{End}_D(D^l) \cong M_l(D^o)$, as desired. $\square$

Theorem 47 (Artin-Wedderburn, Part I). Let R be a ring. Then the following are equivalent:

1. R is left semisimple.
2. R is right semisimple.
3. $R \cong M_{n_1}(D_1) \times ... \times M_{n_k}(D_k)$ for some positive integers $n_1, ..., n_k$ and division rings $D_1, ..., d_k)$.

Proof. (1) $\Rightarrow$ (3) Suppose R is left semisimple. We previously proved that $R \cong R_1 \times ... \times R_k$ where each R_i is a simple left semisimple ring. Then by the previous theorem, $R_i \cong M_{n_i}(D_i)$, as desired. $\square$

(3) $\Rightarrow$ 2) Suppose R is a product of matrices of division rings. We have shown that matrices of division rings are semisimple, so their product is semisimple. $\square$

(2) $\Rightarrow$ (1). Suppose R is right semisimple. Then R^o is left semisimple, so since (1) $\Rightarrow$ (2) $\Rightarrow$ (3), then R^o is right semisimple. Then $R \cong (R^o)^o$ is left semisimple. $\square$

Remark 44. Due to this theorem, a ring is left semisimple if and only if it is right semisimple. Thus we refer to this as simply "semisimple".

If R is a semisimple ring, then $\lambda_R({}_RR) < \infty$ and $\lambda_R(R_R) < \infty$, so R is both left and right Noetherian and Artinian.

Exercise 12. Let $R \cong M_{n_1}(D_1) \times ... \times M_{n_k}(D_k)$, where each D_i is a division ring. Then $\lambda_R({}_R R) = \lambda_R(R_R) = n_1 + ... + n_k$.

Remark 45. History time! Wedderburn came before Emmy Noether (he publish the result in 1907), so he didn't know about chain conditions. He proved the theorem for the case of rings that contain a field and are finite dimensional over this field.

Artin came after Emmy Noether (he published in the 1920s) and generalized the result to rings satisfying the descending chain condition.

Note that we still have not proven the Artin-Wedderburn Theorem.

Theorem 48. (Artin-Wedderburn Theorem) Let R be a left semisimple ring. Then there exists unique positive integers $l, n_1, ..., n_l$ and unique division rings $D_1, \ldots, D_l$ such that $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_l}(D_l)$.

16 Weyl Algebra

16.1 Day 32 - November 11

Let's look at an example of a ring that is simple, but not semisimple.

Example 49 (The Weyl Algebra). Let F be a field, and let x be a variable. Then $F[x]$ is a polynomial ring. Note that an F-basis for $F[x]$ is $\{1, x, x^2, ...\}$.

Let $R = \mathrm{End}_F(F[x])$. Let $f(x) \in F[x]$, and let $\mu_f : F[x] \to F[x]$ by $g \mapsto fg$. Then $\mu_f \in R$ for all $f \in F[x]$. In fact, the map $\rho : F[x] \to R$ by $f \mapsto \mu_f$ is an injective ring homomorphism.

Identify $F[x]$ with $image(\rho)$, so we can assume $F[x] \subseteq R$.

Define also $d : F[x] \to F[x]$ by $d(x^j) = jx^{j-1}$ for all $j = 0, 1, 2, ...$ (and extending linearly to all of $F[x]$. Note that d is the derivative operator: $d(f(x)) = f'(x)$. Therefore $d \in R$.

Finally, the (first) Weyl algebra, denoted $A_1(F)$, is the subring of R generated by $F[x]$, and d.

Because we are lazy, we will write A for $A_1(F)$.

Proposition 27. In the Weyl algebra, for any $j \geq 1$, $dx^j - x^j d = jx^{j-1}$.

Proof. To check two operators are equal, we need only to check that they behave the same on all basis elements. Therefore consider x^l for some $l = 0, 1, 2, ...$

Then

$$\begin{aligned}
(dx^j - x^j d)x^l &= (dx^j)x^l - (x^j d)x^l \\
&= d(x^{j+l} - x^j(lx^{l-1}) \\
&= (j+l)x^{j+l-1} - lx^{j+l-1} \\
&= jx^{j+l-1} \\
&= (jx^{j-1})(x^l)
\end{aligned}$$

for all l. Thus $dx^j - x^j d = jx^{j-1}$. $\square$

Proposition 28. The set $B = \{x^i d^j | i, j \geq 0\}$ is an F-basis for A, if $char\ F = 0$.

Proof. Because of the previous proposition, for any expression involving xs and ds, we can move all the ds to the right in each term. Hence B is at least a spanning set for A.

It then suffices to show that B is linearly independent.

Let $\phi : A \to A$ be given by $\phi(f) = fx - xf$. Observe that $\phi(f+g) = (f+g)x - x(f+g) = fx - xf + gx - xg = \phi(f) + \phi(g)$. Thus ϕ is additive. Since it also respects scalar multiplication by elements of F, then ϕ is F-linear.

Also,

$$\begin{aligned}
\phi(fd) &= (fd)x - x(fd) \\
&= f(xd+1) - xfd \\
&= fxd + f - xfd \\
&= f + (fx - xf)d \\
&= f + \phi(f)d
\end{aligned}$$

That is, $\phi(fd) = f + \phi(f)d$.

By using this result and induction, we will show that $\phi(x^i d^j) = jx^i d^{j-1}$. If $j = 0$, then $\phi(x^i) = x^{i+1} - x^{i+1} = 0$, as desired. If $j = 1$, then $\phi(x^i d) = x^i + \phi(x^i)d = x^i$. If $j > 1$, then

$$\begin{aligned}
\phi(x^i d^j) &= \phi(x^i d^{j-1} d) \\
&= x^i d^{j-1} + \phi(x^i d^{j-1})d \\
&= jx^i d^{j-1}
\end{aligned}$$

This completes the induction. By linearity, we can extend this to all polynomials $f(x)$. That is, $\phi(f(x)d^j) = jf(x)d^{j-1}$ for all polynomials $f(x)$.

Finally we can show that B is an F-basis for A. Suppose $\displaystyle\sum_{finite} a_{i,j}x^i d^j = 0$.

We can write this equation as $f_n(x)d^n + f_{n-1}(x)d^{n-1} + ... + f_0(x)$ for some polynomials f_i. Then by applying ϕ^n, we get that $\phi^n(f_i(x)d^i) = 0$ for $i \leq n-1$, and $\phi^n(f_n(x)d^n) = n!f_n(x)$. Thus $0 = \phi(f_n(x)d^n + ... + f_0(x)) = n!f_n(x)$. Since our field is characteristic 0, then $n! \neq 0$, so $f_n(x) = 0$. Therefore we can remove this term from our linear combination, and repeat until all terms are zero. Thus B is linearly independent, so B is a basis. $\square$

Proposition 29. If F is a field of characteristic 0, then $A_1(F)$ is a simple ring.

Proof. Let $I \neq 0$ be a (two-sided) ideal of A. If $I \neq 0$, then choose some nonzero $g \in I$. Observe that for all $h \in I$, then $\phi(h) = hx - xh \in I$.

We write $g = f_n(x)d^n + ... + f_0(x)$, where $f_n(x) \neq 0$. By applying ϕ^n to g, we get that $phi^n(g) = n!f_n(x) \in I$. Therefore I contains some $f(x) \in F[x] \setminus \{0\}$.

Now we repeat this process with d: $df(x) - f(x)d = f'(x) \in I$. Continuing, we will get that I contains a nonzero constant. Therefore, I contains a nonzero constant. Since F is a field, then $I = A_1(F)$. Therefore the only two-sided ideals in A are A and 0, so A is simple. $\square$

We now have a few exercises that are useful.

Exercise 13. A is neither left nor right Artinian.

Exercise 14. A is a domain.

Exercise 15. A is not semisimple. In fact, A does not contain a simple left ideal.

Now let's move on to the Jacobson density theorem.

Remark 46. Let M and N be R-modules, and let $f : M \to N$ be an R-module homomorphism.

For $n \geq 1$, define $f^{(n)} : M^n \to N^n$ by $f^{(n)}(u_1, ..., u_n) = (f(u_1), ..., f(u_n))$. Then $f^{(n)}$ is an R-module homomorphism.

Let E be an R-module. Let $f \in R''(E) = \mathrm{End}_{R'}(E)$. That is, $f : E \to E$ such that f is additive, and $f\phi = \phi f$ for all $\phi \in R' = \mathrm{End}_R(E)$. Then $f^{(n)} : E^n \to E^n$ is also also $R'(E)$-linear.

We claim that $f^{(n)}$ is $R'(E^n)$-linear. That is, $f^{(n)} \in R''(E^n)$.

This is because $R'(E^n) = \mathrm{End}_R(E^n) = M_n(\mathrm{End}_R(E)) = M_n(R')$. We need to show that $f^{(n)}\phi = \phi f^{(n)}$ for all $\phi \in R'(E^n) = M_n(R')$.

We represent ϕ and $f^{(n)}$ as matrices. Then $f^{(n)} = fI_{E^n}$ and $\phi = \phi_{i,j}$ with each $\phi_{i,j} \in R'(E)$. Then $f^{(n)}\phi = fI_{E^n} \circ \phi_{i,j} = [f\phi_{i,j}] = [\phi_{i,j}f]$ since f is R'-linear. This in turn equals $[\phi_{i,j}] \cdot fI_{E_n}$. Thus $f^{(n)} \in R''(E^n)$ as desired.

16.2 Day 33 - November 13

Recall the following: suppose E is an R-module, $R' = \text{End}_R(E)$ and $R'' = \text{End}_{R'} E$, and $f : E \to E$ is in $R''(E)$. Then $f^{(n)} : E^n \to E^n$ and $f \in R''(E^n)$.

Lemma 20. Let E be a semisimple R-module, and let $f \in R''(E)$. Let $x \in E$. Then there exists $a \in R$ such that $f(x) = ax$.

Proof. Certainly, Rx is a submodule of E. Then since E is semisimple, $E = Rx \oplus N$ for some other submodule N. Define $\pi : E \to E$ by $rx + n \mapsto rx$. Then π is R-linear, so $\pi \in R'(E)$. Also, $\pi(x) = x$, so $f(x) = f(\pi(x))$. Since f is R'-linear, then $f(\pi(x)) = \pi(f(x)) = ax$ for some $a \in R$. Thus by transitivity, $f(x) = ax$ for some $a \in R$. □

Theorem 49 (Jacobson Density Theorem). Let R be a ring, let E be a semisimple R-module, and let $f \in R''(E)$. Let $x_1, ..., x_n \in E$. Then there exists an $a \in R$ such that $f(x_i) = ax_i$ for all i.

Proof. We will use λ_a to denote the map $x \mapsto ax$ for some $a \in R$.

We have that $f^{(n)} \in R''(E^n)$ by the result from last class. Also, E^n is semisimple since E is semisimple. Let $u = (x_1, ..., x_n) \in E^n$. By the lemma there exists $a \in R$ such that $f^{(n)}(u) = au$. That is, $(f(x_1), ..., f(x_n)) = (ax_1, ..., ax_n)$. □

Corollary 15. Let R be a ring, and let E be a semisimple R-module, and suppose E is finitely generated as an R'-module. Then $\lambda : R \to R''(E)$ is surjective. That is, for all $f \in R''(E)$, there exists an $a \in R$ such that $f = \lambda_a$.

Proof. Since E is finitely generated as an R'-module, there exists a finite generating set $\{x_1, ..., x_n\}$. Let $f \in R''(E)$. By the Jacobson Density Theorem, there exists some $a \in R$ such that $f(x_i)\lambda_a(x_i)$ for all i. If $x \in E$, then $x = \sum_{i=1}^{n} s_i x_i$ for some $s_i \in R'$. Then $f(x) = f(\sum s_i x_i) = \sum s_i f(x_i) = \sum s_i \lambda_a(x_i) = \lambda_a(\sum s_i x_i) = \lambda_a(x)$. Thus $f = \lambda_a$. □

Corollary 16. Let R be a semisimple ring, and let $E \neq 0$ be a free R-module (that is, E has an R-basis $\{e_\alpha\}_{\alpha \in I}$). Then $\lambda : R \to R''(E)$ is an isomorphism.

Proof. Let e be any basis element of E. Then $R'e \cong E$ since one can define an R-linear map by sending a basis to any set of elements in E. Therefore E is a finitely generated R' module. Thus $E = \bigoplus R$ is semisimple, since R is. Therefore, by the previous corollary, $\lambda : R \to R''(E)$ is surjective.

Suppose $\lambda(a) = 0$. Then in particular $ae = 0$, so $a = 0$ since e is a basis element. Thus λ is injective, hence bijective. Thus λ is an isomorphism. □

Corollary 17. Let D be a division ring and let $E \neq 0$ be a D-vector space. Then $\lambda : D \to D''(E) = \text{End}_{D'}(E)$ is an isomorphism.

Proof. Since D is a division ring, it is semisimple. Since E is a D-vector space, then it is a free D-module. Then by the previous theorem, λ is an isomorphism. □

Corollary 18. Suppose $M_{n_1}(D_1) \cong M_{n_2}(D_2)$ where D_1 and D_2 are division rings and n_1, n_2 are positive integers. Then $D_1 \cong D_2$ and $n_1 = n_2$.

Proof. Recall that for any ring, $M_n(R) \cong \mathrm{End}_{R^0}(R^o)^n$. Since D_1^o and D_2^o are also division rings, by renaming D_1^o to D_1 and D_2^o to D_2, we will simply show that if $\mathrm{End}_{D_1} D_1^{n_1} \cong \mathrm{End}_{D_2} D_2^{n_2}$, then $D_1 \cong D_2$ and $n_1 = n_2$.

Let $R = \mathrm{End}_{D_1} D_1^{n_1}$. Recall that R is simple and semisimple. Therefore, R has a unique simple left module (up to isomorphism). This simple left module is isomorphic to the rows of this matrix, which are of course $D_1^{n_1}$. Thus $D_1^{n_1}$ is a simple. R-module.

Similarly, $D_2^{n_2}$ is a simple R-module. Therefore $D_1^{n_1} \cong D_2^{n_2}$ as left R-modules. Thus $\mathrm{End}_R(D_1^{n_1}) \cong \mathrm{End}_R(D_2^{n_2})$ as rings. But by Corollary 17, $\mathrm{End}_R(D_1^{n_1}) \cong D_1$ and $\mathrm{End}_R(D_2^{n_2}) \cong D_2$. Thus $D_1 \cong D_2$. But $D_1^{n_1} \cong D_2^{n_2} \cong D_1^{n_2}$, so by taking dimensions, we can see that $n_1 = n_2$. □

Theorem 50 (Artin-Wedderburn, Part 2). Let R be a semisimple ring. Then $R \cong M_{n_1}(D_1) \times ... \times M_{n_k}(D_k)$ for division rings $D_1, ..., D_k$ and positive integers $n_1, ..., n_k$. Furthermore, the $D_1, ..., D_k$ and $n_1, ..., n_k$ that let you write R in this way are unique, up to reordering.

Proof. We have previously shown that there exist division rings and integers satisfying this. It then suffices to show uniqueness.

By a homework problem [edit: see immediately below], the number k is unique, and furthermore the rings $M_{n_i}(D_i)$ are unique up to reordering. But then by the previous corollary, since we know $M_{n_i}(D_i)$, we know what n_i and D_i are. Thus this decomposition is unique. □

Homework Problem 7. *If $A_1 \times ... \times A_l \cong B_1 \times ... \times B_k$ where each A_i and B_j are simple rings, then $k = l$ and after rearrangement $A_i \cong B_i$ for all i.*

Definition 47. Let R be a commutative ring, and let S be a ring. We say S is an *R-algebra* if there exists a ring homomorphism $\phi :\to S$ such that $\phi(R) \subset Z(S) = \{s \in S | st = ts \text{ for all } t \in S\}$.

Remark 47. Let R be a ring, let E be an R-module, and let $r \in Z(R)$. Then $\lambda_r \in R'(E)$, so there exists a ring homomorphism $\lambda : Z(R) \to R'(E)$ by $r \mapsto \lambda_r$.

Remark 48. If E is finitely generated over $Z(R)$ (that is, if $E = Z(R)u_1 + ... + Z(R)u_n$ for some $u_1, ..., u_n \in E$), then $E = R'u_1 + ... + R'u_n$. Thus E is finitely generated as a R'-module.

Remark 49. Suppose k is a field, and R is a finite dimensional k-algebra (that is, $\dim_k(R) < \infty$).

Let E be a finitely generated semisimple R-module. Then $\lambda : R \to R''(E)$ is surjective.

Proof. Since R is a finite dimensional k-algebra, then $R = kv_1 + ... + kv_s \subset Z(R)v_1 + ... + Z(R)v_s$. However, $Z(R)v_1 + ... + Z(R)v_s \subset R$, so $Z(R)v_1 + ... + Z(R)v_s = R$.

Then by substitution, $E = Ru_1 + ... + Ru_t = \displaystyle\sum_{i,j} Z(R)v_iu_j$, so E is finitely generated as a $Z(R)$ module.

Thus E is finitely generated as an R' module. Therefore, by Corollary 15, λ is onto. □

17 k-Algebras

17.1 Day 34 - November 16

Let's do examples of k-algebras!

Example 50. Let k be a field. Then the following are k-algebras: $k[x_1, ..., x_n]$, $k[x_1, ..., x_n]/I$, $k(x_1, ..., x_n)$, $A_1(k)$ (the first Weyl algebra), $M_n(k)$, and $k[G]$ (the group ring). Of these, the finite dimensional ones are $k[x_1, ..., x_n]/I$ (for certain I), $M_n(k)$, and $k[G]$ (if and only if G is finite).

Lemma 21. Let D be a division ring, and let k be an algebraically closed field such that D is a k-algebra. If $\dim_k(D) < \infty$, then $D = k$.

Proof. Let $\alpha \in D$. Then $k[\alpha] \subset D$. Since $\dim_k(D) < \infty$, then there exists a linear dependence among $\alpha, \alpha^2, \alpha^3, ...$ That is, there exists $k_n, ..., k_0$, not all equal to 0, such that $0 = k_n\alpha^n + ... + k_0$. That is, α is a root of $f(x) = k_nx^n + ...k_0$. Thus $\alpha \in k$, so $k = D$. □

Corollary 19. Suppose k is an algebraically closed field and R is a finite dimension k-algebra. Then R is semisimple if and only if $R \cong M_{n_1}(k) \times ... \times M_{n_l}(k)$.

Proof. Suppose $R \cong M_{n_1}(k) \times ... \times M_{n_l}(k)$. Then each of these matrix rings is semisimple, so R is semisimple, as desired.

Suppose instead that R is semisimple. By the Artin-Wedderburn theorem, $R \cong M_{n_1}(D_1) \times ... \times M_{n_l}(D_l)$ where $D_1, ..., D_l$ are division rings.

Recall that $D_i^o = \operatorname{End}_R(E_i)$, where E_i is a semisimple R-module. Note that $\operatorname{End}_R(E_i) \subset \operatorname{End}_k(E_i)$. Then since E_i is simple, $E_i = Rx_i$ for any $x_i \in E_i \setminus \{0\}$. Thus $\dim_k(R) < \infty$, so $\dim_k E_i < \infty$. Thus $E \cong k^n$. Therefore $\operatorname{End}_k(E_i) = M_n(k)$.

But $\operatorname{End}_R(E_i) \subset \operatorname{End}_k(E_i)$, so D_i^o is finite dimensional as a k-vector space. But D_i^o is also a division ring, so by the lemma, $D_i^o \cong k$. Thus $D^i \cong k^o = k$, so $R \cong M_{n_1}(k) \times ... \times M_{n_l}(k)$, as desired. □

Theorem 51 (Burnside). Let k be an algebraically closed field, and let V be a finite-dimensional k-vector space. Let R be a subalgebra of $\operatorname{End}_k(V)$. Then if V is a simple R-module, then

1. $k = \operatorname{End}_R(V)$
2. $R = \operatorname{End}_k(V)$

Proof. (Proof of 1) Certainly, since $k \subset R$, then $\operatorname{End}_R(V) \subset \operatorname{End}_k(V)$. Since V is a finite-dimensional k-vector space, then $\operatorname{End}_k(V) \cong M_n(k)$, so $\operatorname{End}_R(V)$ is a finite dimesnional k-algebra. Also, $\operatorname{End}_R(V)$ is a division ring, as V is a simple R-module. Therefore by the lemma, $k \cong \operatorname{End}_R(V)$. □

(Proof of 2) By the last remark, from last class, the ring homomorphism $R \to R''(V)$ is surjective. But $R''(V) = \operatorname{End}_{R'}(V)$, and $R' = \operatorname{End}_R(V) \cong k$, so $R''(V) = \operatorname{End}_k(V)$. But $R \subset \operatorname{End}_k(V)$, so λ is injective as well. Therefore λ is an isomorphism, so $R = \operatorname{End}_k(V)$. □

Definition 48. Let R be a ring. An element $x \in R$ is *nilpotent* if $x^n = 0$ for some $n \in \mathbb{N}$.

Let I be a left ideal. Recall I^n is the left ideal generated by $\{a_1...a_n | a_i \in I\}$. Then we say an ideal I is *nilpotent* if $I^n = 0$ for some n.

A left ideal I is called *nil* if every element of I is nilpotent.

Remark 50. Every nilpotent left ideal is nil.

It need not follow that a nil ideal is nilpotent, even if the ring is commutative. An example of this is given in the next exercise.

Exercise 16. Let $R = k[x_1, x_2, ...]/(x_1^1, x_2^2, x_3^3...)$, and let $I = (\overline{x}_1, \overline{x}_2, ...)$. Show that I is nil, but not nilpotent.

Exercise 17. If I is a finitely generated ideal, then I is nilpotent if and only if I is nil.

If R is a commutative ring, then the sum of nilpotent elements is nilpotent.

However, if R is not commutative, the sum of two nilpotent elements may not be nilpotent. For instance, let $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and let $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Then $A^2 = 0$ and $B^2 = 0$, but $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $(A+B)^2 = I$, so $A + B$ is not nilpotent.

History time: Wedderburn's actual result was classifying all finite dimensional R-algebras such that the only left ideal which is nil is zero. The criterion of the only nil left ideal being zero is equivalent to a finite-dimensional k-algebra being semisimple.

Artin later gave a more general condition in terms of chain conditions. Later still, Jacobson generalized this to a statement about the intersection of all maximal left ideals. This was later named after him.

18 Jacobson Radical

Definition 49. Let R be a ring. The *Jacobson radical* is defined to be the intersection of all maximal left ideals. We denote this by $J(R)$.

Lemma 22. Let R be a ring and let $y \in R$. Then the following are equivalent:

1. $y \in J(R)$
2. $1 - xy$ is left-invertible for all $x \in R$
3. $yM = 0$ for every simple left R-module M.

Proof. ($1 \Rightarrow 2$) Suppose $y \in J(R)$. Suppose for the sake of contradiction that $1 - xy$ is not left invertible for some $x \in R$. Then $R(1 - xy)$ is a proper ideal of R, so there exists a left-maximal ideal m such that $R(1 - xy) \subset m$. But $y \in m$, so $1 - xy + xy = 1 \in m$. This is a contradiction, so $1 - xy$ is left invertible. □

($2 \Rightarrow 3$) Suppose $1 - xy$ is left invertible for all $x \in R$. Suppose for the sake of contradiction that $yM \neq 0$ for some simple module M. Then $RyM = M$, and in fact $Ryu = M$ for some $u \in M$. Therefore $u = ryu$ for some $r \in R$, so $(1 - ry)u = 0$. As $1 - ry$ is left invertible, then $u = 0$. This is a contradiction, so $yM = 0$.

($3 \Rightarrow 1$) Suppose $yM = 0$ for all simple left R-modules M. Let m be a maximal left ideal. Then R/m is a simple left R-module. Then $y \cdot R/m = 0$, so in particular $y \cdot \overline{1} = \overline{y} = 0$. Thus $y \in m$, so y is in every maximal left ideals. Thus $y \in \bigcap_{m \text{ maximal}} m = J(R)$. □

18.1 Day 35 - November 18

Recall from last class the definition of the Jacobson radical: the intersection of all maximal left ideals. We denote it by $J(R)$. Recall also this characterization from last class:

Lemma 23. Let R be a ring and let $y \in R$. Then the following are equivalent:

1. $y \in J(R)$
2. $1 - xy$ is left-invertible for all $x \in R$
3. $yM = 0$ for every simple left R-module M.

Definition 50. If R is a ring and M is an R-module, then the *annihilator* of M is $\mathrm{Ann}_R(M) = \{r \in R | rm = 0 \text{ for all } m \in M\}$.

Remark 51. Let R be a ring and M is an R-module. Also let $r \in R$, $i \in \mathrm{Ann}_R(M)$ and $m \in M$. Then $(ir)m = i(rm) = 0$ since $i \in \mathrm{Ann}_R(M)$, and $(ri)m = r(im) = r0 = 0$ for the same reason. Thus $\mathrm{Ann}_R(M)$ is a two-sided ideal.

Corollary 20. The Jacobson radical is always a two-sided ideal.

Proof. By the lemma, $J(R) = \{y \in R | yM = 0 \text{ for all simple modules } M\}$. That is, $J(R) = \bigcap_{M \text{ simple}} \mathrm{Ann}_R(M)$. Thus $J(R)$ is the intersection of two-sided ideals, so it is a two-sided ideal. □

Proposition 30. Let R be a ring. Then $y \in J(R)$ if and only if $1 - xyz$ is a unit for all $x, z \in R$.

Proof. Suppose $1 - xyz$ is a unit for all $x, z \in R$. Therefore $1 - xy$ is left invertible for all $x \in R$, so by the characterization Lemma, $y \in J(R)$.

If instead $y \in J(R)$, then since $J(R)$ is a two-sided ideal, then $yz \in J(R)$ for all $z \in R$. Then by the characterization Lemma, $1 - xyz$ is left invertible for all $x \in R$.

let u be the left inverse of $1 - xyz$. That is, $u - uxyz = 1$. Therefore $u = 1 + uxyz$. But $J(R)$ is a two-sided ideal, so $xyz \in J(R)$. Therefore, $1 + uxyz = 1 - (-u)xyz$ is left invertible by the characterization lemma. Thus $u = 1 + uxyz$ has a left inverse v. That is, $vu = 1$. But $1 - xyz = vu(1 - xyz) = v$ so $1 - xyz$ has u as both its left inverse and its right inverse. That is, $1 - xyz$ is invertible. □

Corollary 21. If R is a ring, then $J(R) = \bigcap_{\substack{m \text{ maximal} \\ \text{right ideal}}} m = \bigcap_{\substack{m \text{ maximal} \\ \text{right ideal}}} \mathrm{Ann}_R(M)$.

The proof of this is left as an exercise.

Definition 51. A ring R is called *semiprimitive* if $J(R) = 0$.

Example 51. Any simple ring has $J(R) = 0$, so a simple ring is semiprimitive.

Proposition 31. Let R be a semisimple ring. Then $J(R) = 0$.

Proof. Since R is a semisimple ring, we can write $R = I_1 \oplus ... \oplus I_l$, where each I_j is a simple left module.

Then we write $1 = e_1 + ... + e_l$, where each $e_i \in I_i$. Let $y \in J(R)$. Then $yI_j = 0$ for all j by the characterization lemma. Thus $y = y \cdot 1 = ye_1 + ... + ye_i = 0$. Thus $J(R) = 0$. □

Example 52. If F is a field and $A_1(F)$ is the first Weyl algebra, then $J(A_1(F)) = 0$ since $A_1(F)$ is simple.

Since the maximal ideals in $\mathbb{Z}$ are generated by primes, and no number except zero is divisible by infinitely many primes, then $J(\mathbb{Z}) = 0$.

By a similar argument, if K is a field, then $J(K[x_1, ..., x_n]) = 0$.

Theorem 52. Let R be a ring. Then R is semisimple if and only if R is left Artinian and semiprimitive.

Proof. We have already shown that if R is semisimple, then R is left Artinian. Today in the previous proposition, we showed that if R is semisimple, then $J(R) = 0$. That is, R is semiprimitive, as desired.

Suppose instead that R is semiprimitive and left Artinian. That is, $J(R) = 0$. We will first show that R is semisimple.

To this end, suppose I and L are left ideals of R such that $I \subset L$. Suppose also that I is simple. Since I is simple it is nonzero, and since $J(R) = 0$, then $I \not\subset J(R)$. Thus there exists a maximal left ideal m, with $I \not\subset m$. But then $I + m = R$ since m is maximal, and $I \cap m = 0$ since I is simple and m is maximal. Thus $R = I \oplus m$. From this, one can verify that $L = I \oplus (L \cap m)$.

Note that if R is left Artinian, then every nonzero left ideal contains a simple left ideal (just extend the chain as far as possible). Then if L_1 is any ideal in R, we find a simple left ideal $I_1 \subset L_1$. Then there exists an L_2 such that $L_1 = I_1 \oplus L_2$. If $L_2 = 0$, then we are done. If $L_2 \neq 0$, then there exists a simple left ideal $I_2 \subset L_2$.

We then repeat this process until some $L_n = 0$. If no L_i were ever zero, then $I_1 \subset I_1 \oplus I_2 \subset ...$ is an infinite extending chain, which contradicts the assumption that R is left Artinian. Thus there exists some $L_n = 0$. That is, $L_1 = I_1 \oplus ... \oplus I_n$. Then we are mostly done. [fix this up; we didn't actually show its semisimple.]

□

Proposition 32. Let I be a nil left ideal. Then $I \subset J(R)$.

Proof. Let $y \in I$, and let $x \in R$. Then $xy \in I$, so $(xy)^n = 0$ for some n. Thus $1 - xy$ is a unit since $(1 - xy)(1 + xy + (xy)^2 + ... + (xy)^{n-1}) = 1 - (xy)^n = 1$. Therefore $y \in J(R)$. □

Theorem 53. Suppose R is left Artinian. Then $J(R)$ is nilpotent.

Proof. Let $J = J(R)$. Consider the descending chain $J \supset J^2 \supset J^3....$ As R is left Artinian, there exists k such that $J^k = J^{k+1}$. Let $I = J^k$, and note that $I = I^2$.

Suppose for the sake of contradiction that $I \neq 0$. Then let $\Lambda = \{L \text{ left ideal} | IL \neq 0\}$. Note that $I \in \Lambda$, so $\Lambda \neq \emptyset$. Since R is left Artinian, we can choose $L \in \Lambda$ minimal. Since $L \in \Lambda$, then there exists some $y \in L$ such that $Iy \neq 0$. Certainly, $Iy \subset L$ since L is a left ideal. Also, $I(Iy) = I^2y = Iy \neq 0$. Thus $Iy = L$.

Since $y \in L$, then $y = iy$ for some $i \in I$. Therefore $(1 - i)y = 0$. but $1 - i$ is a unit since $i \in I = J(R)^k$. Thus $y = 0$, but this is a contradiction of the fact that $Iy \neq 0$. Thus $I = 0$, but $I = J(R)^k$.

□

Corollary 22. If R is left Artinian (for instance if R is a finite-dimensional k-algebra), then $J(R)$ is the largest nil left ideal. Hence $J(R) = 0$ if and only if 0 is the only nil left ideal.

Proposition 33. Let M be a semisimple R-module. Then the following are equivalent

1. M is Artinian.
2. M is Noetherian.
3. M is finitely generated.
4. $\lambda_R(M) < \infty$.

Proof. First note that since R is semisimple, then M is semisimple. Write $M = \bigoplus_{i \in \Lambda} M_i$, where each M_i is simple.

Note that $\lambda_R(M_i) = 1$ for each i since M_i is simple, so $\lambda_R(M) = |\Lambda|$.

If $\lambda_R(M) = |\Lambda| < \infty$, then we have already shown that the first three propositions hold.

If $\lambda_(R) = |\Lambda| = \infty$, then note that $M_1 \subsetneq M_1 \oplus M_2 \subsetneq M_1 \oplus M_2 \oplus M_3 \subsetneq ...$ is a strictly ascending chain of infinite length so M is not Noetherian. Therefore it is not finitely generated. Similarly, $M \supsetneq M_2 \oplus M_3 \oplus ... \supsetneq M_3 \oplus ... \supsetneq ...$ therefore M is not Artinian either. ☐

Note also that if R is semisimple, then every R-module is semisimple, so the previous theorem holds.

18.2 Day 36 - November 20

Tom just looked up this definition, so it probably isn't important.

Definition 52. A ring R is *left primitive* if there exists a simple left R-module M such that $\mathrm{Ann}_R(M) = 0$.

Remark 52. Recall that $J(R)$ is the intersection of $\mathrm{Ann}_R(M)$ over all simple left R-modules M, so being primitive implies that $J(R) = 0$. That is, a ring being primitive implies it is semiprimitive.

Also, R being simple (as a ring) implies that R is primitive.

Furthermore, if D is a division ring and V is a D-vector space, then one can show that $\mathrm{End}_D(V)$ is primitive. Also, one can show that $\mathrm{End}_D(V)$ is simple if and only if $\dim_D(V) < \infty$. Thus if V is infinite-dimensional, then $\mathrm{End}_D(V)$ is primitive but not simple.

We now forever leave behind primitive rings, and focus again on the Jacobson radical. Here we shall use it to show that Artinian rings are Noetherian.

Theorem 54. Let R be a left Artinian ring, and let M be an Artinian left R-module. Then $\lambda_R(M) < \infty$. In particular, R is left Noetherian.

Proof. Let $J = J(R)$. Since M is Artinian, then J^iM is Artinian for any $i \geq 0$ (with the convention that $J^0 = R$). Therefore $J^iM/J^{i+1}M$ is Artinian.

But note that $J \cdot (J^iM/J^{i+1}M) = 0$. Therefore $J^iM/J^{i+1}M$ is an R/J-module by the action of $\overline{r} \cdot u = ru$ for $\overline{r} \in R/J$ and $u \in J^iM/J^{i+1}M$.

One can also check (and I should do this) that $J(R/J) = 0$.

Since $J(R/J) = 0$, then R/J is semisimple. Therefore, by the last Proposition from last class, $\lambda_{R/J}(J^iM/J^{i+1}M) < \infty$ for all i. But one can check that $\lambda_R(anything) = \lambda_{R/J}(anything)$, so $\lambda_R(J^iM/J^{i-1}M) < \infty$ for all i.

We will now show that $\lambda_R(M/J^iM) < \infty$ for all i. We will use induction for this. The base case is that $M/JM = J^0M/J^1M$ has finite length, and this follows from the last statement.

In the inductive case, we can make the following exact sequence of modules $0 \to J^{i-1}M/J^iM \to M/J^iM \to M/J^{i-1}M \to 0$. Since length is additive on exact sequences, $J^{i-1}M/J^iM$ is finite length by previous statement, and $M/J^{i-1}M$ is finite length by the inductive hypothesis, then M/J^iM is finite length. Thus by induction M/J^iM is finite length for all $i \geq 0$.

However, by a Theorem from last class, $J^n = 0$ for some n, so $M/J^nM = M/0 \cong M$ is finite length. ☐

Now we will prove Nakayama's Lemma, which is one of the most important claims built off of the Jacobson radical.

Theorem 55 (Nakayama's Lemma). Let R be a ring, and let M be a finitely generated left R-module. Suppose also that $M = J(R)M$. Then $M = 0$.

Proof. Let $J = J(R)$. Suppose for the sake of contradiction that $M \neq 0$. Let n be the least number of generators for M. Since $M \neq 0$, then $n > 0$.

Let $M = Rx_1 + ... + Rx_n$ for some $x_i \in M$. Then $JM = Jx_1 + ... + Jx_n$. Since $x_n \in JM = M$, then $x_n = j_1x_1 + ...j_nx_n$ where each $j_i \in J$. Then $(1 - j_n)x_n = j_1x_1 + ... + x_{n-1}x_{n-1}$. However, $j_n \in J$, so $1 - j_n$ is a unit in R. Thus $x_n = (1 - j_n)^{-1}xj_1x_1 + ... + (1 - j_n)^{-1}j_{n-1}x_{n-1} \in Rx_1 + ... + Rx_{n-1}$.

Therefore $M = Rx_1 + ... + Rx_{n-1}$, which contradicts our choice of n. Thus $M = 0$. $\square$

Remark 53. Nakayama's lemma fails for non-finitely-generated rings. For instance, if k is a field, and $R = k[[x]]$, then $J(R) = m = (x)$. Then $Q(R) = k((x))$ is an R-module, and furthermore $JQ(R) = Q(R)$. However, $Q(R) \neq 0$, so $Q(R)$ is not finitely generated.

This is an example of how Nakayama's Lemma can let you show something is not finitely generated.

Remark 54. If R is a ring and M is an R-module, then we use the following notation. Define $\mu_R(M) = \inf\{n \geq 0 | M = Rx_1 + ... + Rx_n \text{ for some } x_i \in M\}$. That is, $\mu_R(M)$ is the minimal number of generators of M.

Lemma 24. Let M be a finitely generatede R-module, let $N \subset M$ be a submodule, and let $J = J(R)$. Suppose $M = N + JM$. Then $M = N$.

Proof. Note that $M = N + JM$ if and only if $M/N = (JM + N)/N = J \cdot M/N$. As M is finitely generated, then so is M/N. Therefore by Nakayama's Lemma, $M/N = 0$, so $M = N$. $\square$

Remark 55. The term "Nakayama's lemma" is used loosely by mathematicians. The lemma has many immediate corollaries, and mathematicians may refer to any of them as "Nakayama's lemma".

Proposition 34. Let M be a finitely generated R-module, and let $x_1, ..., x_n \in M$. Let $J = J(R)$. Then $x_1, ..., x_n$ generate M if and only if $\overline{x}_1, ..., \overline{x}_n$ generate M/JM.

Proof. Certainly, if $x_1, ..., x_n$ generate M, then their representatives in M/JM generate M/JM.

Conversely, suppose $\overline{x}_1, ..., \overline{x}_n$ generate M/JM. Let $N = Rx_1 + ... + Rx_n$. Then $(N + JM)/JM = R\overline{x}_1 + ...R\overline{x}_n = M/JM$. Therefore $N + JM = M$. By the previous lemma, $N = M$, as desired. $\square$

Corollary 23. Let M be a finitely generated R-module, and let $J = J(R)$. Then $\mu_R(M) = \mu_{R/J}(M/JM)$.

Proof. By the previous proposition, generating sets for M as an R-module correspond to generating sets for R/JM as an R/J-module. Thus their lengths are equal. $\square$

18.3 Day 37 - November 23

Recall from last class the following named theorem:

Theorem 56. (Nakayama's Lemma) Let R be a ring, and let M be a finitely generated left R-module. Suppose also that $M = J(R)M$. Then $M = 0$.

Yet another corollary of Nakayama's Lemma is the following.

Corollary 24. Let R be a commutative ring with a unique maximal ideal m (that is, R is a local ring). Let M be a finitely generated R-module. Then $\mu_R(M) = \dim_{R/m} M/mM$.

Proof. Since m is the unique maximal ideal, then $J(R) = m$. Therefore $\mu_R(M) = \mu_{R/m}(M/mM) = \dim_{R/m}(M/mM)$. $\square$

Definition 53. Let # denote the short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ and let ## denote the short exact sequence $0 \to L \xrightarrow{h} M \xrightarrow{l} N \to 0$. Bothof these are short exact sequences of (left) R-modules.

We say # and ## are *isomorphic* if there exists a commutative diagram [oh boy] (consisting of # above ##, with arrows pointed down from A to L, etc, where each of those arrows is an isomorphism.)

Definition 54. A short exact sequence of the form $0 \to A \xrightarrow{\rho} A \oplus B \xrightarrow{\pi} B \to 0$ where $\rho : a \mapsto (a, 0)$ and $\pi : (a, b) \mapsto b$ is *canonically split*.

We say a short exact sequence is *split* if it is isomorphic to a canonically split short exact sequence.

Theorem 57 (The Splitting Theorem). Let # denote the short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$. Then the following are equivalent

1. # splits.
2. There exists an isomorphism of commutative diagrams between # and $0 \to A \xrightarrow{l} A \oplus C \xrightarrow{\pi} C \to 0$ where the vertical arrows are $1_A : A \to A$, $h : B \to A \oplus C$, $1_C : C \to C$, and such that h is an isomorphism.
3. There exists $i : B \to A$ such that $if = 1_A$.
4. There exists $j : C \to B$ such that $gj = 1_C$.
5. There exists $i : B \to A$ and $j : C \to B$ such that $1_B = fi + jg$.
6. $f(A)$ is a direct summand of B.

Proof. ($1 \Rightarrow 5$) Suppose # splits. That is, there exists an isomorphism between # and $0 \to L \xrightarrow{l} L \oplus M \xrightarrow{\pi} M \to 0$ (where the maps are labelled α, β, γ respectively. Then define $\tau : L \oplus M \to L$ by $\tau(l, m) = l$ and $\delta : M \to L \oplus M$ by $\delta(m) = (0, m)$. Then $1_{L \oplus M} = l\tau + \delta\pi$. Finally, let $i = \alpha^{-1}\tau\beta$ and let $j = \beta^{-1}\delta\gamma$. Then

$$\begin{aligned} fi + jg &= f\alpha^{-1}\tau\beta + \beta^{-1}\delta\gamma g \\ &= \beta^{-1}l\tau\beta + \beta^{-1}\delta\pi\beta \\ &= \beta^{-1}(l\tau + \delta\pi)\beta \\ &= \beta^{-1}\beta \\ &= 1_B \end{aligned}$$

as desired. □

($5 \Rightarrow 4$) [lost].

($4 \Rightarrow 3$) Let $K = \ker g = \operatorname{im} f$. Then $\overline{f} : A \to K$ is an isomorphism. Let $\rho : K \to A$ where $\rho = \overline{f}^{-1}$. Let $b \in B$. Then $g(b - jg(b)) = g(b) - g(b) = 0$. Therefore $(1_B - jg)(b) = b - jb(b) \in K$ so $1 - jg : B \to K$. Let $i = \rho(1 - jg) : B \to A$. Then $if = \rho(1 - jg)f = \rho f = 1_A$. □

($3 \Rightarrow 2$) Define $h : B \to A \oplus C$ by $h : b \mapsto (i(b), g(b))$. Then one can verify that the appropriate diagram commutes. It then suffices to show that h is an isomorphism.

We will now show that h is injective. First, note that if $h(b) = 0$ then $g(b) = 0$, so $b \in im(f)$. Let $b = f(a)$ for some $a \in A$. Then $0 = i(b) = i(f(a)) = a$, so $a = 0$ and therefore $b = f(a) = 0$. Thus h is injective.

We will now show that h is surjective. Let $(a, c) \in A \oplus C$. Since g is onto, then there exists some $b \in B$ such that $g(b) = c$. Let $b' = f(a) + b - f(i(b))$. Then $i(b') = i(f(a)) + i(b) - ifi(b) = a + i(b) - i(b) = a$. Also, $g(b') = g(b)$, so $h(b') = (a, c)$. Thus h is surjective.

Therefore h is bijective, so it is an isomorphism. Thus there exists the desired isomorphism of commutative diagrams. □

($2 \Rightarrow 1$) This is immediate, since such an isomorphism of commutative diagrams is a splitting of #. □

We have now shown that (1) – (5) are equivalent. It then suffices to show that (6) is equivalent.

($6 \Rightarrow 3$) Suppose $B = f(A) \oplus D$ for some submodule D of B. Define $i : B \to A$ by $f(a) + d \mapsto a$. This is well-defined since f is injective and the sum is direct. Also, $i(f(a)) = a$, so $if = 1_A$. □

($2 \Rightarrow 6$) Suppose h is an isomorphism from B to $A \oplus C$. Then $h^{-1} : A \oplus C \to B$ is an isomorphism. Then $B = h^{-1}(A) \oplus h^{-1}(C)$, and $h^{-1}(A) = h^{-1}\rho(A) = f(A)$. Thus B is a direct summand of $f(A)$. □ □

Corollary 25. Suppose $0 \to A \to B \to C \to 0$ is split. Then $B \cong A \oplus C$.

Proof. This is a direct result of ($1 \Rightarrow 2$). □

19 Projective Modules

Definition 55. An R-module P is called *projective* if, given any exact sequence $M \xrightarrow{f} N \to 0$ and map $g : P \to N$, there exists an $h : P \to M$ such that $fh = g$. (This can be represented with a diagram.)

Proposition 35. Any free R-module F is projective.

Proof. Since F is free, there exists an R-basis $\{e_\alpha\}$. Suppose $M \xrightarrow{f} N \to 0$. And suppose $g : F \to N$. Then since f is onto, for each α, there exists $m_\alpha \in M$ such that $f(m_\alpha) = g(e_\alpha)$. Then define $h : F \to M$ by $e_\alpha \mapsto m_\alpha$. One can then verify that $fh = g$. □

19.1 Day 38 - November 30

We're back!

Recall the following definition from last time:

Definition 56. An R-module P is called *projective* if, given any exact sequence $M \xrightarrow{f} N \to 0$ and map $g : P \to N$, there exists an $h : P \to M$ such that $fh = g$. (This can be represented with a diagram.)

Proposition 36. Let R be a ring, and let P be an R-module. Then the following are equivalent:

1. P is projective.
2. Every short exact sequence of the form $0 \to L \to M \to P \to 0$ splits.
3. P is a direct summand of a free module.

Proof. ($1 \Rightarrow 2$) Take a short exact sequence $0 \to L \to M \xrightarrow{f} P \to 0$. Since P is projective and embeds into itself by 1_P, then by the definition of projective, there exists a function $j : P \to M$ such that $fj = 1_P$. Then by one of the criterion for a splitting sequence, the short exact sequence splits.

($2 \Rightarrow 3$) Suppose every short exact sequence with P in it splits. There exists a free module F and a projection $\phi : F \to P$ which is free. Let $K = \ker\ \phi$. Then $0 \to K \to F \to P \to 0$ is a short exact sequence. By (2), this short exact sequence splits. Therefore $F \cong P \oplus K$. That is, P is a direct summand of a free module.

($3 \Rightarrow 1$) Suppose P is a direct summand of a free module. That is, there exists a free module F and a module Q such that $P \oplus Q = F$. Define $\pi : F \to P$ by $(p, q) \mapsto p$ and $rho : P \to F$ by $p \mapsto (p, 0)$. Note that $\pi\rho = 1_P$.

Consider a diagram $M \xrightarrow{f} N \to 0$, with $g : P \to N$. Then there exists a function $h : F \to M$ such that $fh = g\pi$ [why?]. Let $\overline{h} = h\rho : P \to M$. Then $f\overline{h} = fh\rho = g\pi\rho = g$, so P is projective. □

Theorem 58. Let R be a ring. Then R is semisimple if and only if every R-module is projective.

Proof. Suppose R is semisimple. Let M be an R-module. As always, there exists a free module F and a surjective map $\phi : F \to M$. Let $K = ker\phi$. This gives a short exact sequence $0 \to K \to F \xrightarrow{\phi} M \to 0$. Since R is semisimple, F is semisimple, so K is a direct summand of F. Therefore the sequnce splits, so $F \cong M \oplus K$. By the previous proposition, this is equivalent to M being projective, as desired.

Suppose instead that every R-module is projective. Let I be a left ideal of R. Then consider the short exact sequence $0 \to I \to R \to R/I \to 0$. Since R/I is an R-module, it is projective, so this sequence splits. That is $R \cong I \oplus R/I$, so R is semisimple. □

Theorem 59. Let R be a ring. Then R is a division ring if and only if every R-module is free.

Proof. Suppose R is a division ring. Then R-modules are R-vector spaces. By elementary linear algebra, every R-vector space is free.

Suppose every R-module is free. Then since free modules are projective, by the previous theorem R is semisimple. That is, $R = I_1 \oplus ... \oplus I_n$ where each I_j is a simple left ideal. Then $\lambda_R(I_j) = 1$ for all j, since I_j is a simple left ideal. Thus $\lambda_R(R) = n$. Since I_j is simple, it is free, so $I_j \cong R^l$ for some $n > 0$. Thus $1 = \lambda(I_j) = \lambda(R^l) = ln$, so $n = 1$. That is, $R = I_1$, and I_1 is a simple left ideal, so the only left ideals of R are 0 and R. Thus R is a division ring. $\square$

Example 53. Let D be a division ring and let $n > 1$. Let $R = M_n(D)$, and let $P = D^n$. Recall that P is a simple R-module. (In fact, $R \cong P \oplus ... \oplus P$.) Then P is projective but not free.

We can see that P is projective either because it is a direct summand of R, which is a free R-module, or because R is semisimple, so all its modules are projective.

However, P is not free since $\lambda_R(P) = 1 < n = \lambda(R)$.

Example 54. Let $R = \mathbb{Z}[\sqrt{-5}]$. Then $I = (2, 1 + \sqrt{-5})$ is projective, but not free.

Example 55. Let $R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$. Define $\phi : R \to R$ by $(r_1, r_2, r_3) \mapsto r_1\overline{x} + r_2\overline{y} + r_3\overline{z}$. Note that ϕ is surjective since $\phi(r\overline{x}, r\overline{y}, r\overline{z}) = r(\overline{x}^2 + \overline{y}^2 + \overline{z}^2) = r \cdot \overline{1} = \overline{r}$.

Let $P = ker\ \phi$. We have a short exact sequence $0 \to P \to R^3 \xrightarrow{\phi} R \to 0$. As an R-module, R is free, so R is projective as an R-module as well. Therefore this short exact sequence splits, so $R^3 \cong P \oplus R$. Thus P is a direct summand of a free module, so P is projective as an R-module. However, $P \ncong R^2$, so P is not free (this last assertion is nonobvious and the proof uses differential geometry).

Example 56. (Quillen-Suslin, 1976) Let k be a field and let $R = k[x_1, ..., x_n]$ be a polynomial ring over k. Then every projective R-module is free.

20 Group Rings are Semisimple

Recall what a group ring is: if R is a ring and G is a group, then $R[G]$ is the group ring of formal sums of elements of G.

20.1 Day 39 - December 2

We will now continue with the proof of Maschke's Theorem.

Theorem 60 (Maschke's Theorem). Let k be a field and let G be a finite group. Then $R = k[G]$ is semisimple if and only if *char* $k \nmid |G|$.

Proof. Suppose *char* $k \nmid |G|$. Let I be a left ideal of R. We need to show that $0 \to I \to R \to R/I \to 0$ splits.

Since I is an R-module, it is also a k-module. That is, I is a k-vector space, so R is a direct summand as k-modules.

Let $\pi : R \to I$ be a k-linear function such that $\pi(i) = i$ for all $i \in I$.

Let $g \in G$. We wish to show $g\pi g^{-1}$ maps from R into I. Let $a \in R$. Then $\pi(g^{-1}a) \in I$, so $g\pi(g^{-1}a) \in I$ since I is a left ideal. Therefore $g\pi g^{-1} : R \to I$. Also, once can verify that $g\pi g^{-1}$ is k-linear.

Lastly, let $\phi = \frac{1}{|G|} \sum_{g \in G} g\pi g^{-1} : R \to I$. Here we used the fact that *char* $k \nmid |G|$. Since this is the average of k-linear maps, this is k-linear. In order to show that ϕ is R-linear, it suffices to show that it respects multiplication by $h \in G$.

Fix some $h \in G$ and $a \in R$. Then

$$\begin{aligned}
\phi(ha) &= \frac{1}{|G|}\sum_{g\in G} g\pi g^{-1}(ha) \\
&= \frac{1}{|G|}\sum_{hg\in G} (hg)\pi(hg)^{-1}(ha) \\
&= h\left(\frac{1}{|G|}\cdot\sum_{hg\in G} g\pi g(a)\right) \\
&= h\phi(a)
\end{aligned}$$

Also, for all $i \in I$, $\phi(i) = \frac{1}{|G|}\sum_{g\in G} g\pi g^{-1}(i) = \dfrac{1}{|G|}\sum_{g\in G} i = i$, so ϕ fixes I. Thus since $0 \to I \to R \to R/I \to 0$ splits, then $R \cong I \oplus R/I$. Since I was arbitrary, then R is semisimple.

Conversely, suppose $char\ k \big| |G|$. Then $char\ k \neq 0$, so let $p = char\ k$.

Let $x = \sum_{g\in G} g$. Then $x \in k[G]$. Also note that for all $h \in G$, $hx = \sum_{g\in G} hg = x = xh$, so $x \in Z(k[G])$.

But also $x \cdot x = \left(\sum_{g\in G} g\right) x = \sum_{g\in G} gx = \sum_{g\in G} x = |G|x = 0$ (the final inequality follows because $p \big| |G|$. Thus $x^2 = 0$, so Rx is a nilpotent left ideal. Therefore $Rx \subset J(R)$, but $Rx \neq 0$, so R is not semisimple since it has a nontrivial Jacobson radical. □

We can extend the statement of Maschke's Theorem to infinite groups as well.

Proposition 37. Suppose k is a field and G is an infinite group. Then $k[G]$ is not semisimple.

Proof. Let $R = K[G]$ and define $\phi : R \to K$ by $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$. One can verify that ϕ is a homomorphism of rings [and I should do this].

Let $L = ker\ \phi$. Since ϕ is a homomorphism or rings, then L is an ideal of R. Also, $L \neq 0$ since $1 - g \in L$ for all $g \in G$.

Suppose for the sake of contradiction that R is semisimple. Then there exists a left ideal J such that $R = L \oplus J$. Since $L \neq R$, $J \neq 0$.

Let f be a nonzero element of J, and write $f = \sum_{g\in G} a_g g$. Let $h \in G$. Then $1 - h \in L$, so $(1 - h)f \in L$ and $(1 - h)f \in J$. Since $L \cap J = 0$, then $(1 - h)f = 0$, so $f = hf$.

That is, $f = \sum_{g\in G} a_g g = hf = \sum_{g\in G} a_g(hg)$. By comparing coefficients, $a_g = a_{h^{-1}g}$ for all $g \in G$. However, our choice of h was arbitrary as well, so by the correct choice of h, we can show that $a_g = a_{g'}$ for all $g, g' \in G$. Since $\sum_{g\in G} a_g g$ must be a finite sum, then $a_g = 0$ for all g. Thus $f = 0$, which contradicts our choice of f. Therefore R is not semisimple.

□

Let's recap.

Remark 56. If R is both simple and semisimple as a ring, then $R = I \oplus I \oplus ... \oplus I$ for any simple left ideal I. We will write $R = nI$ to denote this, when there are n copies of I. Then $D = \mathrm{End}_R(I)$ is a division ring, and $R \cong \mathrm{End}_D(I)$.

Furthermore, if R is an arbitrary semsimple ring, then there are finitely many distinct simple left ideals up to isomorphism. Let us denote them $I_1, ..., I_t$. For each j, let $B(I_j) = \sum_{J\cong I_j} J$. Then $B(I_j)$ is a ring, and is both simple and semisimple as a ring. Then $R \cong B(I_1) \times ... \times B(I_t) \cong n_1 I_1 \oplus ... \oplus n_t I_t$. Also, $\text{End}_R(I_j) = \text{End}_{B(I_j)}(I_j) = D_j$ for some division ring D_j. Therefore $B(I_j) = \text{End}_{D_j}(I_j)$.

We are interesting in figuring out what the n_is are.

Theorem 61. Let k be an algebraically closed field, and let R be a finite dimensional semisimple k-algebra. Write $R \cong n_1 I_1 \oplus ... \oplus n_t I_t$ where the I_js are simple left ideals of R and distinct including isomorphism.

Then

1. $n_i = \dim_k(I_i)$ for all i.
2. $\dim_k(R) = \displaystyle\sum_{i=1}^{t} n_i^2$.
3. $k = \text{End}_R(I_j)$ for all $j = 1, ..., t$.

Proof. (Proof of 3) Let $D_j = \text{End}_R(I_j)$. Since $\text{End}_R(I_j) \subset \text{End}_k(I_j)$, then $\dim_k(D_j) \leq \dim_k(\text{End}_k(I_j)) = n_j^2$. Also, $k \subset Z(\text{End}_k(I_j))$, so $k \subset Z(D_j)$. Thus D is a finite dimensional extension of k, but since k is an algebraically closed field, $D_j = k$. □

(Proof of 1) Let $m_j = \dim_k(I_j) \leq \dim_k(R) < \infty$. We wish to show that $m_j = n_j$. Let $B(I_j) = n_j I_j$. Since $D_j = k$, we have that $n_j I_j = B(I_j) = \text{End}_k(I_j)$. By comparison of the vector space dimensions, $n_j m_j = n_j^2$, so by cancellation, $m_j = n_j$. □

(Proof of 2) then $\dim_k(R) = \displaystyle\sum_{i=1}^{t} n_i \dim_k(I_i) = \sum_{i=1}^{t} n_i^2$.

□

20.2 Day 40 - December 4

Recall this theorem from last class:

Theorem 62. Let k be an algebraically closed field, and let R be a finite dimensional semisimple k-algebra. Write $R \cong n_1 I_1 \oplus ... \oplus n_t I_t$ where the I_js are simple left ideals of R and distinct including isomorphism.

Then

1. $n_i = \dim_k(I_i)$ for all i.
2. $\dim_k(R) = \displaystyle\sum_{i=1}^{t} n_i^2$.
3. $k = \text{End}_R(I_j)$ for all $j = 1, ..., t$.

Proposition 38. Let G be a finite group, and k be a field. Let $C_1, ..., C_r$ be the distinct conjugacy classes of G. For each $i = 1, ..., r$, let $z_i = \displaystyle\sum_{g \in C_i} g \in k[G]$. Then $\{z_1, ..., z_r\}$ is a k-basis for $Z(k[G])$.

Proof. Let $h \in G$ and let C_i be a conjugacy class. Then $hC_ih^{-1} = C_i$ since conjugation by h is a injective and sends elements of C_i to elements of C_i. Therefore

$$\begin{aligned} hz_ih^{-1} &= h(\sum_{g \in C_i} gh^{-1} \\ &= \sum_{g \in C_i} hgh^{-1} \\ &= \sum_{g \in C_i} g \\ &= z_i \end{aligned}$$

Therefore $hz_i = z_ih$ for all $h \in G$. Thus $z_i \in Z(k[G])$ for all i, so $\{z_1, ..., z_r\} \subset Z(k[G])$.
Also, since $C_i \cap C_j = \emptyset$ for all $i \neq j$, then $\{z_1, ..., z_r\}$ is linearly independent.
Now suppose $w \in Z(k[G])$, and write $w = \sum_{g \in G} a_g g$. Then for all $h \in G$, $hw = wh$, so $hwh^{-1} = w$. Then

$$\begin{aligned} \sum_{g \in G} a_g g &= w \\ &= hwh^{-1} \\ &= \sum_{g \in G} a_g hgh^{-1} \\ &= \sum_{g \in G} a_{hgh^{-1}} g \end{aligned}$$

Then by comparing coefficients, $a_g = a_{hgh^{-1}}$ for all $h \in G$. That is, for all g_1, g_2 which are conjugates of each other, $a_{g_1} = a_{g_2}$. Thus $w \in span(\{z_1, ..., z_r\}$, so $\{z_1, ..., z_r\}$ is a basis for $Z(k[G])$.

□

Proposition 39. Let G be a finite group, let $k = \overline{k}$ be a field such that $char\ K \nmid |G|$, and let $R = k[G]$. Let $I_1, ..., I_t$ be the distinct (up to isomorphism) simple left ideals of R. Then t is the number of conjugacy classes of G.

Proof. By the Theorem from last class, we can write $R = nI_1 \oplus ...n_tI_t$, where $n_i = \dim_k(I_i)$.

Then if we write $B(I_i) = \sum_{J \cong I_i} J$, then $R = B(I_1) \times ... \times B(I_t) \cong M_{n_1}(k) \times ... \times M_{n_t}(k)$.

Therefore $Z(R) = Z(M_{n_1}(k)) \times ... \times Z(M_{n_t}(k))$. One can verify that $Z(M_{n_i}(k)) = k1_{n_i}$ (the center of a matrix ring are the diagonals matrices with the same thing on the diagonal), so $Z(R) = k1_{n_1} \times ... \times k1_{n_t}$. Therefore a k-basis for $Z(R)$ is $\{\overline{1}_{n_1}, ...\overline{1}_{n_t}\}$ (where $\overline{1}_{n_i}$) represents the natural embedding of 1_{n_i} into R). Thus $\dim_k(Z(R)) = t$.

But by the previous theorem, another basis for $Z(R)$ is $\{z_1, ..., z_r\}$, so $\dim_k(Z(R)) = t = r$, where r is the number of conjugacy classes. □

Remark 57. (Standard Hypothesis) The next several theorems have a "standard hypothesis" that G is a finite group, k is an algebraically closed field, such that $char\ K \nmid |G|$, and $R = k[G]$. Recall that by a previous theorem, R is then semisimple. Recall also that we can write $R = n_1I_1 \oplus ... \oplus n_tI_t$.

Then we can summarize the previous results into the following theorem:

Theorem 63. Suppose the standard hypothesis holds. Then

1. $|G| = \sum_{i=1}^{t} n_i^2$.
2. t is the number of conjugacy classes of G.
3. t is the number of simple left ideals of $k[G]$.
4. If $I_1, .., I_t$ are the simple left ideals, then $n_i = \dim_k I_i$ and this equals the number of times I_i appears in a decomposition of $k[G]$ into simple left ideals.

Corollary 26. Suppose the standard hypothesis holds. Then the following are equivalent

1. G is abelian
2. $t = |G|$
3. $n_i = 1$ for all i

4. Every simple left ideal in R has dimension 1 over k.

Example 57. Let $G = S_3$ under the standard hypothesis. Then the conjugacy classes of G are $\{e\}, \{(12), (23), (13)\}, \{(123), (1$ so $t = 3$. Also, $|G| = 6 = n_1^2 + n_2^2 = n_3^2$. Therefore $n_1 = n_2 = 1$ and $n_3 = 2$. Then we can write $k[S_3] = I_1 \oplus I_2 \oplus 2I_2$, where I_1, I_2, I_3 are simple left ideals in R, and $\dim_k(I_1) = \dim_k(I_2) = 1$, but $\dim_k(I_3) = 2$.

21 Representaions of Finite Groups

Now let's talk about linear actions.

Definition 57. Let G be a group and let X be a set. An *action* of G on X is a map $G \times X \to X$ which we denote by $(g, u) \mapsto gu$ such that $(g_1g_2)u = g_1(g_2u)$ and $1u = u$ for all $u \in X$ and $g_1, g_2 \in G$.

If V is a vector space, a *linear action* of G on V is an action of G on V such that $g(u_1 + u_2) = gu_1 + gu_2$ and $g(ku) = k(gu)$ for all $g \in G$, $u \in V$, and $k \in K$.

Definition 58. Suppose G acts linearly on V. For each $g \in G$, let $\phi_g : V \to V$ by $u \mapsto gu$. Note that $(\phi_g)^{-1} = \phi_{g^{-1}}$. Then $\phi_g \in \mathrm{End}_k(V)* = GL_k(V)$ (this is the "general linear group").

Define $\rho : G \to GL_k(V)$ by $g \mapsto \phi_g$. Then ρ is a group homomorphism. We call ρ a *k-linear representation* of G.

Remark 58. Continuing the last definition, if $\rho : G \to GL_k(V)$ is a linear representation, we can define a linear action of G on V by $gu = \rho(g)(u)$.

Therefore k-linear representations of G are in correspondence with k-linear actions of G on V.

Remark 59. Given a linear representation of $\rho : G \to GL_k(V)$, we can define a $k[G]$-module M_ρ as follows:

The underlying set $M_\rho = V$ as a k-vector space. For $g \in G$ and $u \in M_rho$, we give the action of g on u by $gu = \rho(g)(u)$. We then linearly extend this to give an action of $k[G]$ on M_ρ.

This makes M_ρ into a $k[G]$-module.

Remark 60. Conversely, given a $k[G]$-module, we can make it into a group action. Let M be a $k[G]$-module. Let V_M be M as the underlying k-vector space. For $g \in G$, let $\phi_g : V_M \to V_m$ by $u \mapsto gu$. Then $\phi_g \in GL_k(V)$. Define $\rho_M : G \to GL_k(V)$ by $\rho(g) = \phi_g$.

Then one can verify that ρ_M is a k-linear representation of G.

Definition 59. Let $\rho : G \to GL_k(V)$ be a linear representation of G. we say ρ is *irreducible* if and only if M_rho is a simple $k[G]$-module.

Additionally, the *degree* of the representation ρ is $\dim_k(V) = \dim_k(M_\rho)$.

Remark 61. It follows immediately from the definitions that if ρ has degree 1, then ρ is irreducible.

Additionally, under the standard hypothesis, G is abelian if and only if every irreducible k-linear representation of G has degree 1.

21.1 Day 41 - December 7

Recall from last class that there are actions of groups on sets, and linear actions of groups on vector spaces. Also, linear actions of a G on a vector space are in natural correspondence with the module actions of $k[G]$ on that vector space. If ρ is our group action, then we use M_ρ to denote the group action. Alternatively, if M is our module action, then we use ρ_M to denote the corresponding group action.

Definition 60. Let ρ, ϕ be two k-linear representations of a group G. Let $\rho : G \to GL_k(V)$ and $\phi : G \to GL_k(W)$. An *isomorphism of representations* between ρ and ϕ is a k-vector space isomorphism $f : V \to W$ such that for all $g \in G$ and $u \in V$, $f(\rho(g)(u)) = \phi(f(u))$.

This is equivalent to f inducing a $k[G]$-module isomorphism between M_ρ and M_ϕ. In fact, we will use the fact that ρ and ϕ are isomorphic as representations if and only if M_ρ and M_ϕ are isomorphic as $k[G]$-modules.

Remark 62. Recall that if ρ is a representation, we say that ρ is irreducible if and only if M_ρ is simple as a $k[G]$ module. We also define $\deg(\rho) = \dim_k(M_rho)$.

From this it immediately follows that degree 1 representations are irreducible.

Definition 61. We define the direct sum of two representations as follows: if $\rho : G \to GL_k(V)$ and $\phi : G \to GL_k(W)$ are k-linear representations, then we say $\rho \oplus \phi : G \to GL_k(V \oplus W)$ by $g \mapsto (\rho \oplus \phi)(g) : (v, w) \mapsto (\rho(g)(v), \phi(g)(w))$.

As a matrix, we can represent this as $\begin{pmatrix} \rho(g) & 0 \\ 0 & \phi(g) \end{pmatrix}$.

Alternatively, one can "define" $\rho \oplus \phi$ by $M_{\rho\oplus\phi} = M_\rho \oplus M_\phi$.

Example 58. (Trivial representation) Let G be a group, and k be a field. Then define $\rho : G \to k^* = GL(k^1)$ by $g \mapsto 1$. Since $\deg \rho = \dim_k k = 1$, then ρ is irreducible.

Then $M_\rho = k$, and the module action is defined by $g\alpha = \alpha$ for all $g \in G$ and $\alpha \in k$.

Example 59. Let G be a finite group, and k is an algebraically closed field such that *char* $k \nmid |G|$. Let ρ be any representation of G. Then M_ρ is simple by a previous theorem [which one?], and since $k[G]$ is semisimple, then M_ρ is isomorphic to a simple left ideal. Let $w = \sum_{g\in G} g$. Then $hw = w$ for all $h \in G$ (since left multiplication by h simply permutes the elements of G).

Let $R = k[G]$, and $I = Rw$. Since $hw = w$ for all $h \in G$, then $Rw = kw$. Therefore I is a simple left ideal, so $I \cong M_\rho$. Therefore I is the simple left ideal corresponding to the trivial representation.

In fact, since $\dim I = 1$, then in the decomposition of $k[G]$ into the direct sum of simple left ideals, there is only one copy of an ideal isomorphic to I. That is, I is the unique simple left ideal isomorphic to the trivial representation.

Example 60. (Regular Representation) Let G be a group, and let k be a field. Let $V = \sum_{g\in G} kg = k[G]$ (as a k-vector space). Define $\rho : G \to GL_k(V)$ by $g \mapsto \phi_g$, where $\phi_g : V \to V$ is given by $u \mapsto gu$. That is, we have given ρ by $\rho = \rho_{k[G]}$.

Then $\deg \rho = \dim_k(k[G]) = |G|$. Then, given the standard hypothesis, ρ is irreducible if and only if $G = \{1\}$.

Under the standard hypothesis, we can write $k[G] \cong n_1 I_1 \oplus ... \oplus n_t I_t$ where the I_j are simple left ideals with $I_j \neq I_l$ for all $j \neq l$.

Then we can write $\rho = \rho_{k[G]} \cong n_1\rho_{I_1} \oplus ... \oplus n_t\rho_{I_t}$. Here, each ρ_{I_j} is irreducible since I_j is simple as a module.

Since every simple $k[G]$-module is isomorphic to one of the I_j, then every irreducible representation of G is isomorphic to one of the ρ_{I_j}s. Hence every irreducible representation of G occurs as a direct summand of the regular representation.

Example 61. (Cyclic groups) Let $G =< \alpha >\cong C_n$. Assume the standard hypothesis. To find the number of irreducible representations, it is the number of conjugacy classes. Since C_n is abelian, then this is simply n. But at the same time, $|G| = \sum_{i=1}^{t} n_i^2$, so each $n_i = 1$.

Then we can explicitly give the representations by $\rho_i : G \to GL_k(k) = k^*$ by $a \mapsto \lambda_i$. Since $a^n = 1$, then $\lambda_i^n = \rho_i(a)^n = 1$. Therefore, λ_i must be an n-th root of unity, and since *char* $k \nmid n$, there are n distinct roots of unity. Thus the representations are $a \mapsto \zeta_n^i$ where ζ_n is a primitive n-th root of unity and $1 \leq i \leq n$.

21.2 Day 42 - December 9

Let us continue our example from last class. Last time we dealt with it as a linear representation of a group, but we can do it with group rings instead. Let us do so now.

Example 62. (Cyclic groups) Let $G =< \alpha >\cong C_n$. Assume the standard hypothesis. Then define $\phi : k[x] \to k[G]$ by $x \mapsto a$, so $f(x) \mapsto f(a)$. Note that ϕ is surjective.

Note also that $x^n - 1 \in \ker \phi$, so we can mod out by $x^n - 1$. Then consider $\overline{\phi} : k[x]/(x^n - 1) \to k[G]$. Note that $\overline{\phi}$ is still surjective, and the dimensions on both sides are n. Therefore, since $\overline{\phi}$ is a k-linear transformation, it has no kernel as a linear transformation. Thus $\overline{\phi}$ is injective as a ring homomorphism. Thus $\overline{\phi}$ is a ring isomorphism.

But by the Chinese Remainder Theorem, $k[G] \cong k[x]/(x^n - 1) \cong k[x]/(x - \lambda_1) \times ... \times k[x]/(x - \lambda_n) \cong k \times ... \times k$.

Remark 63. For this statement, we used the Chinese Remainder Theorem, which is the following statement for rings:

Let R be a commutative ring, and let $I_1, ..., I_n$ be ideals in R such that $I_i + I_j = 1$ for $i \neq j$. Then $R/(I_1...I_n) = R/(I_1 \cap ... \cap I_n) \cong R/I_1 \times ... \times R/I_n$. Furthermore, this isomorphism is given by $\overline{r} \mapsto (\overline{r}, ...\overline{r})$.

Remark 64. Let $H \lhd G$ and let ρ be a representation for G/H. That is, $\rho : G/H \to GL_k(V)$ is a group homomorphism.

Then, if $\pi : G \to G/H$ is the natural projection, then $\overline{\rho} : G \to GL_k(V)$ is a group homomorphism. That is, it is a representation.

Claim 4. Let $H \lhd G$ and let ρ be a representation for G/H. Let $\overline{\rho} : G \to GL_k(V)$ be the induced representation on G. Then the ρ-submodules of V are exactly the $\overline{\rho}$-submodules of V.

Proof. Let W be a $k[G/H]$-module of V. Then $\overline{g}W \subset W$ for all $\overline{g} \in G$. But note that the action of g on W from the induced representation is given by $gW = \overline{g}W$. Therefore W is a $k[G]$ submodule of V. Similarly, if W is a $k[G]$ submodule of V, then W is a $k[G/H]$ submodule of V. □

Corollary 27. Let $H \lhd G$ and let ρ be a representation for G/H. Let $\overline{\rho} : G \to GL_k(V)$ be the induced representation on G. Then ρ is irreducible if and only if $\overline{\rho}$ is irreducible.

Proof. Recall that an irreducible representation is one with precisely two submodules, namely the whole space and the zero space. Since the ρ-submodules and $\overline{\rho}$-submodules are the same set, then ρ is irreducible if and only if $\overline{\rho}$ is irreducible. □

Remark 65. We have a special case if $H \lhd G$ such that $[G : H] = 2$. Then $G/H \cong C_2 =< \overline{\alpha} >$. Then there are exactly two one-dimensional representations, $\rho_1 : G/H \to k^*$ by $\overline{a} \mapsto 1$ and $\rho_2 : G/H \to k^*$ by $\overline{a} \mapsto -1$. This gives two irreducible representations of G, the trivial one $\overline{\rho}$ and also $\overline{\rho}_2 : G \to k^*$ by $g \mapsto \begin{cases} 1 \text{ if } g \in H \\ -1 \text{ if } g \notin H \end{cases}$.

Example 63. Let $G = S_n$ and $H = A_n$. Then $[S_n : A_n] = 2$, so the sign $sgn^* : S_n \to k^*$ by $\sigma \mapsto (-1)^{sgn \sigma}$ is the *sign representation.*

Remark 66. Let's do another construction of a representation. Let $H \leq G$ with $[G : H] = n$. Let $C_1, ..., C_n$ be the two left cosets of H in G. For each $i = 1, ..., n$, let $u_i = \sum_{g \in C_I} g$. For every $g \in G$, $gC_i = C_j$ for some j, so $gu_i = u_j$. Thus $I = ku_1 \oplus ... \oplus ku_n$ is a left ideal of $k[G]$. Then I is irreducible (if $n > 1$) since $k(u_1 + ... + u_n)$ is a left subideal. (Recall that $k(u_1 + ... + u_n)$ is the trivial representation.)

Example 64. Let $G = S_3$, and assume the standard hypothesis. Let t be the number of irreducible representations of G. Then t is the number of conjugacy classes of G, which happens to be 3 in this case. Since $\sum_{i=1}^{3} n_i^2 = 6$, then $n_1 = 1$, $n_2 = 1$, and $n_3 = 2$.

Let us consider the representations associated with each of these. For n_1, this is the trivial representation. For n_2, this is the sign representation, discussed earlier.

What about the $n_3 = 2$ representation? This would be a representation in dimension 2. Let $H =< (12) >$. Then we shall do the previous construction on $H \leq G$.

The three cosets of H are $C_1 = H$, $C_2 = (23)H$, and $C_3 = (13)H$. Let $u_i = \sum_{\sigma \in C_1} \sigma$. Then $I = ku_1 \oplus ku_2 \oplus ku_3 subsetk[S_3]$. Then, as before, $k(u_1 + u_2 + u_3)$ is an invariant submodule, so we can write $I = k(u_1 + u_2 + u_3) \oplus J$ for some invariant submodule J. Note that J is a left ideal of dimension 2.

We wish to show that J is irreducible. Note that if J does reduce, then it would reduce into one-dimensional representations. But we have already found all of the one-dimensional representations, and they had multiplicity one, so they can't appear again! Therefore J is irreducible.

Therefore $J \cong I/k(u_1 + u_2 + u_3) = k\overline{u}_1 \oplus k\overline{u}_2$ where $\overline{u}_3 = -\overline{u}_1 - \overline{u}_2$.

We can give this explicitly by $\phi : S_3 \to GL_k(k^2) = GL_2(k)$. Then $(12) \mapsto \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ and $(123) \mapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ and this defines what ϕ does for the whole group.

21.3 Day 43 - December 11

How do you do problems 3 and 4 on Test 2?

Claim 5. (Exam problem 3) Let R be a left Artinian ring. Then R has only finitely many two-sided ideals containing its Jacobson Radical.

Proof. Recall that for any ring R and any ideal I, there is a natural bijection between {ideals in R containing I} and {ideals in R/I}.

Then we can use this correspondence for the Jacobson radical $J(R)$, so consider the two-sided ideals in $R/J(R)$. Since R is left Artinian, then so is $R/J(R)$. Also, $J(R/J(R)) = 0$ for some reason. Therefore $R/J(R)$ is semisimple.

Then we can write $R/J(R) \cong M_{n_1}(D_1) \times ... \times M_{n_t}(D_t)$ as the product of matrix rings. But each matrix ring is simple, so it has only two left ideals. In the finite product, the ideals of the product are products of ideals, so there are 2^t two-sided ideals. □

Claim 6. (Exam problem 4) Let R be a left Artinian ring and let M, N be simple R-modules such that $\text{Ann}_R(M) \cong \text{Ann}_R(N)$. Then $M \cong N$.

Proof. Let $J = J(R)$. Then $JM = 0$ for all simple modules M. Therefore every simple module is an R/J module by the action $\overline{r} \cdot u = r \cdot u$.

One can verify that $M \cong N$ as R-modules if and only if $M \cong N$ as R/J-modules.

However, R/J is a semisimple ring for the same reasoning above. Therefore the problem reduces to the case of a semisimple ring. Therefore assume without loss of generality that R is semisimple.

It was a theorem that simple modules over semisimple rings are isomorphic to simple left ideals of the ring. That is, $M \cong I$ and $N \cong L$ for some simple left ideals of R.

Now consider the decomposition of R into matrix rings given by the Artin-Wedderburn Theorem. If $I \ncong L$, then they would have different annihilators, so $M \ncong N$. This is a contradiction, so $M \cong N$. □

Chapter 2

MATH 902

1 Representation Theory

1.1 Day 1 - January 11

What we'll cover this semester is representation theory, commutative algebra, and maybe a dash of category theory.

Definition 62. Let A be an $n \times n$ matrix with entries for a ring R (usually, R is commutative). Let the entries be denoted $A = [a_{i,j}]$. Then we say $\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{i,i}$ is the *trace* of the matrix.

Remark 67. One can easily verify the following facts:

1. $\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$.
2. $\mathrm{Tr}(cA) = cTr(A)$ for any $c \in R$.
3. If R is a commutative ring, then $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.
4. If R is a commutative ring, then $\mathrm{Tr}(PAP^{-1}) = \mathrm{Tr}(A)$ for all invertible matrices P.

Using these facts, we can make the following definition.

Definition 63. Let k be a field and let V be a finite dimensional k-vector space. For a linear transformation $f : V \to V$, define the *trace* of f to be $\mathrm{Tr}(f) := \mathrm{Tr}([f]_\beta)$ for any basis β of V. Note that the trace is independent of our choice of basis by part 4 of the previous remark.

Remark 68. From the previous remark, we get that $\mathrm{Tr} : \mathrm{End}_k(V) \to k$ is a linear functional.

Definition 64. Let k be a field, let R be a finite-dimensional k-algebra, and let M be a finitely generated (left) R-module. (Note that this implies that M is a finite dimensional k-vector space.)

For each $r \in R$, note that the map $r_m : M \to M$ by $u \mapsto ru$ is k-linear. Define the *character* χ_m (of R) associated to M by $\chi_m : R \to K$ by $r \mapsto \mathrm{Tr}(r_m)$.

We say that the *degree* of χ_m is $\dim_k M$.

Theorem 64. We have the following results:

1. $\chi_m(1) = \dim_k(M) \cdot 1_k$ (and if *char* $k = 0$ then this equals $\deg \chi_m$).
2. $\chi_m : R \to k$ is a linear functional.
3. If β is a k-basis for R, then χ_m is determined by $\chi_m\Big|_\beta$.

4. $\chi_{M\oplus N} = \chi_M + \chi_N$.

5. Suppose $M \cong N$ as R-modules. Then $\chi_M = \chi_N$.

Proof. (of part 2) $\chi_m(r+s) = \mathrm{Tr}((r+s)_m) = \mathrm{Tr}(r_m + s_m) = \mathrm{Tr}(r_m) + \mathrm{Tr}(s_m) = \chi_m(r) + \chi_m(s)$. Similarly, if $c \in k$, then $\chi_m(cr) = c\chi_m(r)$ for all $r \in R$. □

Proof. (of part 4) Identify M, N as submodules of $M \oplus N$, and let β_1 and β_2 be bases for M and N respectively. Then $\beta_1 \cup \beta_2$ is a basis for $M \oplus N$. Let $r \in R$. Then $[r_{M\oplus N}]_{\beta_1\cup\beta_2} = \begin{pmatrix} [r_M]_{\beta_1} & 0 \\ 0 & [r_N]_{\beta_2} \end{pmatrix}$. Thus $\mathrm{Tr}(r_{M\oplus N}) = \mathrm{Tr}(r_M) + \mathrm{Tr}(r_N)$. But at the same time the lefthand side equals $\chi_{M+N}(r)$ and the righthand side equals $\chi_M(r) + \chi_N(r)$. □

Proof. (of part 5) Let $\phi : M \to N$ be a k-linear isomorphism. Let β be a basis for M. Then $\phi(\beta)$ is a basis for N. Let $\beta = \{u_1, ..., u_n\}$. Let $r \in R$. Let $[r_M]_\beta = [a_{i,j}]$. Then $r_M(u_j) = ru_j = \sum_{j=1}^{n} a_{i,j}u_j$. If we apply ϕ to both sides, we get that $r_N(\phi(u_i)) = r\phi(u_i) = \phi(ru_i) = \sum_{j=1}^{n} a_{i,j}\phi(u_j)$.

Therefore $[r_N]_{\phi(\beta)} = [a_{i,j}]$. Hence $\chi_M(r) = \mathrm{Tr}(r_M) = \mathrm{Tr}(r_N) = \chi_N(r)$ for all $r \in R$. □

Example 65. Let $R = k[x]/(x^2)$ (note that R is not semisimple). Let $M = R$. A basis for R is $\beta = \{1, x\}$. Then $[1_M]_\beta = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $\chi_M(1) = 2$. Also, $[x_M]_\beta = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Thus $\chi_M(x) = 0$.

Let $N = R/(x) \oplus R/(x)$. Then $[1_N]_\beta = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $[x_N]_\beta = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Thus $\chi_M(1) = 2$ and $\chi_M(x) = 0$.

Therefore the characters of both of these are equal, but the modules are not isomorphic. After all, $xN = 0$, but $xM \neq 0$.

Proposition 40. Let R be a semisimple finite dimensional k-algebra such that *char* $k = 0$. Let M, N be finitely generated modules. Then $\chi_M = \chi_N$ if and only if $M \cong N$.

Proof. We have already shown that $M \cong N$ implies $\chi_M = \chi_N$.

Conversely, suppose $\chi_M = \chi_N$. Then let $R = n I_1 \oplus ... \oplus n_t I_t = B(I_1) \times ... \times B(I_t)$ where the I_j are distinct simple left ideals. Recall that this is the unique decomposition given by the Artin-Wedderburn theorem.

We can write $M \cong m_1 I_1 \oplus ... \oplus m_t I_t$ and $N \cong r_1 I_1 \oplus ... r_t I_t$. Then $M \cong N$ if and only if $m_i \cong r_i$.

Let e_i be the identity element of $B(I_i)$. Recall that $e_i I_j = 0$ for all $j \neq i$. Then $(e_i)_M : M \to M$ by $u \mapsto e_i u$. Therefore $(e_i)_M\Big|_{m_j I_j} = 0$ for $j \neq i$. However, $(e_i)_m\Big|_{m_i I_i} = 1_{m_i I_i}$. Thus $\chi_M(e_i) = (\dim_k(m_i I_i)) \cdot 1_k = m_i \dim_k(I_i) \cdot 1_k$.

Similarly, $\chi_N(e_i) = r_i \dim_k(I_i) \cdot k$. Then we can set these equal to zero, and since $1_k \neq 0$ and $\dim_k(I_i) \neq 0$, we can cancel by these and get that $m_i = r_i$. Since i was arbitrary, then $M \cong N$. □

Note that this makes us really excited. Now, a finitely generated semisimple ring is uniquely determined by its character.

Definition 65. Let R be a finite dimensional k-algebra. Then a *character* for R is a χ_M for some R-module M. A character $\chi \neq 0$ is *irreducible* if, whenever $\chi = \chi_1 + \chi_2$, with both the χ_is being characters, then either $\chi_1 = 0$ or $\chi_2 = 0$.

Corollary 28. Suppose R is a semisimple finite-dimensinal k-algebra with *char* $k = 0$. Then a character $\chi = \chi_M$ is irreducible if and only if M is simple.

Proof. Suppose $M = N_1 \oplus N_2$. Then $\chi_M = \chi_{N_1} + \chi_{N_2}$. Note that $\chi_{N_i} = 0$ if and only if $N_i = 0$. Therefore any decomposition of the character leads to a decomposition of the module, and vice versa. □

1.2 Day 2 - January 13

Recall the following theorem:

Theorem 65. Let R be a semisimple, finite-dimensional k-algebra (where k is an algebraically closed field of characteristic 0). Then $R \cong n_1 I_1 \oplus ... \oplus n_t I_t$ where $I_i \neq I_j$ for $i \neq j$. Let $\chi_i = \chi_{I_i}$ for $i = 1, ..., t$.

Then

1. $\{\chi_1, ..., \chi_t\}$ is the complete set of all irreducible characters from R.

2. Every character χ for R can be expressed uniquely in the form $m_1\chi_1 + ...m_t\chi_t$ where each $m_i \geq 0$.

3. $n_i = \chi_i(1)$.

4. $\chi_R = \chi_1(1)\chi_1 + ... + \chi_t(1)\chi_t$.

Proof. (Proof of 1) As proved last class, $\chi = \chi_M$ is irreducible if and only if M is simple. But this is the case if and only if $M \cong I_i$ for some i, and this is the case if and only if $\chi_M = \chi_{I_i}$ (since isomorphic modules have the same character). $\square$

(Proof of 2) Let $\chi = \chi_M$ where M is a finitely generated R-module. Then $M \cong m_1 I_1 \oplus ... \oplus m_t I_t$ for some $m_i \geq 0$. (This decomposition is unique by the Jordan-Holder Theorem). Then $\chi_M = m_1\chi_1 + ... + m_t\chi_t$. If $\chi_M = r_1\chi_1 + ... + r_t\chi_t$, then $M \cong r_1 I_1 \oplus ... \oplus r_t I_t$, so $m_i = r_i$ for all i. $\square$

(Proof of 3) Recall that $\chi_i(1)$ is the trace of the map given by left multiplication by 1. But this is the identity, and the trace of the identity is the dimension of the vector space. That is, $\chi_i(1) = \dim_k(I_i) = n_i$. $\square$

(Proof of 4) By decomposing R into the direct sum of simple modules and using the fact that $\chi_{M\oplus N} = \chi_M + \chi_N$, we get that $\chi_R = n_1\chi_1 + ...n_t\chi_t$. Then applying part 3, we know that $n_i = \chi_i(1)$, so $\chi_R = \chi_1(1)\chi_1 + ...\chi_t(1)\chi_t$, as desired. $\square$

Recall the following things about linear representations:

Remark 69. We will usually work under a common set of hypotheses: that k is a field, V is a finite dimensional vector space over k, G is a finite group, and $\rho : G \to GL_k(V)$ is a (k-linear) representation for G. The character χ_ρ of ρ is defined by $\chi_\rho : G \to k$ by $g \mapsto \text{Tr}(\rho(g))$.

Let M be the $k[G]$-module corresponding to ρ. That is, M has an underlying set equal to V, with the k-vector space structure. We define the action of G on M by ρ, thereby making M a $k[G]$-module. Then $\chi_\rho(g) = \chi_M(g)$, so we get a one-to-one correspondence between characters of $k[G]$ modules, and characters of k-linear representations of G.

Remark 70. We will often work under the following hypotheses:

Let k be an algebraically closed field. Let G be a finite group such that *char* $k \nmid \#G$. Then $k[G]$ is a semisimple ring, so we can decompose it into $k[G] = B(I_1) \times ... \times B(I_t) \cong n_1 I_1 \oplus ... \oplus n_t I_t$. Let $\chi_i = \chi_{I_i}$ for $i = 1, ..., t$.

Let $e_i \in B(I_i)$ be the identity element. Let $c_1, ..., c_t$ denote the distinct conjugacy classes of G. Let $m_i = |c_i|$, and let $z_i = \displaystyle\sum_{g \in c_i} g \in k[G]$. Then $Z(k[G]) = ke_1 \times ... \times ke_t = kz_1 \oplus ... \oplus kz_t$.

These hypotheses will be referred to by (#).

Theorem 66. Let χ be a character of a representation $\rho : G \to GL_k(V)$. Let $\sim$ denote the equivalence relation on G given by "is conjugate to". Then whenever $g \sim h$, then $\chi(g) = \chi(h)$. (Such functions are called *class functions*.)

Proof. If $g = xhx^{-1}$, then $\rho(g) = \rho(xhx^{-1}) = \rho(x)\rho(h)\rho(x^{-1})$. So $\chi(g) = \text{Tr}(\rho(g)) = \text{Tr}(\rho(h)) = \chi(h)$. $\square$

Lemma 25. Suppose (#). Let $\phi = \chi_{k[G]}$. Then $\phi(g) = \begin{cases} |G| \text{ if } g = 1 \\ 0 \text{ if } g \neq 1 \end{cases}$

Proof. Note that $\phi(g) = \chi_{k[G]}(g) = \mathrm{Tr}(g_{k[G]})$. We can use any basis, so let's use the basis given by the elements of g. If $g = 1$, then $g_{k[G]}$ is the identity, so $\phi(g) = |G|$. If $g \neq 1$, then $gh \neq h$ for all $h \in G$, so multiplication by g permutes the basis elements without fixed points. Thus the matrix corresponds to a permutation matrix with no 1s on the diagonal, so $\phi(g) = 0$. $\square$

Theorem 67. Suppose (#). Then

1. $e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$

2. $z_i = m_i \sum_{j=1}^{t} \frac{\chi_j(g)}{n_j} e_j$ for any $g \in c_i$.

Proof. (Proof of 1) Recall that $e_i \in k[G]$, so e_i can be written unique as a linear combination of elements of g. Thus let $e_i = \sum a_g g$ (where each $a_g \in k$. It suffices to show that $a_g = \frac{n_i}{|G|}\chi(g^{-1})$.

Let $h \in G$. Then, let $\phi = \chi_{k[G]}$, we have that $\phi(e_i h^{-1}) = \phi(\sum_{g \in G} a_g g h^{-1}) = \sum_{g \in G} a_g \phi(gh^{-1}) = a_h|G|$. But $e_i h^{-1} I_j = e_i I_j = 0$ when $j \neq i$. Thus $\chi_j(e_i h^{-1}) = 0$ for $j \neq i$.

But on the other hand,

$$\begin{aligned} \phi(e_i h^{-1}) &= (n_1\chi_1 + ... + n_t\chi_t)(e_i h^{-1}) \\ &= n_i \chi_i(e_i h^{-1}) \\ &= n_i \chi_i(h^{-1}) \end{aligned}$$

Thus $a_h|G| = n_i\chi(h^{-1})$, so $a_h = \frac{n_i}{|G|}\chi(h^{-1})$. $\square$

1.3 Day 3 - January 15

Recall the following set of hypotheses:

Remark 71. We will often work under the following hypotheses:

Let k be an algebraically closed field. Let G be a finite group such that *char* $k \nmid \#G$. Then $k[G]$ is a semisimple ring, so we can decompose it into $k[G] = B(I_1) \times ... \times B(I_t) \cong n_1 I_1 \oplus ... \oplus n_t I_t$. Let $\chi_i = \chi_{I_i}$ for $i = 1, ..., t$.

Let $e_i \in B(I_i)$ be the identity element. Let $c_1, ..., c_t$ denote the distinct conjugacy classes of G. Let $m_i = |c_i|$, and let $z_i = \sum_{g \in c_i} g \in k[G]$. Then $Z(k[G]) = ke_1 \times ... \times ke_t = kz_1 \oplus ... \oplus kz_t$.

These hypotheses will be referred to by (#).

Recall also this theorem, which we previously stated and proved the first half of:

Theorem 68. Suppose (#). Then

1. $e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$

2. $z_i = m_i \sum_{j=1}^{t} \frac{\chi_j(g)}{n_j} e_j$ for any $g \in c_i$.

We will now prove the second half of this theorem:

Proof. (Proof of 2) Note that from the first half of the theorem, since no e_i is 0, then $n_i \neq 0$ in k, since $e_i = \frac{n_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})g$. Thus $char\ k \nmid n_i$ for all i.

Since $z_i \in k[G] = n_1 I_1 \oplus ... \oplus n_t I_t$, then $z_i = \sum_{j=1}^{t} u_j e_j$ for some u_j. Then

$$\begin{aligned}
\chi_l(z_i) &= \chi_l(\sum_{j=1}^{t} u_j e_j) \\
&= \sum_{j=1}^{t} u_j \chi_l(e_j) \\
&= u_l \chi_l(e_l) \\
&= u_l n_l
\end{aligned}$$

Note that the penultimate equation is true since $\chi_l(e_j) = 0$ for all $j \neq l$, and that the last equation is true since $\chi_l(e_l) = \mathrm{Tr}(id_{I_l}) = \dim_k(I_l) = n_l$. Then $z_i = \sum_{g\in C_i} g$, so

$$\begin{aligned}
\chi_l(z_i) &= \chi_l(\sum_{g\in C_i} g) \\
&= \sum_{g\in C_i} \chi_l(g) \\
&= m_i \chi_l(g)
\end{aligned}$$

For any $g \in C_i$.

Therefore $u_l = \frac{m_i \chi_l(g)}{n_l}$, and this completes the proof. □

Corollary 29. Suppose (#). Then

1. For all $i, j \in \{1, ..., t\}$, we have that $\sum_{g\in G}\chi_i(g)\chi_j(g^{-1}) = \delta_{i,j}|G|$.

2. For all $g, h \in G$, we have that $\sum_{i=1}^{t}\chi_i(g)\chi_i(h^{-1}) = \delta_{g,h}|C_G(g)|$.

Proof. (Proof of 1) Recall that $e_i = \frac{n_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})g$, so $n_i\delta_{i,j} = \chi_j(e_i) = \frac{n_i}{|G|}\sum_{g\in G}\chi_i(g^{-1})\chi_k(g)$. By multiplying by $\frac{|G|}{n_i}$, we get the desired equation. □

(Proof of 2) Recall that

$$\begin{aligned}
z_i &= m_i \sum_{j=1}^{t} \frac{\chi_j(g)}{n_j} e_j \\
&= m_i \sum_{j=1}^{t} \frac{\chi_j(g)}{n_j}(\frac{n_j}{|G|}\sum_{h\in G}\chi_j(h^{-1})h) \\
&= \frac{m_i}{|G|}\sum_{h\in G}(\sum_{j=1}^{t}\chi_j(g)\chi_j(h^{-1}))h
\end{aligned}$$

Also, by definition we have that $z_i = \sum_{h \in C_i} h$, so we shall compare coefficients. By doing so, we get that if $h \in C_i$ (that is, if $g \sim h$), then $\frac{m_i}{|G|} \sum_{j=1}^{t} \chi_j(g)\chi_j(h^{-1}) = 1$, so $\sum_{j=1}^{t} \chi_j(g)\chi_j(h^{-1}) = \frac{|G|}{m_i} = |C_G(g)|$. On the other hand, if $h \notin C_i$, then $\sum_{j=1}^{t} \chi_j(g)\chi_j(h^{-1}) = 0$, as desired. $\square$

Remark 72. A special case of interest to us of part (2) in the corollary is that for all $g \neq 1$, $\sum_{j=1}^{t} \chi_j(g)\chi_j(1) = 0$.

Definition 66. A function $f : G \to k$ is called a (k-) *class function* if $f(g) = f(h)$ whenever $g \sim h$. Let $F_k(G) = \{f |\ f \text{ is a } k\text{-class function on } G\}$.

Then $F_k(G)$ is a k-vector space.

Remark 73. Let $f_i : G \to k$ be defined by $f_i(g) = 1$ if $g \in C_i$ and $f_i(g) = 0$ if $g \notin C_i$. Then $\{f_1, ..., f_t\}$ is a basis for $F_k(G)$. Therefore $\dim_k F_k(G) = t$ (that is, the dimension is the number of conjugacy classes of G).

Definition 67. Let V be a vector space, and $f : V \times V \to k$ be a function. We say f is a *bilinear form* if, whenever you fix one component, f is linear in the other component.

We say a bilinear form f is *symmetric* if $f(x, y) = f(y, x)$.

Definition 68. Suppose (#). Define the following bilinear form $(-,-) : F_k(G) \times F_k(G) \to K$ by $(\phi, \psi) = \frac{1}{|G|} \sum_{g \in G} \phi(g)\psi(g^{-1})$ for all $phi, \psi \in F_k(G)$. One can verify that this is also symmetric.

Proposition 41. Suppose (#). Then $(\chi_i, \chi_j) = \delta_{i,j}$, so $\{\chi_1, ..., \chi_t\}$ is a basis for $F_k(G)$.

Proof. Suppose $c_1\chi_1 + ... + c_t\chi_t = 0$. Then $0 = (\chi_i, 0) = (\chi_i, c_1\chi_1 + ... + c_t\chi_t) = \sum_{j=1}^{t} c_i(\chi_i, \chi_j) = c_i$. Therefore $\chi_1, ..., \chi_t$ is linearly independent. One call also verify that they are spanning, hence a basis. $\square$

Lemma 26. Suppose (#) and that $k = \mathbb{C}$. For all $i \in \{1, ..., t\}$ and $g \in G_i$, we have that $\chi_i(g^{-1}) = \overline{\chi_i(g)}$ (meaning the complex conjugate).

Proof. Recall that $\chi_i(g) = \mathrm{Tr}(g_{I_i})$. Let $n = |G|$. Since $g^n = 1$, then $(g_{I_i})^n = 1_{I_i}$. Hence, the minimal polynomial of g_{I_i} divides $x^n - 1$, and thus has distinct roots. Hence g_{I_i} is diagonalizable as a matrix, so $g_{I_i} \sim \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_r \end{pmatrix}$, where each λ_r is a distinct n-th root of unity, and $r = \dim_C I_i$. Let l_j be the integers such that $\lambda_j = e^{\frac{2\pi i l_j}{n}}$. Then $\lambda_j^{-1} = e^{-2\pi i l_j} n = \overline{\lambda_j}$.

Then $\mathrm{Tr}(g_{I_i}^{-1}) = \lambda_1^{-1} + ... + \lambda_r^{-1} = \overline{\lambda_1} + ... + \overline{\lambda_r} = \bar{(}\chi_i(g))$.

Definition 69. Suppose (#) and let $k = \mathbb{C}$. We can define the *Hermitian inner product* $< -,- >$: $F_{\mathbb{C}}(G) \times F_{\mathbb{C}}(G) \to \mathbb{C}$ by $< \phi, \psi >= \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)}$.

Remark 74. The Hermitian inner product has some perks. It is sesquilinear. We have that $< \phi, \phi >= 0$ if and only if $\phi = 0$. Also, $< \phi, \psi >= \overline{< \psi, \phi >}$.

This is an inner product.

Proposition 42. Suppose (#) and that $k = \mathbb{C}$. Then $< \chi_i, \chi_j >= \delta_{i,j}$.

Proof. Note that $<\chi_i,\chi_j>=\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)}=\dfrac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_j(g^{-1})=(\chi_i,\chi_j)=\delta_{i,j}$. $\square$

From this we can conclude that $\{\chi_1,...,\chi_t\}$ are in fact an orthonormal basis for $F_{\mathbb{C}}(G)$.

1.4 Day 4 - January 20

We are now working under the following assumptions:

Let G be a finite group, $k=\mathbb{C}$, $\chi_1,...\chi_t$ the set of irreducible characters of G. For $\phi,\psi\in F_{\mathbb{C}}(G)$ (the set of class functions), we define $<\phi,\psi>=\frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)}$. Then we have that $<\chi_i,\chi_j>=\delta_{i,j}$.

Let $\phi:G\to GL_n(\mathbb{C})$. Let $\chi(g)=\text{Tr}(\phi(g))$. If χ is a character of a representation of G, then $\chi=m_1\chi_1+...+m_t\chi_t$ where $m_i\geq 0$ and $m_i\in\mathbb{Z}$ for all i. Furthermore, $m_i=<\chi,\chi_i>$,

Also, $<\chi,\chi>=m_1^2+...+m_t^2$, so $<\chi,\chi>=1$ if and only if $\chi=\chi_i$ for some i.

We can now move onto character tables. This is a table of characters χ_i and elements of conjugacy classes g_j, whose entries are $\chi_i(g_j)$.

	1	g_1	...	g_{t-1}
χ_1	1	1	...	1
χ_2	n_2			
$\vdots$				
χ_t	n_t			

Example 66. Let $G=C_3=<a>$. Then there are 3 conjugacy classes of elements in G, so $t=3$. Thus there are 3 irreducible representations, all of degree 1. If $\omega=e^{\frac{2\pi i}{3}}$, then they are given by $\phi_j:C_3\to GL_1(\mathbb{C})=\mathbb{C}^*$ by $a\mapsto\omega^j$. Then $\chi_j(a)=\text{Tr}(\phi_j(a))=\omega_j$. Then the character table is

	1	a	a^2
χ_0	1	1	1
χ_1	1	ω	ω^2
χ_2	1	ω^2	ω

Note that columns are always orthogonal because of the orthogonality relation.

Example 67. Let $G=V_4=\{1,a,b,c\}$, the Klein 4-group. Recall that if $H\lhd G$ and $\overline{\rho}:G/H\to GL_n(\mathbb{C})$ is a representation, then $\rho:G\to GL_n(\mathbb{C})$ given by $\rho:G\xrightarrow{\pi}G/H\xrightarrow{\overline{\rho}}GL_n(\mathbb{C})$ is also a representation. Furthermore, ρ is irreducible if and only if $\overline{\rho}$ is irreducible.

In our case, let $H=<a>$. Then $G/H\cong C_2$, so let $\overline{r}ho:G/H\to\mathbb{C}^*$ by $\overline{b}\mapsto -1$. Then the induced representation $\rho:G\to\mathbb{C}^*$ is given by $1\mapsto 1$, $a\mapsto 1$, $b\mapsto -1$ and $c\mapsto -1$. Then let us make our character table:

	1	a	b	c
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

Example 68. Let $G=S_3$. Then there are 3 conjugacy classes (corresponding to 1-cycles, 2-cycles, and 3-cycles). This gives us the following table:

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

The second row corresponds to modding out by (123) to get C_2, and the last row comes from orthogonality with the previous ones.

Remark 75. Unfortunately, there exist distinct groups with the same character table. We will talk about what they are later (after the homework).

Example 69. Let $G = A_4$. Then $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ is normal in G. Then there are four conjugacy classes: $(1), H \setminus \{1\}, (123)H$, and $(132)H$. We can then build the following character table:

	1	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

(Where ω is a primitive 3rd root of unity. The first three rows are given by the three representations of $G/H \cong C_3$. The last one is given by the columns' orthogonality relation.

1.5 Day 5 - January 22

Let's do the character table for the quaternions!

Example 70. Let $G = Q_8$ (the quaternion group). The conjugacy classes of G are $\{1\}$, $\{-1\}$, $\{\pm i\}$, $\{\pm j\}$ and $\{\pm k\}$. Since $H = Z(G) = \{\pm 1\} \lhd G$, then we get characters from $G/H \cong V_4$. This gives us three characters, and we get the trivial character for free. Then the final row can be computed by the orthogonality relation.

	1	-1	i	j	k
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

In fact, χ_5 is the charcter from the representation of $\rho : Q_8 \to GL_2(\mathbb{C})$ by $i \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $j \to 0ii0$ and $k \to \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$.

Example 71. Let $G = S_4$. The conjugacy classes are the distinct cycle types (represented by) $(1), (12), (12)(34), (123), (1234)$. We will find characters by looking at a normal subgroup. Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Then $H \lhd S_4$. Furthermore, S_4 has no elements of order 6, so S_4/H has no element of order 6. Therefore $S_4/H \cong S_3$. From last class, we know that S_3 has three conjugacy classes, giving us three characters for free.

Also, we know that the sum of the squares of the first column add up to 24, and the first three entries are 1,1,2, so the last two entries must be 3, 3. This gives us:

	1	(12)	(123)	(12)(34)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3				
χ_5	3				

We can get another representation from the action of S_4 on $V = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3 \oplus \mathbb{C}e_4$ by $\sigma : e_1 \to e_{\sigma(i)}$. Note that $W = \mathbb{C}(e_1 + e_2 + e_3 + e_4)$ is fixed under σ, so let's instead consider the action of G on $V/W = \mathbb{C}\overline{e_1} \oplus \mathbb{C}\overline{e_2} \oplus \mathbb{C}\overline{e_3}$. Then this gives another representation, which happens to be irreducible because its inner product with itself is 1. The last row we can get by orthogonality relations. Thus we get this completed character table:

	1	(12)	(123)	(12)(34)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	-1	1

2 Spectrum of a Ring

We now emerge from group theory to commutative algebra!

Let R be a commutative ring with unity with $1 \neq 0$.

Definition 70. An ideal $\mathfrak{p} \neq R$ is *prime* if for all $a, b \in R$ such that $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Remark 76. One can show that $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is a domain.

Exercise 18. If $\mathfrak{p}$ is a prime ideal and $\mathfrak{p} \supseteq I_1 \cap ... \cap I_n$, then $\mathfrak{p} \supseteq I_i$ for some i.

From this, prove that if $\mathfrak{p} \supset I_1 I_2 ... I_n$, then $\mathfrak{p} \supset I_i$ for some i. In particular, if $\mathfrak{p} \supset I^n$, then $\mathfrak{p} \supset I$.

Exercise 19. Show that maximal ideals are prime.

Definition 71. The *prime spectrum* of R is $Spec\ R = \{\mathfrak{p} | \mathfrak{p}$ is a prime ideal of $R\}$.

Example 72. Let F be a field. Then $Spec\ F = \{0\}$. If R is a ring with $Spec\ R = \{0\}$, then in fact R is a field.

Also, $(0) \in Spec\ R$ if and only if R is a domain.

Example 73. $Spec\ \mathbb{Z} = \{(0)\} \cup \{(p) | p \in \mathbb{Z}$ is a prime number$\}$.

Let F be a field. Then $Spec\ F[x] = \{(0)\} \cup \{(f(x)) | f(x) \in F[x]$ is irreducible$\}$.

2.1 Day 6 - January 24

Recall from last class the definition of a prime ideal, and the definition of the spectrum of a ring.

Proposition 43. Let R be a ring, and $a_1, ..., a_n \in R$. Define $\phi : R[x_1, ..., x_n] \to R$ by $f(x_1, ..., x_n) \mapsto f(a_1, ..., a_n)$. Then ϕ is a surjective ring homomorphism and $\ker \phi = (x_1 - a_1, ..., x_n - a_n)$, and $R[x_1, ..., x_n]/(x_1 - a_1, ..., x_n - a_n) \cong R$.

Proof. Certainly, $(x_1 - a_1, ..., x_n - a_n) \subset \ker \phi$. To show the other direction, we will use induction on n.

For $n = 1$, $f(x) \in R[x]$, so by the division algorithm, $f(x) = (x - a)g(x) + r$ for some $r \in R$. Then $f(a) = 0$ if and only if $r = 0$. Therefore $f(a) = 0$ if and only if $f(x) \in (x - a)$.

For the inductive case, suppose the claim holds for $n - 1$. Suppose $f(x_1, ..., x_n) \in R[x_1, ..., x_n]$ and that $f(a_1, ..., a_n) = 0$. Let $g(x_1) = f(x_1, ..., a_2, ..., a_n) \in R[x_1]$. Then $g(a_1) = 0$. By the $n = 1$ case, $g(x_1) = (x_1 - a_1)\ell(x_1)$.

Consider $h(x_2, ..., x_n) = f(x_1, ..., x_n) - g(x_1) \in S[x_2, ..., x_n]$, where $S = R[x_1]$. Then $h(a_2, ..., a_n) = (x_1, a_2, ..., a_n) - g(x_1) = 0$. By the $n - 1$ case applied to S, we get that $h(x_2, ..., x_n) \in (x_2 - a_2, ..., x_n - a_n)S[x_2, ..., x_n]$.

Therefore $f(x_1, ..., x_n) - g(x_1) = (x_2 - a_2)u_2(\underline{x}) + ... + (x_n - a_n)u(\underline{x})$. Therefore $f(x_1, ..., x_n) = (x_1 - a_1)l(x_1) + ... + (x_n - a_n)u_n(\underline{x}) \in (x_1 - a_1, ..., x_n - a_n)$.

Thus $\ker \phi = (x_1 - a_1, ..., x_n - a_n)$. The remainder of this theorem follows from the first isomorphism theorem. $\square$

Corollary 30. Let k be a field. For any $c_1, ..., c_n \in k$, we have that $(x_1 - c_1, ..., x_n - c_n) = \{f(x_1, ..., x_n) \in k[x_1, ..., x_n] | f(c_1, ..., c_n) = 0\}$, and that this ideal is maximal in $k[x_1, ..., x_n]$.

Remark 77. If k is an algebraically closed field, then every maximal ideal of $k[x_1, ..., x_n]$ has this form (this is the Nullstellensatz).

Exercise 20. For any $c_1, ..., c_m \in k$ (with $m \leq n$), we have that $(x_1 - c_1, ..., x_m - c_m)$ is a prime ideal of $k[x_1, ..., x_n]$. (In fact, $k[x_1, ..., x_n](x_1 - c_1, ..., x_m - c_m) \cong k[x_{m+1}, ..., x_n]$.

Example 74. From the previous results, we have that $\operatorname{Spec} \mathbb{C}[x, y] = \{(0)\} \cup \{(x - c, y - d) | c, d \in \mathbb{C}\} \cup \{(f(x, y)) | f(x, y)$ irred$\}$.

Definition 72. For $p \in \operatorname{Spec} R$, define the *height* of p by $ht(p) = \sup\{n |$there exists a chain in $\operatorname{Spec} R$ with $p = p_n \supsetneq ... \supsetneq p_0\}$

Example 75. In $\mathbb{C}[x, y]$, we have that $ht((x, y) \geq 2$ as $(x, y) \supset (x) \supset (0)$. On the other hand, $ht(x) \geq 1$ since $(x) \supset (0)$.

Definition 73. Let R be a ring. The *dimension* of R is $\dim R = \sup\{ht(p) | p \in \operatorname{Spec} R\}$.

Definition 74. Let I be an ideal of R. Define $V(I) = \{p \in \operatorname{Spec} R | p \supset I\}$.

Proposition 44. Let I, J, and I_α be ideals in a ring R. Then

1. $V(I) \cup V(J) = V(I \cap J)$.
2. $\bigcap_{\alpha \in \Lambda} V(I_\alpha) = V(\sum_{\alpha \in \Lambda} I_\alpha)$.
3. $V((0)) = \operatorname{Spec} R$, and $V(R) = \emptyset$.

Definition 75. We can define the *Zariski topology* on $\operatorname{Spec} R$ by saying a set $F \subset \operatorname{Spec} R$ is closed if and only if $F = V(I)$ for some ideal I. The fact that this satisfies the axioms of a topology is given in the previous proposition.

Proposition 45. The Zariski Topology is T_0 but not T_1 (in general).

Proof. Let $p \neq q \in \operatorname{Spec} R = X$ be two distinct ideals in $\operatorname{Spec} R$. Then one of these ideals does not contain the other, so let $p \subsetneq q$. Let $U = X \setminus V(p)$. Then $p \notin U$, but $q \in U$. Thus the Zariski topology is T_0.

However, if $p \supset q$, every open set containing q also contains p, so X is not T_1. □

Proposition 46. The Zariski topology is compact (although sometimes this is called "semi-compact" because algebraists use outdated terminology).

Proof. Let $X = \bigcup_{\alpha \in \Lambda} U_\alpha$, where each $U_\alpha = X \setminus V(I_\alpha)$ for some ideal I_α.

Then the fact that the U_α cover X implies that $\cap_\alpha V(I_\alpha) = \emptyset$, and by a previous proposition, then $V(\sum I_\alpha) = \emptyset$. Since every proper ideal is contained in a maximal ideal (and maximal ideals are prime), then it must be that $\sum I_\alpha = R$.

Thus $1 \in \sum I_\alpha$, so $1 = i_{\alpha_1} + ... i_{\alpha_n}$ for some $\alpha_1, ..., \alpha_n \in \Lambda$. Thus $\sum_{i=1}^{n} I_{\alpha_i} = R$, so $V(\sum_{i=1}^{n} I_{\alpha_i}) = \emptyset$. Thus $\cap V(I_{\alpha_i}) = \emptyset$, so $X = \bigcup_{i=1}^{n} U_{\alpha_i}$. □

Definition 76. A nonempty subset S of R is *multiplicatively closed* if for all $a, b \in S$, $ab \in S$.

Proposition 47. Let S be a multiplicatively closed set of R and assume $0 \notin S$. Then there exists a $p \in \operatorname{Spec} R$ such that $p \cap S = \emptyset$.

Proof. Let $\Lambda = \{I | I \text{ is an ideal} I \cap S = \emptyset\}$. Note that $(0) \in \Lambda$, so $\Lambda \neq \emptyset$. Note that Λ is partially ordered by subset.

Also, if $\mathcal{C}$ is a chain in Λ, then $I_{\mathcal{C}} = \bigcup_{I \in \mathcal{C}} I$ is an ideal. It is also disjoint from S, so $I_{\mathcal{C}} \in \Lambda$. Finally, $I_{\mathcal{C}}$ is an upper bound of $\mathcal{C}$.

Thus Zorn's lemma applies to $\mathcal{C}$. Let p be a maximal element in Λ. We wish to show that p is a prime ideal.

Suppose for the sake of contradiciton it is not. Then [something] and we get a contradiction. □

2.2 Day 7 - January 27

Recall from last class the following theorem:

Proposition 48. Let S be a multiplicatively closed set of R and assume $0 \notin S$. Then there exists a $\mathfrak{p} \in \operatorname{Spec} R$ such that $\mathfrak{p} \cap S = \emptyset$.

We can use this to prove (one of) Krull's Theorem(s):

Theorem 69 (Krull's Theorem). Let R be a commutative ring. Then $Nilrad(R) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} p$.

Proof. Let $x \in Nilradical(R)$. Then $x^n = 0 \in \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Spec} R$. But since $\mathfrak{p}$ is prime and $x \cdot x \cdot \ldots \cdot x \in \mathfrak{p}$, then $x \in \mathfrak{p}$. Thus $x \in \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} p$.

Conversely, suppose $x \notin Nilrad(R)$. Then $0 \notin S = \{x^n\}_{n \geq 1}$. By the proposition, there exists a $\mathfrak{p} \in \operatorname{Spec} R$ such that $\mathfrak{p} \cap S = \emptyset$, so $x \notin \mathfrak{p}$.

$\square$

Proposition 49. Let R be a commutative ring, and let $I \neq R$ be an ideal in R. Then the map $f : V(I) \to Spec(R/I)$ by $\mathfrak{p} \mapsto \mathfrak{p}/I$ is a bijection. (In fact, f is a homeomorphism).

Definition 77. Let I be an ideal in a ring R. Then the *radical* of I is $\sqrt{I} = \{r \in R | \ r^n \in I \text{ for some } n \in \mathbb{N}\}$.

This theorem is also called Krull's theorem:

Theorem 70. Let I be an ideal in a ring R. Then $\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$.

Proof. Observe that $\sqrt{I}/I = \sqrt{(\overline{0})}$, where $(\overline{0})$ is I/I in R/I.

Then by Krull's theorem about nilradicals and the previous proposition, $\sqrt{I}/I = \sqrt{(\overline{0})} = \cap_{\mathfrak{p} \in V(I)} \mathfrak{p}/I = (\cap_{\mathfrak{p} \in V(I)} \mathfrak{p})/I$. Then by lifting to R, we can see that $\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$ $\square$

Definition 78. Let $\mathfrak{p} \in \operatorname{Spec} R$. We say $\mathfrak{p}$ is a *minimal prime* of R if $ht(\mathfrak{p}) = 0$.

We denote the set of minimal primes by $Min_R(R) = \{\mathfrak{p} \in \operatorname{Spec} R | \ ht(\mathfrak{p}) = 0\}$.

Let I be an ideal of a ring R, $\mathfrak{p} \in \operatorname{Spec} R$, and suppose $I \subset \mathfrak{p}$. Then we say $\mathfrak{p}$ is *minimal over* I if $ht(\mathfrak{p}/I) = 0$.

We denote the set of minimal primes over I by $Min_R(R/I) = \{\mathfrak{p} \in V(I) | ht(\mathfrak{p}/I) = 0\}$.

Exercise 21. Let R be a commutative ring, and let I be an ideal of R with $I \neq R$. Let $\mathfrak{p} \in V(I)$. Then $\mathfrak{p} \supset \mathfrak{q}$ for all $\mathfrak{q} \in Min_R(R/I)$.

Proof. We apply Zorn's lemma to $\Lambda = \{\mathfrak{q} \in V(I) | \mathfrak{q} \subset \mathfrak{p}\}$ (with the partial order of reverse inclusion). $\square$

Corollary 31. If I is a proper ideal of a ring R, then $\sqrt{I} = \bigcap_{\mathfrak{p} \in Min_R(R/I)} \mathfrak{p}$.

Exercise 22. If R is Noetherian, then $Min_R(R/I)$ is a finite set.

Remark 78. By combining the previous exercise and previous corollary, we get that in a Noetherian ring, each proper radical ideal is the finite intersection of prime ideals.

Theorem 71. Let R be a commutative ring, and let $X = \operatorname{Spec} R$. Then X is connected if and only if R has no nontrivial idempotents. (A trivial idempotent is 0 and 1).

Proof. Recall that X is disconnected if and only if it can be partitioned into two open sets. But if those sets are both open, then they are both closed.

Thus X is disconnected if and only if $X = V(I) \cup V(J)$, where $V(I)$ and $V(J)$ are nonempty and disjoint. But if they are disjoint then $\emptyset = V(I) \cap V(J) = V(I + J)$. Since $V(I + J) = \emptyset$, then $I + J = R$. But since $V(I)$ and $V(J)$ are nonempty, then $I \neq R$ and $J \neq R$.

Furthermore, $X = V(I) \cup V(J) = V(IJ)$. Thus $X = V(IJ)$, so every prime ideal contains IJ. Thus $IJ \subset \sqrt{(0)}$.

Thus we have translated the topological property of disconnectedness into finding two ideals I, J such that $I \neq R$, $J \neq R$, and $I + J = R$, and $IJ \subset \sqrt{(0)}$. We now wish to show that the existence of such ideals is equivalent to the existence of nontrivial idempotents.

Suppose that e is a nontrivial idempotent. Then $e^2 = e$. Furthermore, $1 - e$ is also an idempotent. Let $I = (e)$ and $J = (1 - e)$. Note that $I = R$ if and only if e is a unit. But $e^2 = e$, so if e were a unit, then $e = 1$. Since e is a nontrivial idempotent, this is not the case, so $I \neq R$. Similarly, since $1 - e$ is a nontrivial idempotent, then $J \neq R$. Furthermore, $1 = e + (1 - e$, so $1 \in I + J$. Thus $R = I + J$. Finally, $IJ = (e)(1 - e) = (e(1 - e)) = (0) \subset \sqrt{(0)}$.

Conversely, suppose we have two ideals satisfying the previously described properties. Then $R = I + J$, so $1 = i + j$. Since $ij \in IJ \subset \sqrt{(0)}$, then there exists an $n \in \mathbb{N}$ such that $(ij)^n = 0$.

Consider the ideal $(i^n) + (j^n)$. If this ideal were strictly contained in R, there would be a maximal ideal $\mathfrak{m}$ such that $(i^n) + (j^m) \subset \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, it is prime, and since $i^n \in \mathfrak{m}$, then so is i. Similarly, $j \in \mathfrak{m}$, so $R = (i) + (j) \subset \mathfrak{m}$. This is a contradiction of the fact that $\mathfrak{m}$ is a maximal ideal, so we know that $(i^n) + (j^n) = R$.

Thus $1 = ri^n + sj^n$ for some $r, s \in R$. Let $e = ri^n$. Then $e(1 - e) = (ri^n)(sj^n) = rs(ij)^n = 0$. Thus $e^2 = e$. However, if $e = 1$, then $1 \in I$. If $e = 0$, then $1 = 1 - e \in J$. Either way, this is a contradiction. Thus e is a nontrivial idempotent.

□

Example 76. If R is a domain, then it has no nontrivial idempotents, so its spectrum is connected.

If $R = R_1 \times R_2$, where both R_1 and R_2 are rings with unit, then R has nontrivial idempotents (such as $(1, 0)$), so its spectrum is disconnected.

If R is a local ring then R is connected.

Exercise 23. Show that if R is a local ring, then $\operatorname{Spec} R$ is connected.

Proposition 50. If R is a ring, and e is an idempotent in R, then $\phi : R \to (e) \times (1-e)$ by $r \mapsto (re, r(1-e))$ is an isomorphism of rings. (Note that (e) is indeed a ring with unit, because e acts as the multiplicative identity on it.)

From this we can conclude that a ring R has a disconnected spectrum if and only if it can be factored into the product of two rings with unit.

2.3 Day 8 - January 29

Theorem 72. Let R be a commutative ring. Then R is Artinian if and only if R is Noetherian and $\dim R = 0$.

Proof. Suppose R is Artinian. Then we have already shown that R is Noetherian. We then have to show that R has dimension 0. Recall that the dimension of a ring is the length of a maximal chain of prime ideals. Therefore a ring is dimension 0 if and only if no prime ideals are contained in any other prime ideals.

To this end, let $\mathfrak{p}$ be a prime ideal. Then $R/\mathfrak{p}$ is a domain. Furthermore, since R is Artinian, then $R/\mathfrak{p}$ is as well. We have previously proven that Artinian domains are fields, so $R/\mathfrak{p}$ is a field. Thus $/p$ is a maximal ideal. Thus no prime ideal contains another one, so $\dim R = 0$.

Conversely, suppose R is Noetherian and that $\dim R = 0$. Therefore $\operatorname{Spec} R = \min R = \max R$. Since R is Noetherian, then by homework problem #5 on problem set 2 [edit: see immediately below], $\min R$ is finite.

Then let $\operatorname{Spec} R = \{\mathfrak{m}_1, ..., \mathfrak{m}_t\}$ (where each $\mathfrak{m}_i$ is maximal and minimal).

Let $J = \cap_{i=1}^t \mathfrak{m}_i$. Then J is both the Jacobson radical (the intersection of maximal ideals) and the Nilradical (the intersection of prime ideals) of R.

Note that for $i \neq j$, we have that $\mathfrak{m}_i + \mathfrak{m}_j = R$. Therefore by the Chinese Remainder Theorem, we have that $R/J = R/(\mathfrak{m}_1 \cap ... \cap \mathfrak{m}_t) \cong R/\mathfrak{m}_1 \times ... \times R/\mathfrak{m}_t$ as rings. Since the righthand side is the finite product of fields, then R/J is semisimple, so it is Artinian.

We now wish to show that R/J^i is Artinian for all i, using induction on i.. We have just shown this claim is true for $i = 1$, completing the base case. Now suppose R/J^{i-1} is Artinian. Then consider the R/J-module J^{i-1}/J^i. Since R is Noetherian, then J^i is finitely generated. Hence J^{i-1}/J^i is also finitely generated. Since R/J is semismiple, then J^{i-1}/J^i has finite length. Hence J^{i-1}/J^i is Artinian.

Furthermore, the sequence $0 \to J^{i-1}/J^i \to R/J^i \to R/J^{i-1} \to 0$. is exact. Then since J^{i-1}/J^i is Artinian, and R/J^{i-1} is Artinian by induction, then so is R/J^i (as an R-module). Therefore R/J^i is Artinian as a ring.

But J is finitely generated, so let $J = (a_1, ..., a_n)$. Since J is also the nilradical, then there exist n_i such that $a_i^{n_i} = 0$. Let $n = \sum n_i$. Then $J^n = 0$, so $R/J \cong R$. Thus R is Artinian.

□

Homework Problem 8. *Let R be a Noetherian ring, and let I be a proper ideal of R. The the set of minimal primes over I is finite.*

Example 77. Consider $R = \mathbb{Z}/100\mathbb{Z}$. Since $\mathbb{Z}$ is Noetherian, so is R. Recall that $\dim \mathbb{Z} = 1$, but all such chains contained (0). Since (0) is not a prime ideal in R, then $\dim \mathbb{Z}/(100) = 0$, so it is Artinian.

3 Localization

Let's talk about localization.

Definition 79. Let R be a commutative ring (with $1 \neq 0$). Let S be a multiplicatively closed set of R. Let $R \times S = \{(r,s) | r \in R, s \in S\}$. Define a relation $\sim$ on $R \times S$ by $(r_1, s_1) \sim (r_2, s_2)$ if and only if there exists $t \in S$ such that $t(s_2 r_1 - s_1 r_2) = 0$ (or equivalently $ts_2 r_1 = ts_1 r_2$).

Proposition 51. The relation $\sim$ defined above is an equivalence relation.

Proof. We will only verify transitivity (the other two properties are easy to check).

Suppose $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$. Then there exists a $t \in S$ such that $ts_2 r_1 = ts_1 r_2$, and there exists a $u \in S$ such that $us_3 r_2 = us_2 r_3$.

Let $p = uts_2$. Since $u, t, s_2 \in S$, and S is multiplicatively closed, then $p \in S$. Furthermore,

$$\begin{aligned} ps_3 r_1 &= uts_2 s_3 r_1 \\ &= us_3(ts_2 r_1) \\ &= us_3(ts_1 r_2) \\ &= ts_1(us_3 r_2) \\ &= ts_1(us_2 r_3) \\ &= uts_2(s_1 r_3) \\ &= ps_1 r_3 \end{aligned}$$

Thus $(r_1, s_1) \sim (r_3, s_3)$.

□

Remark 79. We will use $\frac{r}{s}$ to denote the equivalence class of (r, s).

Definition 80. Let $R_S = \{\frac{r}{s} | r \in R, s \in S\}$. Sometimes we instead denote this by $S^{-1}R$.

We furthermore define two operations on R_S by $\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}$, and $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$. One can verify that these operations are well-defined.

Theorem 73. The two operations given above make R_S a commutative ring with identity.

Remark 80. From now on, we will assume that $1 \in S$. We will usually assume $0 \notin S$, but it will be possible for this to be the case.

Remark 81. If $x \in R$, and we let $s = \{x^n\}_{n \geq 0}$, then we will write R_x for R_S.

If $\mathfrak{p} \in \operatorname{Spec} R$, then we write R_p for R_S, where $S = R \setminus \mathfrak{p}$.

Example 78. Let $R = \mathbb{Z}$, and let $S = \{2^n\}_{n \geq 0}$. Then $\mathbb{Z}_2 = \{\frac{a}{2^n} | a \in \mathbb{Z}, n \geq 0\} \subset \mathbb{Q}$.

Also, $\mathbb{Z}_{(2)} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \text{ is odd}\} \subset \mathbb{Q}$.

Example 79. Let $R = \mathbb{Z}/(6)\mathbb{Z}$. Let $S = \{2^n\}_{n \geq 0}$. Then $_S = \{\frac{a}{2^n} | a \in \mathbb{Z}/(6), n \geq 0\}$. Then we can do a lot of collapsing, and show that $R_S \cong \mathbb{Z}/(3)$.

3.1 Day 9 - February 1

Recall that if R is a commutative ring, and S is a multiplicatively closed set, then we use R_S to denote the ring of fractions.

Recall that we, without loss of generality, let $1 \in S$.

Remark 82. We have a natural map $\phi : R \to R_S$ by $r \mapsto \frac{r}{1}$.

Note that this map may have nontrivial kernel, as $\ker \phi = \{r \in R | \text{ there exists } t \in S \text{ such that } \mathrm{Tr} = 0\}$.

Therefore ϕ is injective if and only if S contains no zero divisors.

Remark 83. All of these constructions work in the noncommutative case, so long as $S \subset Z(R)$.

Proposition 52. Let R be a ring, and let S be a multiplicatively closed set in R. Let $f : R \to T$ be a ring homomorphism such that $f(s)$ is a unit for all $s \in S$.

Then there exists a unique ring homomorphism $\psi : R_S \to T$ such that the $\psi \circ \phi = f$, where ϕ is the natural map as before.

Proof. "Define" $\psi(\frac{r}{s}) = f(r)f(s)^{-1}$. We wish to show that this is well defined.

Suppose $\frac{r_1}{s_1} = \frac{r_2}{s_2}$. Then there exists $t \in s$ such that $ts_2r_1 = ts_1r_2$. Then $f(t)f(s_2)f(r_1) = f(t)f(s_1)f(r_2)$. By multiplying both sides by $f(t)^{-1}f(s_1)^{-1}f(s_2)^{-1}$, then we get that $f(r_1)f(s_1)^{-1} = f(r_2)f(s_2)^{-1}$. Thus ψ is well defined.

One can then verify that ψ is a ring homomorphism.

Suppose that another ψ' meets the required properties. Then for all $r \in R$ and $s \in S$,

$$\begin{aligned} f(r) &= \psi'(\frac{r}{1}) \\ &= \psi'(\frac{s}{1} \cdot \frac{r}{s}) \\ &= \psi'(\frac{s}{1}) \cdot \psi'(\frac{r}{s}) \\ &= f(s)\psi'(\frac{r}{s}) \end{aligned}$$

Since $f(s)$ is a unit in T, then $\psi'(\frac{r}{s}) = f(r)f(s)^{-1} = \frac{f(r)}{f(s)}$. That is, $\psi' = \psi$. This completes the proof of uniqueness. $\square$

Exercise 24. Suppose $g : R \to A$ is a ring homomorphism with the following propoerty: given any $f : R \to T$ such that $f(s)$ is a unit for all $s \in S$, there exists a unique homomorphism $\psi : A \to T$ such that $f = \psi \circ g$. Then there exists a unique isomorphism $h : R_S \to A$ such that $g = \phi \circ h$.

Remark 84. We use the following notation:

If $f(R) \to T$ is a ring homomorphism, then T is naturally an R-module via $r \cdot t := f(r)t$. If I is an ideal of R, then $IT = \{\sum i_k t_k | i_k \in I, t_k \in T\}$ is an ideal of T. In particular, IT is the ideal of T generated by $f(I)$.

Proposition 53. Let S be a multiplicatively closed set of R. Let I be an ideal of R, and let $\phi : R \to R_S$ be the canonical map. Define $I_S := \{\frac{i}{s} | i \in I, s \in S\}$. Then

1. $I_S = IR_S$ (so I_S is an ideal of R_S)

2. Every ideal of R_S is of the form I_S, for some $I \lhd R$

3. $I_S = R_S$ if and only if $I \cap S \neq \emptyset$.

Proof. (Proof of (1)) Let $\frac{i}{s} \in I_S$, wher $i \in I_S$ and $s \in S$. Then $\frac{i}{s} = i \cdot \frac{1}{s}$. Since $i \in I$ and $\frac{1}{s} \in R_S$, then $\frac{i}{s} \in IR_S$. Thus $I_S \subset IR_S$.

Let $\sum i_k \dfrac{r_k}{s_k} \in IR_S$, where each $i_k \in I$, each $r_k \in R$, and each $s_k \in S$. Without loss of generality, we can change everything to a common denominator, so $s_i = s_j$ for all i and j. Then we will call all denominators s. Then $\sum i_k \dfrac{r_k}{s_k} = \dfrac{\sum i_k r_k}{s} \in I_S$. Thus $I_S = IR_S$. □

(Proof of (2)) Let J be an ideal of R_S. Let $I = \phi^{-1}(J) = \{a \in R | \frac{a}{1} \in J\}$. We wish to show that $I_S = J$. If $\frac{i}{s} \in I_S$, where $i \in I$ and $s \in S$, then $\frac{i}{1} \in J$, so $\frac{i}{s} = \frac{1}{s}\frac{i}{1} \in J$. Thus $I_S \subset J$. Conversely, let $\frac{r}{s} \in J$. Then $\frac{r}{1} = \frac{s}{1}\frac{r}{s} \in J$. Therefore $r \in I$, so $\frac{r}{s} \in I_S$. Thus $I_S = J$. □

(Proof of (3)) Suppose $I_S = R_S$. Then $\frac{1}{1} \in I_S$, so $\frac{1}{1} = \frac{i}{s}$ for some $i \in I$ and $s \in S$. Therefore there exists a $t \in S$ such that $ti = ts$. Then $ti \in I$ and $ts \in S$, so $ti \in I \cap S$. Thus $I \cap S \neq \emptyset$. Conversely, if $i \in I \cap S$, then $1 = \frac{i}{i} \in I_S$, so $I_S = R_S$. □

Example 80. Ideals of R_S are always of the form I_S, but the ideal I which makes this happen might not be unique. For instance, if $R = S = \mathbb{Z}$, then $R_S \cong \{0\}$, and every ideal in R maps down to the same ideal in R_S.

Corollary 32. If R is Noetherian, so is R_S for any multiplicatively closed set S.

Proof. Let J be in ideal of R. Then $J = I_S = IR_S$ for some ideal I of R. Since R is Noetherian, then $I = (a_1, ..., a_n)R$. Therefore $J = (a_1, ..., a_n)R_S = (\frac{a_1}{1}, ..., \frac{a_n}{1})$. Thus J is finitely generated. □

Exercise 25. If R is Artinian, so is R_S for all multiplicatively closed sets S.

Exercise 26. If S consists of units, then the map $R \to R_S$ by $r \mapsto \frac{r}{1}$.is an isomorphism.

Proposition 54. Let R be a commutative ring, let S be a multiplicatively closed set, and let I be an ideal in R. Let $\overline{S} = \{\overline{s} + I | s \in S\}$. Then $\overline{S}$ is a multiplicatively closed set of R/I. Then the map $R_S/I_S \to (R/I)_{\overline{S}}$ by $\frac{\overline{r}}{s} \mapsto \frac{\overline{r}}{\overline{s}}$ is an isomorphism.

Proof. Let $\pi : R \to R/I$ by $r \mapsto \overline{r}$, and let $\phi : R/I \to (R/I)_{\overline{S}}$. Then, by composition, $f = \phi \circ \pi$ is a ring homomorphism, and $f(s) = \overline{s}$ is a unit for all $s \in S$. x‘ By the universal property that we proved earlier, there exists a $\psi : R_S \to (R/I)_{\overline{S}}$ where $\psi(\frac{r}{s}) = \frac{f(r)}{f(s)} = \frac{\overline{r}}{\overline{s}}$. Furthermore, ψ is a surjective ring homomorphism. Then one can show that $\ker \psi = I_S$, so by the first isomorphism theorem, we know that $R_S/I_S \cong (R/I)_{\overline{S}}$. □

3.2 Day 10 - February 3

Recall the following notation: if R is a ring, and S is multiplicatively closed set, then R_S is R localized at S, and $\phi : R \to R_S$ is the natural map given by $r \mapsto \frac{r}{1}$.

Proposition 55. Let J be an ideal of R_S. Then $\phi^{-1}(J)_S = J$.

Proof. Let $\frac{r}{s} \in J$. Then $\frac{r}{1} \in J$, so $r \in \phi^{-1}(J)$, so $\frac{r}{s} \in \phi^{-1}(J)_S$. Thus $J \subset \phi^{-1}(J)_S$.

Conversely, if $\frac{r}{s} \in \phi^{-1}(J)_S$, then without loss of generality we can assume $r \in \phi^{-1}(J)$. Then $\frac{r}{1} \in J$, so $\frac{r}{s} \in J$. Thus $J = \phi^{-1}(J)_S$. □

Remark 85. Let $\mathfrak{q} \in \operatorname{Spec} R_S$. Then $\phi^{-1}(q) \in \operatorname{Spec} R$.

Proposition 56. With the notation as above, there is an inclusion-preserving bijection between $\{\mathfrak{p} \in \operatorname{Spec} R | p \cap S = \emptyset\} \leftrightarrow \operatorname{Spec} R_S$ given by $\mathfrak{p} \mapsto \mathfrak{p}_S$ and $q \mapsto \phi^{-1}(\mathfrak{q})$.

Proof. If $\mathfrak{q} \in \operatorname{Spec} R_S$, then $\phi^{-1}(\mathfrak{q}) \in \operatorname{Spec} R$ by the second remark. Convervsely, if $\phi^{-1}(\mathfrak{q}) \cap S \neq \emptyset$, let $s \in \phi^{-1}(\mathfrak{q}) \cap S$. Then $\frac{s}{1} \in \mathfrak{q}$, so $q = R_S$, as $\frac{s}{1}$ is a unit. Thus prime ideals (and only prime ideals) in R_S are taken to prime ideals in R which are disjoint from S.

Suppose instead that $\mathfrak{p} \in \operatorname{Spec} R$, and $\mathfrak{p} \cap S = \emptyset$. Notice that $R_S/\mathfrak{p}_S \cong (R/\mathfrak{p})_{\overline{S}}$, where $\overline{S} = \{s + \mathfrak{p} | s \in S\}$. As $P \cap S = \emptyset$, then $\overline{0} \notin \overline{S}$.

Since $R/\mathfrak{p}$ is a domain, then $(R/\mathfrak{p})_{\overline{S}}$ is a subring of the field of fractions of $R/\mathfrak{p}$. Hence $(R/\mathfrak{p})_{\overline{S}}$ is a domain, so $\mathfrak{p}_S$ is a prime ideal.

It follows directly from the definition that these maps are inclusion preserving.

Also, we proved in the previous proposition that $\phi^{-1}(\mathfrak{q})_S = \mathfrak{q}$. It therefore suffices to show that $\phi^{-1}(\mathfrak{p}_S) = \mathfrak{p}$. To this end, let $a \in \mathfrak{p}$. Then $\frac{a}{1} \in \mathfrak{p}_S$, so $a \in \phi^{-1}(\mathfrak{p}_S)$. Now let $b \in \phi^{-1}(\mathfrak{p}_S)$. Then $\frac{b}{1} \in \mathfrak{p}_S$, so $\frac{b}{1} = \frac{a}{s}$ for some $a \in \mathfrak{p}, s \in S$. Therefore there exists $t \in S$ such that $tsb = ta \in \mathfrak{p}$. Since $ts \in S$, then $ts \notin \mathfrak{p}$, so $b \in \mathfrak{p}$. □

Remark 86. This map above, given by $\mathfrak{p} \mapsto \mathfrak{p}_S$ is a homeomorphism (for the Zariski topology).

Remark 87. We have a special case when $S = R \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal. Recall that $R_\mathfrak{p}$ denotes R_S. Then $q \cap S = \emptyset$ if and only if $q \subset \mathfrak{p}$. Then $\operatorname{Spec} R_\mathfrak{p} = \{\mathfrak{q}_\mathfrak{p} = \mathfrak{q}R_\mathfrak{p} | \mathfrak{q} \in \operatorname{Spec} R, \mathfrak{q} \subset \mathfrak{p}\}$. Thus $R_\mathfrak{p}$ has a unique maximal ideal, namely $\mathfrak{p}_\mathfrak{p} = \mathfrak{p}R_S$.

Furthermore, $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong (R/\mathfrak{p})_{\overline{\mathfrak{p}}} = (R/\mathfrak{p})_{(\overline{0})}$. This is the field of fractions of $R/\mathfrak{p}$.

Definition 81. A *quasi-local* ring is a commutative ring R with a unique maximal ideal $\mathfrak{m}$. To emphasize this, we write it as $(R, \mathfrak{m})$.

The *residue field* of R is $R/\mathfrak{m}$.

A *local* ring is a ring which is both Noetherian and quasi-local.

Example 81. If R is Noetherian, then $R_\mathfrak{p}$ is a local ring for all $\mathfrak{p} \in \operatorname{Spec} R$.

Example 82. With $R = \mathbb{Z}$ and $\mathfrak{p} = (2)$, then $\operatorname{Spec} \mathbb{Z}_{(2)} = \{(0)_{(2)}, (2)_{(2)}\}$. Therefore $\mathbb{Z}_{(2)}$ is a local ring.

Definition 82. *(Localization of a module)* Let M be an R-module, and let S be a multiplicatively closed subset of R. Let $\Lambda = \{(m, s) | m \in M, s \in S\}$. Define a relation $\sim$ on Λ by $(m_1, s_1) \sim (m_2, s_2)$ if there exists a $t \in S$ such that $t(s_2 m_1 - s_1 m_2) = 0$.

By the same proofs as before, $\sim$ is an equivalence relation. Let $\frac{m}{s}$ denote the equivalence class of (m, s).

Then let M_S (sometimes instead denoted by $S^{-1}M$ be the set $\{\frac{m}{s} | m \in M, s \in S\}$.

We then define $\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$, and $\frac{r_1}{s_1} \cdot \frac{m}{s} = \frac{r_1 m}{s_1 s}$. These are well-defined, thereby making M_S and R_S-module.

Proposition 57. Let M be an R-module. Then the following are equivalent:

1. $M = 0$
2. $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec} R$
3. $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$.

Definition 83. We will often use colon-ideals: if I and J are ideals of R, then $(J :_R I) = \{r \in R | rI \subset J\}$. It is a theorem that $(J :_R I)$ is an ideal of R containing J.

Proof. $(1 \Rightarrow 2,\ 2 \Rightarrow 3)$ Certainly, if $M = 0$, then $M_\mathfrak{p} = 0$ for all ideals $\mathfrak{p}$, including the prime ones. This (1) implies (2). Since every maximal ideal is prime, then (2) implies (3).

It then suffices to show that (3) implies (1). To this end, suppose $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$. Let $x \in M$. Then whenever $\mathfrak{m}$ is a maximal ideal of R, $\frac{x}{1} \in M_\mathfrak{m} = \{\frac{0}{1}\}$, so there exists a $t_\mathfrak{m} \in R \setminus \mathfrak{m}$ such that $t_\mathfrak{m} x = 0$.

But $\operatorname{Ann}_R(x) = \{r \in R | rx = 0\}$ is an ideal of R. Therefore $t_\mathfrak{m} \in \operatorname{Ann}_R(x)$ for all $\mathfrak{m}$, so $\operatorname{Ann}_R(x) \not\subset \mathfrak{m}$ for all $\mathfrak{m}$. But the only ideal not contained in any maximal ideal is R itself. Thus $\operatorname{Ann}_R(x) = R$, so $x = 0$. Thus $M = 0$.

□

Theorem 74 (Nakayama's Lemma). Let $(R, \mathfrak{m})$ be a quasi-local ring. Then $\mathfrak{m}$ is the Jacobson radical of R. Let M be a finite generated R-module. Then the following are all referred to as Nakayama's Lemma:

1. $M = 0$ if and only if $M = \mathfrak{m}M$.
2. If $N \subset M$ then $M = N$ if and only if $M = N + \mathfrak{m}M$.

3. For $x_1, ..., x_n \in M$, we have that $x_1, ..., x_n$ generate M if and only if $\overline{x}_1, ..., \overline{x}_n$ spans $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space.
4. $M = Rx_1 + ...Rx_n$ if and only if $\{x_1, ..., x_n\}$ contains a basis for $M/\mathfrak{m}M$. Therefore $\mu_R(M) = \dim_{R/\mathfrak{m}} M/\mathfrak{m}M$. (Recall that $\mu_R(M)$ denotes the minimal number of generators for M as an R-module.)

Definition 84. We say $\{x_1, ..., x_n\}$ is a *minimal generating set* for M if $M = Rx_1 + ... + Rx_n$ and $n = \mu_R(M)$.

Proposition 58. Let $(R, \mathfrak{m})$ be a quasi-local ring, and let P be a finitely-generated projective module. Then P is a free R-module (that is, $P \cong \mathbb{R}^n$ for some $n \in \mathbb{N}$).

Proof. Since P is finitely generated, then let $n = \mu_R(P) = \dim_{R/\mathfrak{m}}(P/\mathfrak{m}P)$. Let $x_1, ..., x_n$ be a minimal generating set for P.

Define $\phi : R^n \to P$ in the natural way. That is, $\phi : e_i \mapsto x_i$. Certainly, this is a surjective ring homomorphism.

Let $K = \ker\phi$. Then we get a short exact sequence

$$0 \to K \to R^n \xrightarrow{\phi} P \to 0$$

Then by a theorem about projective modules, the sequence splits. Thus $R^n \cong P \oplus K$. Then $R^n/\mathfrak{m}R^n \cong (P \oplus K)/\mathfrak{m}(P \oplus K)$. Therefore $(R/\mathfrak{m})^n = P/\mathfrak{m}P \oplus K/\mathfrak{m}K$. By comparing dimensions, we have that $\dim K/\mathfrak{m}K = 0$, so $K = \mathfrak{m}K$, so $K = 0$ by Nakayama's Lemma. $\square$

3.3 Day 11 - February 5

When life gives you Lemmas, make Lemma-nade!

(All of these lemmas will be stated without proof, but are easy to prove. Also, they will be stated for modules, but they can also be applied directly to rings.)

Lemma 27. Let S be a multiplicatively closed set of a commutative ring R. Then

1. $\left(\bigoplus_\alpha M_\alpha\right)_S \cong \bigoplus_\alpha (M_\alpha)_S$ (as R_S-modules).
2. Suppose $S \subset T$, where T is also a multiplicatively closed set. Then $(M_S)_{\frac{T}{S}} \cong M_T$ as R_T-modules (where $\frac{T}{S} = \{\frac{t}{s} | t \in T, s \in S\}$.
3. For $a, b \in R$, $M_{ab} \cong (M_a)_{\frac{b}{1}}$ as R_{ab}-modules.
4. For $a \in R$, $M_a \cong M_{a^n}$. (This could be considered a corollary to the previous result.)
5. Let $\mathfrak{q} \subset \mathfrak{p}$ be prime ideals. Then $R \setminus p \subset R \setminus q$, so $(M_\mathfrak{p})_{\mathfrak{q}_\mathfrak{p}} \cong M_\mathfrak{q}$.

This lemma is pretty important:

Lemma 28. Let M be an R-module, and let S be a multiplicatively closed set. Then,

1. If $\operatorname{Ann}_R M \cap S \neq \emptyset$, then $M_S = 0$.
2. If M is finitely generated, then the converse to 1 holds. That is, if $M_S = 0$, then $\operatorname{Ann}_R M \cap S \neq \emptyset$.

Proof. Suppose $\operatorname{Ann}_R M \cap S \neq \emptyset$. Then there exists some $s \in \operatorname{Ann}_R M \cap S$. That is, there exists an $s \in S$ such that $sM = 0$. Then $s \cdot m \cdot 1 = s \cdot 0 \cdot t$ for all $m \in M$ and $t \in S$, so $\frac{m}{t} = \frac{0}{1}$. Thus $M_S = 0$.

Conversely, if M is finitely generated, we can write $M = Rx_1 + ... + Rx_n$. Then $\frac{x_i}{1} = 0$ in M_S for all i. Therefore, for each x_i, there exists $s_i \in S$, such that $s_i x_i = 0$. Let $s = s_1 ... s_n$. Then $s \in S$ and $sx_i = 0$ for all i. Therefore $sM = 0$. $\square$

Let's look at some not-finitely-generated examples where this fails.

Example 83. Let $R = \mathbb{Z}$, and let $M = \bigoplus_{n \geq 1} \mathbb{Z}/(2^n)$. Then $\operatorname{Ann}_{\mathbb{Z}} M = 0$, but $M_2 = 0$.

Example 84. Let $R = k[x]$ (for some field k). Then let $M = k[x, x^{-1}]/k[x]$. Then $\operatorname{Ann}_R M = 0$, but $M_x = 0$.

Proposition 59. Let R be a commutative ring, S be a multiplicatively closed subset, and let P be a projective R-module. Then P_S is a projective R_S-module.

Proof. Since P is projective, there exists an R-module such that$Q$ such that $P \oplus Q \cong \sum_{\alpha} R$. Then $P_S \oplus Q_S \cong \oplus_\alpha R_S$. Therefore P_S is a direct summand of a free R_S-module. In other words, P_S is a projective R_S-module. $\square$

Note that usually P_S will not be a projective R-module.

Corollary 33. Let P be a finitely generated projective R-module. Then for all $\mathfrak{q} \in \operatorname{Spec} R$, $P_\mathfrak{q}$ is a free $R_\mathfrak{q}$-module.

Proof. By the previous proposition, $P_\mathfrak{q}$ is a finitely generated $R_\mathfrak{q}$-module. But finitely generated projectives over quasi-local rings are always free. $\square$

Remark 88. If F is a finitely generated free R-module, then $F \cong R^n$ for a unique number n. We call n the *rank* of F, and write $n = \operatorname{rk} F$.

Combining these two results, for each finitely generated projective P, we have a function $f_P : \operatorname{Spec} R \to \mathbb{N}_0$ by $\mathfrak{q} \mapsto \operatorname{rk} P_\mathfrak{q}$.

Remark 89. If $f : M \to N$ is an R-homomorphism and S is a multiplicatively closed set, then $\frac{f}{1} : M_S \to N_S$ defined by $\frac{f}{1}(\frac{m}{s}) = \frac{f(m)}{s}$ is an R_S-homomorphism.

Note also that $\frac{f}{1} \circ \frac{g}{1} = \frac{fg}{1}$. Also note that $\frac{1_M}{1} = 1_{M_S}$.

These properties combined make localization a functor.

Proposition 60. (Localization is exact) If $L \xrightarrow{f} M \xrightarrow{g} N$ is exact, then so is $L_S \xrightarrow{\frac{f}{1}} M_S \xrightarrow{\frac{g}{1}} N_S$ (where R is a commutative ring, S is a multiplicatively closed subset of R, and L, M, and N are R-modules).

Proof. We know that $\frac{g}{f} = 0$, so $\frac{g}{1} \circ \frac{f}{1} = \frac{gf}{1} = 0$. Thus $\operatorname{im} \frac{g}{1} \subset \ker \frac{g}{1}$.

Suppose $\frac{m}{s} \in \ker \frac{g}{1}$. That is, $\frac{g(m)}{s} = 0$, so there exists a $t \in S$ such that $tg(m) = 0$. Since g is an R-module homomorphism, then $g(tm) = 0$. Thus $tm \in \ker g = \operatorname{im} f$. That is, there exists an $l \in L$ such that $f(l) = tm$. Then $\frac{f}{1}(\frac{l}{st}) = \frac{f(l)}{st} = \frac{tm}{st} = \frac{m}{s}$. Hence $\operatorname{im} \frac{f}{1} \supset \ker \frac{g}{1}$.

Thus $\operatorname{im} \frac{f}{1} = \ker \frac{g}{1}$, so the sequence is exact. $\square$

Remark 90. Recall that we use $V(I)$ to denote the set $\{\mathfrak{p} \in \operatorname{Spec} R | \mathfrak{p} \supset I\}$. Then every closed set is $V(I)$ for some I, but we don't have a similar notation for open sets.

We can (partially) fix that: for $a \in R$, let $D(a) = \operatorname{Spec} R \setminus V((a)) = \{\mathfrak{p} \in \operatorname{Spec} R | a \notin \mathfrak{p}\}$. Then $D(a)$ is open.

Theorem 75. Let P be a finitely generated projective R-module. Give $\mathbb{N}_0$ the discrete topology. Then the map $f : \operatorname{Spec} R \to \mathbb{N}_0$ by $\mathfrak{q} \mapsto \operatorname{rk} P_\mathfrak{q}$ is continuous.

Proof. Since $\mathbb{N}_0$ has the discrete topology, then the singletons are a basis for the open sets. Therefore continuity is equivalent to the preimage of every singleton being open.

Let $n \in \mathbb{N}_0$. If $f^{-1}(n) = \emptyset$, then this is open, so suppose instead that $f^{-1}(n) \neq \emptyset$. Then let $\mathfrak{q} \in f^{-1}(n)$. We'll show that there exists an $a \in R$ such that $\mathfrak{q} \in D(a) \subset f^{-1}(n)$.

Since $\operatorname{rk} P_\mathfrak{q} = n$, then $P_\mathfrak{q} \cong R_\mathfrak{q}^n$. Then let $\{\frac{u_1}{s_1}, ..., \frac{u_n}{s_n}\}$ be an $R_\mathfrak{q}$-basis for $P_\mathfrak{q}$. Then each $s_i \notin \mathfrak{q}$ for all i. However, bases are invariant under multiplication by unit scalars, then $\{\frac{u_1}{1}, ..., \frac{u_n}{1}\}$ is also a basis.

Define $\phi : R^n \to P$ by $e_i \to u_i$. Then $\frac{\phi}{1} : R_\mathfrak{q}^n \to P_\mathfrak{q}$ is an isomorphism. Let $K = \ker \phi$, and let $C = \operatorname{coker} \phi = P/\operatorname{im} \phi$.

Since $\frac{\phi}{1}$ is exact, then $K_\mathfrak{q} = C_\mathfrak{q} = 0$. Since P is finitely generated, then so is C. By the lemma, we know that $\operatorname{Ann}_R C \cap R \setminus \mathfrak{q} \neq \emptyset$. That is, there exists a $b \notin \mathfrak{q}$ such that $bC = 0$. Thus $C_b = 0$.

[Proof to be finished later.] $\square$

3.4 Day 12 - February 8

Recall from last class that we had started the following proof:

Theorem 76. Let P be a finitely generated projective R-module. Give $\mathbb{N}_0$ the discrete topology. Then the map $f : \operatorname{Spec} R \to \mathbb{N}_0$ by $\mathfrak{q} \mapsto \operatorname{rk} P_\mathfrak{q}$ is continuous.

Proof. Since $\mathbb{N}_0$ has the discrete topology, then the singletons are a basis for the open sets. Therefore continuity is equivalent to the preimage of every singleton being open.

Let $n \in \mathbb{N}_0$. If $f^{-1}(n) = \emptyset$, then this is open, so suppose instead that $f^{-1}(n) \neq \emptyset$. Then let $\mathfrak{q} \in f^{-1}(n)$. We'll show that there exists an $a \in R$ such that $\mathfrak{q} \in D(a) \subset f^{-1}(n)$.

Since $\operatorname{rk} P_\mathfrak{q} = n$, then $P_\mathfrak{q} \cong R_\mathfrak{q}^n$. Then let $\{\frac{u_1}{s_1}, ..., \frac{u_n}{s_n}\}$ be an $R_\mathfrak{q}$-basis for $P_\mathfrak{q}$. Then each $s_i \notin \mathfrak{q}$ for all i. However, bases are invariant under multiplication by unit scalars, then $\{\frac{u_1}{1}, ..., \frac{u_n}{1}\}$ is also a basis.

Define $\phi : R^n \to P$ by $e_i \to u_i$. Then $\frac{\phi}{1} : R_\mathfrak{q}^n \to P_\mathfrak{q}$ is an isomorphism. Let $K = \ker \phi$, and let $C = \operatorname{coker} \phi = P/\operatorname{im} \phi$.

That is, we have the exact sequence $0 \to K \to R^n \xrightarrow{\phi} P \to C \to 0$.

Since $\frac{\phi}{1}$ is exact, then $K_\mathfrak{q} = C_\mathfrak{q} = 0$. Since P is finitely generated, then so is C. By the lemma, we know that $\operatorname{Ann}_R C \cap R \setminus \mathfrak{q} \neq \emptyset$. That is, there exists a $b \notin \mathfrak{q}$ such that $bC = 0$. Thus $C_b = 0$.

Then by localizing the above exact sequence, we get that $0 \to K_b \to R_b^n \to P_b \to 0 \to 0$.

[This is where we stopped last time.]

From a theorem from last class, since P is projective as an R-module, then P_b is also projective as an R_b-module.

Therefore K_b is finitely generated. Note that $(K_b)_{\mathfrak{q}_b} \cong K_\mathfrak{q} = 0$. Then, since K_b is finitely generated, then by the lemma there exists a $\frac{c}{b^n} \in R_b \setminus \mathfrak{q}_b$ such that $\frac{c}{b^n} K_b = 0$. Thus $\frac{c}{1} K_b = 0$.

Thus $(K_b)_{\frac{c}{1}} = 0$. But since localization is associative, we know that $K_{bc} = 0$. Let $a = bc$. Since $b \notin \mathfrak{q}$ and $c \notin \mathfrak{q}$, and $\mathfrak{q}$ is a prime ideal, then $a \notin \mathfrak{q}$. Therefore $K_a = 0$ and $C_a = (C_b)_{\frac{c}{1}} = 0$.

Suppose $\mathfrak{p} \in D(a)$. Then $\mathfrak{p}_a \in \operatorname{Spec} R_a$, so $P_\mathfrak{p} \cong (P_a)_{\mathfrak{p}_a}$. Since $K_a = C_a = 0$, then the exact sequence localized at a is $0 \to R_a^n \to P_a \to$. Thus $P_a \cong R_a^n$. Substituting this in, we get that $P_\mathfrak{p} \cong (R_a^n)_{\mathfrak{p}_a} \cong R_\mathfrak{p}^n$. Thus $\operatorname{rk} P_\mathfrak{p} = n$.

Therefore $D(a) \subset f^{-1}(\{n\})$, so f is continuous. $\square$

Definition 85. Let P be a finitely generated projective R-module. Then P is said to be of *constant rank* if $\operatorname{rk} P_\mathfrak{q} = \operatorname{rk} P_\mathfrak{p}$ for all $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R$.

Theorem 77. Let R be a commutative ring. Then every finitely generated projective R-module has constant rank if and only if R has no nontrivial idempotents. (And as we showed before, having no nontrivial idempotents is equivalent to $\operatorname{Spec} R$ being connected.)

Proof. Suppose R has no nontrivial idempotents. Then as we showed before, $\operatorname{Spec} R$ is connected. Let P be a finitely generated projective R-module.

As before, let $f : \operatorname{Spec} R \to \mathbb{N}_0$ by $\mathfrak{q} \mapsto \operatorname{rk} P_\mathfrak{q}$. Suppose $n \in \operatorname{im} f$. Then since $\mathbb{N}_0$ has the discrete topology, then $\{n\}$ is both closed and open. Thus $f^{-1}(\{n\})$ is both closed and open. But since $\operatorname{Spec} R$ is connected, then either $f^{-1}(\{n\})$ is either $\operatorname{Spec} R$ or the empty set. But since $n \in \operatorname{im} f$, it is nonempty. Thus $f^{-1}(\{n\}) = \operatorname{Spec} R$. That is, f is constant, as desired.

Conversely, suppose there exist a nontrivial idempotent $e \in R$. Let $I = (e)$ and $J = (1-e)$. Note that $R = I \oplus J$. Also, I and J are finitely generated (they are generated by a single element), and they are projectives.

Extend I to a maximal ideal $\mathfrak{q} \in \operatorname{Spec} R$. Then $(1-e) \notin \mathfrak{q}$. Furthermore, $(1-e)I = 0$ since $(1-e)e = 0$. Therefore $I_{\mathfrak{q}} = 0$. Thus $f(\mathfrak{q}) = 0$. Now extend J to a maximal ideal $\mathfrak{p}$. Then $I \not\subset \mathfrak{p}$, so $I_{\mathfrak{p}} = R_{\mathfrak{p}}$, so $f(\mathfrak{q}) > 0$. Thus f is not constant. ☐

4 Tensor Products

Now let's talk about tensor products.

Definition 86. Let R be a ring with unit (not necessarily commutative). Let M be a right R-module, let N be a left R-module, and let A be an abelian group.

A function $f : M \times N \to A$ is called *R-biadditive* if for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$, then we have that

1. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$
2. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$
3. $f(mr, n) = f(m, rn)$

Example 85. One example is $f : (R \times R) \to R$ by $(r, s) \mapsto rs$.

Another example is $f : R^2 \times M \to M^2$ by $((r, s), m) \mapsto (rm, sm)$.

A third example works for any right ideal I. Let $f : R/I \times M \to M/IM$ by $(\overline{r}, m) \to \overline{rm}$.

Another example works for any multiplicatively closed set S which is in the center of R. (Note that we haven't actually defined how to localize in a non-commutative ring, but one can image that it is doable.) Define $f : R_S \times M \to M_s$ by $(\frac{r}{s}, m) \mapsto \frac{rm}{s}$.

We now define tensor products using a universal property.

Definition 87. Let R, M, and N be as above. An abelian group $M \otimes_R N$ together with an R-biadditive map $h : M \times N \to M \otimes_R N$ is called the *tensor product* of M and N if it has the following property (which we call the universal property): For any abelian group A and R-biadditive map $f : M \times N \to A$, there exists a unique group homomorphism $g : M \otimes_R N$ such that $f = g \circ h$.

Remark 91. The tensor product (if it exists) is unique, up to isomorphism.

We can show this by supposing there exist two "tensor products" T_1 with map h_1 and T_2 with map h_2. Then since h_1 and h_2 are biadditive maps, there exists $\phi : T_1 \to T_2$ such that $h_2 \circ \phi = h_1$ and $h_1 \circ \psi = h_2$. Then $h_1 \circ id_{T_1} = h_1 \circ \psi \circ \phi$. But we assumed there was a unique group homomorphism which makes the diagram commute, so $id_{T_1} = \psi \circ \phi$. Thus $T_1 \cong T_2$.

4.1 Day 13 - February 10

Recall that we "defined" the tensor product last class in the following way:

Definition 88. Let R be a commutative ring, let M be a right R-module and let N be a left R-module. An abelian group $M \otimes_R N$ together with an R-biadditive map $h : M \times N \to M \otimes_R N$ is called the *tensor product* of M and N if it has the following property (which we call the universal property): For any abelian group A and R-biadditive map $f : M \times N \to A$, there exists a unique group homomorphism $g : M \otimes_R N$ such that $f = g \circ h$.

We showed last time that $M \otimes_R N$ is unique (up to isomorphism), if it exists.

We will now show existence:

Proposition 61. With R, M, and N, as above, $M \otimes_R N$ exists.

Proof. Let F be the free abelian groupwith basis of cardinality $|M \times N|$. That is, we write $F = \bigoplus_{(m,n)\in M\times N} \mathbb{Z}$. Let $[m,n]$ denote the basis element of F corresponding to (m,n).

Then every element of F can be uniquely written in the form $\sum_{finite} r_i[m_i,n_i]$ where $r_i \in \mathbb{Z}$.

Let S be the submodule of F generated by all elements of the form

1. $[m, n_1+n_2] - [m,n_1] - [m,n_2]$ for any $m \in M$ and $n_1, n_2 \in N$.
2. $[m_1+m_2, n] - [m_1,n] - [m_2,n]$ for any $m_1, m_2 \in M$ and $n \in N$.
3. $[mr, n] - [m, rn]$ for any $m \in M$, $n \in n$, and $r \in R$.

Then let $M \otimes_R N = F/S$. For $m \in M$ and $n \in N$, let $m \otimes n$ denote $[m,n] + S \in F/S/$ Hence, every element of $M \otimes_R N$ is of the form $\sum_{finite} r_i(m_i \otimes n_i)$ for $r_i \in \mathbb{Z}$. Note that there may be more than one way to write an element now.

Note also that

1. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$ for all $m \in M$, $n_1, n_2 \in N$.
2. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ for all $m_1, m_2 \in M$ and $n \in N$.
3. $(mr) \otimes n = m \otimes (rn)$ for all $m \in M$, $n \in N$ and $r \in R$.

These follow from the elements generating our submodule.

Finally, define $h : M \times N \to M \otimes_R N$ by $(m,n) \to m \otimes n$. By our previous observations, this map is R-biadditive.

Finally, we must show that $M \otimes_R N$ satisfies the universal property. Suppose $f : M \otimes N \to A$ is any R-biadditive function.

Define a group homomorphism $\overline{g} : F \to A$ by $[m,n] \to f(m,n)$. Since f is R-biadditive, then each of the generators for S live in the kernel. Hence $S \subset \ker \overline{g}$. Therefore we get an induced group homomorphism $g : F/S \to A$ by $m \otimes n \mapsto f(m,n)$ (and this is well-defined).

But then $f(m,n) = g(m \otimes n) = g(h((m,n)))$, so $f = g \circ h$.

It then suffices to show that this is the unique group homomorphism g for which this is true. To this end, suppose $g_1 : M \otimes_R N \to A$ is a group homomorphism such that $g_1 \circ h = f$. Then $g_1(m \otimes n) = f(m,n)$, so $g_1 = g$ on all generators of $M \otimes_R N$. Thus $g_1 = g$, so g is unique.

□

Example 86. Consider $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$. Consider the element $1 \otimes \overline{1}$.

Definition 89. Let R, S be rings. An $R-S$ *bimodule* is an abelian group M such that M is a left R-module and a right S-module, and for all $r \in R$, $s \in S$, and $m \in M$, we have that $(rm)s = r(ms)$.

Example 87. Let k be a field, and let n and m be positive integers. Then let $R = M_m(k)$, $S = M_n(k)$, and $M = M_{m\times n}(k)$. Then M is an R-S bimodule.

Example 88. Any ring R is an R-R bimodule.

Example 89. Let R be a commutative ring. Let M be a (left) R-module. Then M is an R-R bimodule, where the action on the right is defined to be the same as the action on the left.

Example 90. Suppose R is a commutative ring, M is an R-module, and I is an ideal such that $IM = 0$. Then M is an R/I-module. That is, M is an R/I-R bimodule (or and R-R/I bimodule).

Example 91. Let R be a commutative ring, with $Char\ R = p$ (a prime). Let M be a left R-module.

We can consider M as an $R-R$ bimodule via the actions $r \cdot m = rm$, $m \cdot r = r^p m$. This makes it and R-R bimodule. This is called the *Frobenius bimodule structure*.

Proposition 62. Let M be an S-R bimodule and N a left R-module. (so N is an R-$\mathbb{Z}$ bimodule). Then $M \otimes_R N$ is a left S-module by the action $s \cdot (m \otimes n) = (sm) \otimes n$.

Proof. We first need to verify that this is well-defined. Fix an $s \in S$. Define a map $f_s : M \times N \to M \otimes_R N$ by $m, n \mapsto (sm) \otimes n$. One can check that f_s is R-biadditive. Then there exists a unique group homomorphism $\overline{f}_s : M \otimes_R N \to M \otimes_R N$ by $m \times n \to (sm) \otimes n$. Hence the multiplication is well-defined!

It is then easy to see that the rest of the module properties hold. □

4.2 Day 14 - February 12

Recall from last time that if M is an $S - R$ bimodule, and N is a left R-module, then $M \otimes_R N$ is a left S-module via the action $s(m \otimes n) = (sm) \otimes n$.

Similarly, if N is an $R - S$ bimodule, and M is a right R-module, then $M \otimes_R N$ is a right S-module via the action $(m \otimes n)s = m \otimes (ns)$.

Remark 92. We can use this property of tensor products for a "base change". If $\phi : R \to S$ is a ring homomorphismm, then we can give S an $S - R$ bimodule structure by the standard method: S acts on the left my multiplication, and $r \in R$ acts on the right by multiplication by $\phi(r)$. Then if M is a left R-module, then $S \otimes_R M$ is a left S-module via $s'(s \otimes m) = (s's) \otimes m$.

Example 92. Suppose $H \leq G$ are are groups, and k is a field. Then $k[H] \hookrightarrow k[G]$ is a ring homomorphism. Given a left $k[H]$-module M, $k[G] \otimes_{k[H]} M$ is a left $k[G]$-module.

Proposition 63. Let R be a ring. Then

1. If M is a left R-module, then $R \otimes_R M \cong M$ as left R-modules (with the map $r \otimes m \mapsto rm$).
2. Let I be a two-sided ideal of R, with M a left R-module. Then $R/I \otimes_R M \cong M/IM$ as left R/I-modules (with the map $\overline{r} \otimes m \mapsto \overline{rm}$).
3. Let S a multiplicatively closed subset of $Z(R)$, and let M be a left R-module. Then $R_S \otimes_R M \cong M_S$ as left R-modules (with the map $\frac{r}{s} \mapsto \frac{rm}{s}$).
4. If R is commutative, and M and N are R-modules, then $M \otimes_R N \cong N \otimes_R M$ as R-modules (with the map $m \otimes n \to n \otimes m$).

Proof. For all of these, we define homomorphisms in both directions, and verify that they are inverses of each other.

(Proof of (1)) Define $f : R \times M \to M$ by $(r, m) \mapsto rm$. Then f is R-biadditive, so by the universal property there is a unique group homomorphism $\overline{f} : R \otimes_R M \to M$ by $r \otimes m \mapsto rm$. Furthermore, $\overline{f}(r'(r \otimes m)) = \overline{f}((r'r) \otimes m) = (rr')m = r'(rm) = r'\overline{f}(r \otimes m)$. Thus $\overline{f}$ is an R-module homomorphism.

Now define $g : M \to R \otimes_R M$ by $m \mapsto 1 \otimes m$. Then $g(rm) = 1 \otimes (rm) = 1 \cdot r \otimes m = r(1 \otimes m) = rg(m)$.

One can verify that $g\overline{f}$ and $\overline{f}g$ are the identity, and this completes the proof. □

(Proof of part of (2)) Define $\hat{g} : M \to R/I \otimes M$ by $m \mapsto \overline{1} \otimes m$. Then one can see that $\hat{g}$ is an R-module homomorphism.

For all $i \in I$ and $m \in M$, $\hat{g}(im) = \overline{1} \otimes im = \overline{i} \times m = \overline{0} \times m = 0$. Therefore $IM \subset \ker \hat{g}$.

This is the only hard part of the proof, and the rest is left as an exercise to the reader. □

The proof of (3) is a homework problem. □

(Proof of part of (4)) Define $f : M \times N \to N \otimes_R M$ by $(m, n) \to n \otimes m$ (note that this is heavily dependent on R being commutative, or this would make no sense). Then we can get that f is an R-biadditive group homomorphism. Then there exists a unique R-module homomorphism $\overline{f} : M \otimes N \to N \otimes M$ by $m \otimes n \to n \otimes m$.

Similary, one creates a $g : N \times M \to M \otimes_R N$ by $(n, m) \to m \otimes n$, and once gets an $\overline{g}$. Then $\overline{f}\overline{g}$ and $\overline{g}\overline{f}$ are the identities on the appropriate things. Thus $M \otimes_R N \cong N \otimes_R M$.

□

Proposition 64. Let M be an R-S bimodule, let N be an $S - T$ bimodule, and let P be a left T-module. Then $(M \otimes_S N) \otimes_T P \cong M \otimes_S (N \otimes_T P)$ as left R-modules.

Omitted. □

Remark 93. Here is an application of tensor products. Let R be a commutative ring, and let M and N be R-modules. Let $I \subset R$ such that $IM = 0$ (this implies that M is naturally and R/I-module).

Then

$$\begin{aligned} M \otimes N &\cong (M \otimes_{R/I} R/I) \otimes_R N \\ &\cong (M \otimes_{R/I} (R/I \otimes_R N) \\ &\cong M \otimes_{R/I} N/IN \end{aligned}$$

As R/I-modules. If $IN = 0$ as well, then $M \otimes_R N \cong M \otimes_{R/I} N$.

This leads to the following theorem:

Theorem 78. If F and G are free R-modules, with bases $\{f_i\}, \{g_j\}$ respectively, then $F \otimes_R G$ is free, and a basis for it is $\{e_i \otimes f_j\}$.

4.3 Day 15 - February 15

Remark 94. Let R be a ring, and let $f : M \to A$ and $g : N \to B$ be homomorphisms of right R-modules and left R-modules, respectively. Then we can define $f \times g : M \times N \to A \otimes_R B$ by $(m, n) \mapsto f(m) \otimes g(n)$.

Since f and g are homomorphisms, then $f \times g$ is is R-biadditive. Then by the universal property, there exists a unique group homomorphism $f \otimes g : M \otimes_R N \to A \otimes_R B$ by $m \otimes n \mapsto f(m) \otimes g(n)$.

Remark 95. We can expand the previous example to give a module homomorphism under the following conditions: If M and A are $S - R$ bimodules, and f is an $S - R$ bimodule homomorphism, then $f \otimes g$ will be an S-module homomorphism.

Remark 96. We also get a nice result if f and g are isomorphisms. Namely, if f and g are isomorphisms, then $f \otimes g$ is an isomorphism, since $(f \otimes g)^{-1} = f^{-1} \otimes g^{-1}$. [This makes use of the easily-verified fact that $(f \otimes g) \circ (h \otimes l) = fh \otimes gl$.]

Hence if $M \cong A$ and $N \cong B$, then $M \otimes_R N \cong A \otimes_R B$.

Remark 97. Let R be a commutative ring, and let M and N be R-modules. If $\{m_\alpha\}$ is a generating set for M, and $\{n_\beta\}$ is a generating set for N, then $\{m_\alpha \otimes n_\beta\}$ is a generating set for $M \otimes_R N$.

Proposition 65. Let R be a commutative ring, and let F and G be free R-modules with bases $\{f_\alpha\}$ and $\{g_\beta\}$, respectively. Then $F \otimes_R G$ is a free R-module with basis $\{f_\alpha \otimes g_\beta\}$. (So $rank(F \otimes_R G) = rank(F) \cdot rank(G)$.)

Proof. By the previous remark, we know that $\{f_\alpha \otimes g_\beta\}$ generates $F \otimes_R G$. It then suffices to show linear independence.

Suppose $\sum r_{\alpha,\beta} f_\alpha \otimes g_\beta = 0$. Fix an $i \in I$ and $j \in J$. We wish to show $r_{i,j} = 0$.

Define $\phi : F \to R$ by $f_\alpha \mapsto \begin{cases} 1 & \text{if } \alpha = i \\ 0 & \text{otherwise} \end{cases}$. Similarly, define $\psi : G \to R$ by $g_\beta \mapsto \begin{cases} 1 & \text{if } \beta = j \\ 0 & \text{otherwise} \end{cases}$.

Then we get an R-module homomorphism $F \otimes_R G \to R \otimes RR \overset{\cong}{\to} R$ by $f_\alpha \otimes g_\beta \mapsto \phi(f_\alpha) \otimes \phi(g_\beta) \mapsto \phi(f_\alpha)\phi(g_\beta)$. In other words, $f_\alpha \otimes g_\beta \mapsto \begin{cases} 1 & \text{if } \alpha = i, \beta = j \\ 0 & \text{otherwise} \end{cases}$.

Then $0 = (\phi \otimes \psi)(0) = (\phi \otimes \psi)(\sum r_{\alpha,\beta} f_\alpha \otimes g_\beta) = r_{i,j}$. Thus $0 = r_{i,j}$, so these are linearly independent. $\square$

Corollary 34. Suppose K is a field, and V and W are k-vector spaces. Then $\dim_k V \otimes_k W = (\dim_k V) \otimes (\dim_k W)$. In particular, $V \otimes_k W = 0$ if and only if $V = 0$ or $W = 0$.

Proposition 66. If R is a commutative ring, and I and J are ideals, then $R/I \otimes_R R/J \cong R/(I + J)$. In particular, if $I = \mathfrak{m}_1$ and $J = \mathfrak{m}_2$, a pair of distinct maximal ideals, then $R/I \neq 0$ and $R/J \neq 0$, by $R/I \otimes_R R/J = 0$.

Proposition 67. Let A be a right R-module, and $\{\beta_\alpha\}_{\alpha \in I}$ be a collection of left R-modules. Then $A \otimes_R (\bigoplus_\alpha \beta_\alpha) \cong \bigoplus_\alpha (A \otimes_R \beta_\alpha)$.

Proof. For $i \in I$, let $\rho_i : \beta_i \to \bigoplus_\alpha \beta_\alpha$ be the inclusion map, and let $\Pi_i : \beta_\alpha \to \beta_i$ be the projection map.

Define $\psi : A \times \bigoplus_\alpha \beta_\alpha \to \oplus(A \otimes_R \beta_\alpha)$ by $(a, v) \mapsto (a \otimes \Pi_\alpha(v)$. Then ψ is R-biadditive, so by the universal property we get an induced map $\tilde{\psi} : A \otimes \bigoplus B_\alpha rightarrow \oplus (A \otimes_R \beta_\alpha)$ by $a \otimes v \mapsto (a \otimes \Pi_\alpha(v))$.

Also, define $\phi_\alpha : A \times B_\alpha \to A \otimes_R (\oplus B_\alpha)$ by $(a, b) \to a \otimes \rho_\alpha(b)$.

Then by the universal property, this gives a group homomorphism $\tilde{\phi}_\alpha : A \otimes_R B_\alpha \to A \otimes_R (\oplus B_\alpha)$ by $a \otimes b \to a \otimes \rho_\alpha(b)$. Define $\tilde{\phi} : \bigoplus(A \otimes_R B_\alpha) \overset{\oplus\tilde{\phi}_\alpha}{\to} A \otimes_R (\oplus B_\alpha)$ by $(u_\alpha) \to (\tilde{\phi}_\alpha(u_\alpha))$.

Then one can check that $\tilde{\phi} \circ \tilde{\psi} = 1$ and $\tilde{\psi} \circ \tilde{\phi} = 1$, and this completes the proof. □

Exercise 27. How many elements are in the $\mathbb{Z}$-module $\mathbb{Z}/(100) \otimes_\mathbb{Z} \mathbb{Z}^3 \otimes_\mathbb{Z} \mathbb{Z}_4 \otimes \mathbb{Z}/(150)$.

First, we can recall that $\mathbb{Z}/(100) \otimes_\mathbb{Z} \mathbb{Z}/(150) \cong \mathbb{Z}/(50)$.

Furthermore, $\mathbb{Z}/(50) \otimes_\mathbb{Z} \mathbb{Z}_4 \cong \mathbb{Z}_4/(5)\mathbb{Z}_4 \cong \mathbb{Z}_4/(25)\mathbb{Z}_4 \cong (\mathbb{Z}/(25))_{\frac{1}{4}} \cong \mathbb{Z}/25$.

Finally, by the previous theorem, $\mathbb{Z}/(25) \otimes_\mathbb{Z} \mathbb{Z}^3 \cong (\mathbb{Z}/(25) \otimes_\mathbb{Z} \mathbb{Z})^3 \cong (\mathbb{Z}/(25))^3$. Therefore this module has 25^3 elements in it.

4.4 Day 16 - February 17

Great googly-moogly, it's time for an application! This is apparently used for quantum physics.

Remark 98. Let R be a commutative ring, let A be an $m \times n$ matrix, and let B be a an $r \times s$ matrix. Define the tensor product (or Kronecker product) $A \otimes B$ to be the $mr \times ns$ matrix with the form:

$$\begin{pmatrix} a_{1,1}B & \ldots & a_{1,n}B \\ a_{2,1}B & \ldots & \vdots \\ \vdots & & \vdots \\ a_{m,1}B & \ldots & a_{m,n}B \end{pmatrix}$$

Let F_1 and F_2 be free modules of rank n and m, respectively. Fix bases β_1 and β_2 for F_1 and F_2. Let $\beta_1 = \{e_1, ..., e_m\}$ and $\beta_2 = \{f_1, ..., f_n\}$. Define $\phi : F_1 \to F_2$ by $e_j \mapsto \sum_{i=1}^{n} a_{i,j} f_i$. Thus $[\phi]_{\beta_1}^{\beta_2} = A$.

Let $\psi : G_1 \to G_2$ be defined similarly with bases β_1' and β_2'. Then as we showed in last class, $\phi \otimes \psi : F_1 \otimes G_1 \to F_2 \otimes G_2$ is a well-defined function.

Furthermore, $\beta_1 \otimes \beta_1'$ is a basis for $F_1 \otimes G_1$ and similarly $\beta_2 \otimes \beta_2'$ is a basis for $F_2 \otimes G_2$. Order the bases lexicographically. Then $A \otimes B$ is the matrix for $\phi \otimes \psi$ with respect to these matrices.

5 Category Theory and Functors

Now let's move on to the opposite of an application: categories!

Definition 90. A *category* $\mathcal{C}$ consists of the following:

1. A "class" of *objects* $\text{obj}\,\mathcal{C}$

2. For any two objects A and B of $\mathcal{C}$, we have a set of *morphisms* $Hom_\mathcal{C}(A, B)$ (we sometimes write $f : A \to B$ instead of $f \in Hom_\mathcal{C}(A, B)$). These morphisms are sometimes called *arrows*.

3. For objects A, B, C of $\mathcal{C}$, there is a function $\circ : Hom_\mathcal{C}(B \times C) \times Hom_\mathcal{C}(A, B) \to Hom_\mathcal{C}(A, C)$. We write $(f, g) \mapsto f \circ g = fg$, and we call this function *composition*. Composition satisfies the following axioms:
   - For all appropriate f, g, h, $(fg)h = f(gh)$.
   - For each object A of $\mathcal{C}$, there exists a $1_A \in Hom_\mathcal{C}(A, A)$ such that $f1_A = f$ and $1_A g = g$ for all $f : A \to B$ and all $g : C \to A$.

Example 93. Let $\mathcal{C}$ denote the class of all sets, with morphisms being all functions. Then $\mathcal{C}$ is a category, and we denote it by $\langle\langle Sets\rangle\rangle$.

Example 94. Let $\mathcal{C}$ denote the class of all groups, with morphisms being all group homomorphisms. Then $\mathcal{C}$ is a category, and we denote it by $\langle\langle Groups\rangle\rangle$.

Example 95. Let $\mathcal{C}$ denote the class of all topological spaces, with morphisms being all continuous functions. Then $\mathcal{C}$ is a category, and we denote it by $\langle\langle Top\rangle\rangle$.

Example 96. Let R be a ring (not necessarily commutative) and let $\mathcal{C}$ denote the class of all left R-modules, with morphisms being all homomorphisms of left R-modules. Then $\mathcal{C}$ is a category, and we denote it by $\langle\langle R - mod\rangle\rangle$.

We also use $\langle\langle mod - R\rangle\rangle$ to denote the category of right R-modules, and $\langle\langle S - R\ mod\rangle\rangle$ to denote the set of $S - R$ bimodules.

Example 97. Let $\mathcal{C}$ denote the class of all short exact sequences, with morphisms being all commuting stuff (chain complexes?). Then $\mathcal{C}$ is a category, and we denote it by $\langle\langle s.e.s.\rangle\rangle$.

Definition 91. Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A *covariant functor* $F : \mathcal{C} \to \mathcal{D}$ is the the following:

1. For each object A of $\mathcal{C}$, there is a unique object, denoted $F(A)$ in $\mathcal{D}$.
2. For every pair of objects A, B of $\mathcal{C}$, there is a function taking $Hom_{\mathcal{C}}(A, B) \to Hom_{\mathcal{D}}(F(A), F(B))$ by $f \mapsto F(f)$, such that $F(1_A) = 1_{F(A)}$ and $F(fg) = F(f)F(g)$ whenever fg makes sense.

A *contravariant functor* is the same thing, but we make two modifications. First, $F : Hom_{\mathcal{C}}(A, B) \to Hom_{\mathcal{D}}(F(B), F(A))$ (i.e. we switched $F(B)$ and $F(A)$). Second, $F(fg) = F(g)F(f)$.

Example 98. Define $F : \langle\langle Groups\rangle\rangle \to \langle\langle Sets\rangle\rangle$ by taking the underlying set. Then F is a covariant functor, which we call the *forgetful functor*.

Define $F : \langle\langle S - R - bimod\rangle\rangle \to \langle\langle \mathbb{Z} - mods\rangle\rangle$ by taking the underlying abelian group. Then F is a covariant functor, which we also call the forgetful functor.

Example 99. Define $F : \langle\langle comm\ rings\rangle\rangle \to \langle\langle Top\rangle\rangle$ by $F(R) = \operatorname{Spec} R$. Then F is a contravariant functor.

Example 100. Let R be a commutative ring, and S a multiplicatively closed set. Then define $F : \langle\langle R - mod\rangle\rangle \to \langle\langle R_S - mod\rangle\rangle$ by $F(M) = M_S$. Then F is a covariant functor which we call the *localization functor*.

Example 101. Let R be a commutative ring, and let I be an ideal. Then $F : \langle\langle R - mod\rangle\rangle \to \langle\langle R/I - mod\rangle\rangle$ by $F(M) = M/IM$ is a covariant functor.

Example 102. Let R be a ring, and let M be a right R-module. Define a functor $F = M\otimes - : \langle\langle R - mod\rangle\rangle \to \langle\langle \mathbb{Z} - mod\rangle\rangle$ by $F(N) = M \otimes_R N$. Then F is a covariant functor.

If N is an $S - R$ bimodule, then $F(N)$ is in the category of S-modules. In particular, if R is commutative, then our $M \otimes -$ maps into the category of R-modules.

In fact, the previous two examples were secretly this one.

5.1 Day 17 - February 19

Definition 92. A functor of R-modules, F, is called *additive* if, for all $f, g \in Hom_R(M, N)$, we have that $F(f + g) = F(f) + F(g)$.

Example 103. Let M be an $S - R$ bimodule. Let $F = M \otimes_R -$. Then observe that $F(f + g) = 1_M \otimes (f + g) = 1_M \otimes f + 1_M \otimes g = F(f) + F(g)$. Therefore F is additive.

Definition 93. A functor of R-modules, F, is called *multiplicative* if, for all $r \in R$ and R-modules N, we have $F(\mu_{r,N}) = \mu_{r,F(N)}$. Where $\mu_{r,N} : N \to N$ is given by $n \mapsto rn$.

Example 104. Let M be an R-module (where R is commutative). Then let $F = M \otimes_R -$. Then $\mu_{r,N} : N \xrightarrow{r} N$, and $1_M \otimes \mu_{r,N} : M \otimes_R N \to M \otimes_R N$ by $m \otimes n \mapsto m \otimes rn = mr \otimes n = r(m \otimes n) = \mu_{r, M\otimes_R N}(m \otimes n)$. Thus F is multiplicative.

Definition 94. Let F be an additive covariant functor on module categories. We say F is *exact* if whenever $A \xrightarrow{f} B \xrightarrow{g} C$ is exact at B, then $F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$ is exact at $F(B)$.

Example 105. As we previously showed, the localization functor is exact.

Definition 95. Let F be an additive covariant functor on module categories. Then we say F is *left exact* if, whenever $0 \to A \to B \to C$ is exact, then $0 \to F(A) \to F(B) \to F(C)$ is exact.

Similarly, we say F is *right exact* if, whenever $A \to B \to C \to 0$ is exact, then $F(A) \to F(B) \to F(C) \to 0$ is exact.

Exercise 28. If F is an additive covariant functor on module categories, then F is exact if and only if F is both left exact and right exact.

Theorem 79. Let M be an $S-R$ bimodule. Then $M \otimes_R - : \langle\langle R - mod \rangle\rangle \to \langle\langle S - mod \rangle\rangle$ is right exact.

Proof. Let $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be an exact sequence in $\langle\langle R - mod \rangle\rangle$. Apply $M \otimes_R -$, to get: $M \otimes_R A \xrightarrow{1\otimes f} M \otimes_R B \xrightarrow{1\otimes g} M \otimes_R C \to 0$.

First we will show that $1 \otimes g$ is onto. Let $m \otimes c \in M \otimes_R C$. Since g is onto, then there exists a $b \in B$ such that $g(b) = c$. Then $(1 \otimes g)(m \otimes c) = m \otimes c$. Thus $1 \otimes g$ is onto, so the sequence is exact at $M \otimes_R C$.

We now need to show that $\operatorname{im} 1 \otimes f = \ker 1 \otimes g$.

Note that since F is additive, then $F(0) = 0$ (this is a statement about the zero map). If $gf = 0$, then $0 = F(gf) = F(g)F(f)$ (the last equality is due to the fundamental property about composing functors). Thus $\operatorname{im} F(g) \subset \ker F(f)$. [Note that if we stop here, this shows that a functor F takes complexes to complexes.] But $F(g) = 1_M \otimes g$, and $F(f) = 1_M \otimes f$, so $\operatorname{im} 1 \otimes f \subset \ker 1 \otimes g$.

It then suffices to show that $\ker 1 \otimes g \subset \operatorname{im} 1 \otimes f$.

Now define $h : M \times C \to M \otimes RB/\operatorname{im}(1 \otimes f)$ by $(m, c) \mapsto \overline{m \otimes b}$, where b is any element such that $g(b) = c$. We will first show that h is well defined. Suppose $g(b_1) = g(b_2) = c$. Then $g(b_1 - b_2) = 0$, so $b_1 - b_2 \in \ker g = \operatorname{im} f$. Let $a \in A$ be an element such that $f(a) = b_1 - b_2$. Then $m \otimes b_1 - m \otimes b_2 = m \otimes (b_1 - b_2) = m \otimes f(a) = (1 \otimes f)(m \otimes a) \in \operatorname{im}(1 \otimes f)$. So $\overline{m \otimes b_1} = \overline{m \otimes b_2}$ in $M \otimes_R B/\operatorname{im}(1 \otimes f)$.

Furthermore, it follows immediately from the definition of h that h is R-biadditive. Therefore there is an induced S-module homomorphism $\tilde{h} : M \otimes_R C \to M \otimes RB/\operatorname{im}(1 \otimes f)$ by $m \otimes c \mapsto \overline{m \otimes b}$ (where $g(b) = c$).

Let $x = \sum_{i=1}^{n} m_i \otimes b_i \in M \otimes_R B$, and suppose $x \in \ker 1 \otimes g$. Then

$$\begin{aligned} 0 &= \tilde{h}(0) \\ &= \tilde{h}((1 \otimes g)(\sum m_i \otimes b_i)) \\ &= \tilde{h}(\sum m_i \otimes g(b_i)) \\ &= \sum \tilde{h}(m_i \otimes g(b_i)) \\ &= \sum \overline{m_i \otimes b_i} \\ &= \overline{\sum m_i \otimes b_i} \\ &= \overline{x} \end{aligned}$$

Therefore, $x \in \operatorname{im}(1 \otimes f)$. That is, $\ker(1 \otimes g) \subset \operatorname{im}(1 \otimes f)$.

Thus $\ker(1 \otimes g) = \operatorname{im}(1 \otimes f)$, so the sequence is exact at $M \otimes_R B$, so it is exact.

□

Example 106. Consider the short exact sequence $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$. Applying $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} -$, we get $\mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{1} \mathbb{Z}/2/Z \to 0$, which is no longer exact.

Definition 96. Let R be a commutative ring. Then an R-module M is called *flat* if $M \otimes_R -$ is an exact functor.

Example 107. Let R be a commutative ring. Then R is flat as an R-module. Also, R_S is flat. Also, any projective R-module is flat.

5.2 Day 18 - February 22

Remark 99. If R is a commutative ring, and $A \subset B$ and $C \subset D$ are R-modules, then we know that $A \times C \subset B \times D$. We also know that $A \oplus C \subset B \oplus D$. However, it need not follow that $A \otimes_R C \subset B \otimes_R D$. There certainly is a function form the former to the latter, but that function need not be injective, because tensor products can be tricky.

Definition 97. Let R be a ring, and let M and N be left R-modules. Then we define $Hom_R(M, N)$ to be $Hom_R(M, N) = \{f : M \to N | f \text{is a homomorphism of left } R\text{-modules}\}$.

Remark 100. We always know that $Hom_R(M, N)$ is an abelian group. Furthermore, if R is commutative, then $Hom_R(M, N)$ is an R-module in the natural way:

For $r \in R$, and $f : M \to N$, define $rf : M \to N$ by $rf(m) = f(rm) = rf(m)$.

More generally, suppose M is an $R{-}S$ bimodule. Then $Hom_R(M, N)$ has the structure of a left S-module. That is, for $s \in S$ and $f : M \to N$, define $sf : M \to N$ by $(sf)(m) = f(ms)$.

Similarly, if N is an $R - T$ bimodule, then $Hom_R(M, N)$ is a right T-module. That is, for $t \in T$ and $f : M \to N$, define $(ft)(m) = f(m)t$.

Remark 101. We like Hom because it lets us do a change of base. Let $\phi : R \to S$ be a ring homomorphism, and let N be a left R-module. Recall that S has the structure of an $R - S$ bimodule.

Then $Hom_R(S, N)$ is a left S-module.

Definition 98. Let M be an $R{-}S$ bimodule. Then define a *hom functor* $F = Hom_R(M, -) : \langle\langle R{-}mod\rangle\rangle \to \langle\langle S - mod\rangle\rangle$ by $N \mapsto Hom_R(M, N)$.

Remark 102. Let's verify that F is indeed a functor. By the previous remarks, F does indeed take objects from $\langle\langle R - mod\rangle\rangle$ to $\langle\langle S - mod\rangle\rangle$. Let's check that F behaves well on arrows. If $f : N_1 \to N_2$, then we have that $F(f) = f_* : Hom_R(M, N_1) \to Hom_R(M, N_2)$ by $g \mapsto fg$. Then one can verify that this satisfies all the other requirements of a functor.

Proposition 68. We have the following properties about the $Hom_R(M, -)$ functor.

1. The $Hom_R(M, -)$ functor is covariant.
2. The $Hom_R(M, -)$ functor is additive.
3. If R is commutative, then the $Hom_R(M, -)$ functor is multiplicative.

(Proof omitted.)

Definition 99. Let N be an $R - T$ bimodule. Define a contravariant functor $G = Hom_R(-, N) : \langle\langle R - mod\rangle\rangle \to \langle\langle mod - T\rangle\rangle$ by $M \mapsto Hom_R(M, N)$.

Remark 103. As before, we can verify that this is a contravariant functor.

Also, G is additive, and if R is commutative then G is multiplicative.

Proposition 69. Let M be an $R - S$ bimodule. Then $Hom_R(M, -)$ is left exact.

Proof. Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ be exact. We need to show that $0 \to Hom_R(M, A) \xrightarrow{f_*} Hom_R(M, B) \xrightarrow{g_*} Hom_R(M, C)$ is exact.

First we will show that f_* is injective. Suppose $f_*(h) = 0$. Then $fh = 0$. Since f is injective, then $h = 0$.

We will now show that $\operatorname{im} f_* \subset \ker g_*$. We can see that $g_* f_* = (gf_*) = (0)_* = 0$.

It then suffices to show that $\ker g_* \subset \operatorname{im} f_*$. Let $h \in \ker g_*$. Then $gh = 0$. Therefore $\operatorname{im} h \subset \ker g = \operatorname{im} f$.

Let $m \in M$. Then $h(M) = f(a_m)$ for some $a_m \in A$. Since f is injective, then this a_m is unique. Define $\alpha : M \to A$ by $m \mapsto a_m$. Then $\alpha \in Hom_R(M, A)$. Note that $f_*(\alpha) = h$. In other words, $f\alpha = h$. Hence $h \in \operatorname{im} f_*$. ☐

Definition 100. Let F be a contravariant functor (in $\langle\langle R - mod\rangle\rangle$). Then F is sait to be *left exact* if, whenever $A \to B \to C \to 0$ is exact, then $0 \to F(C) \to F(B) \to F(A)$ is exact.

Exercise 29. Let N be an $R - T$ bimodule. Then $Hom_R(-, N)$ is left exact.

Let's list some properties of the Hom functors.

Proposition 70. Let M be a left R-module. Then $Hom_R(R, M) \cong M$ (as left R-modules).

Proof. Define $\phi : Hom_R(R, M) \to M$ by $f \mapsto f(1)$. For $m \in M$, we have that $f : R \to M$ by $r \mapsto rm$ is in $Hom_R(R, M)$. Therefore ϕ is surjective.

Also, if $\phi(f) = 0$, then $f(1) = 0$, so f is the constant 0 map. Thus ϕ is surjective.

Finally, $\phi(rf) = rf(1) = r\phi(f)$. Thus ϕ respects multiplication by elements of R. Thus ϕ is an isomorphism of left R-modules. ☐

Proposition 71. Let R be a commutative ring. Let I be an ideal of R. Then $Hom_R(R/I, M) \cong (0 :_M I)$. (Recall that $(0 :_M I) = \{m \in M | Im = 0\}$.

Proposition 72. If $\{A_i\}_{i=1}^n$ is a set of $R - S$ bimodules, then $Hom_R(\bigoplus_{i=1}^n A_i, B) \cong \bigoplus_{i=1}^n Hom_R(A_i, B)$ (as left S-modules).

Proposition 73. If $\{B_i\}_{i=1}^n$ is a set of $R - T$ bimodules, then $Hom_R(A, \bigoplus_{i=1}^n B_i) \cong \bigoplus_{i=1}^n Hom_R(A, B_i)$ (as right T-modules).

Example 108. If R is commutative, then $Hom_R(R^n, M) \cong \bigoplus_{i=1}^n Hom_R(R, M) \cong M^n$.

If R is commutative, $Hom_R(R^n, R^m) \cong (R^m)^n \cong R^{mn}$.

Next time: Homs and Tensors and Lions, oh my!

5.3 Day 19 - February 24

Proposition 74. Let P be a left R-module. Then $Hom_R(P, -)$ is exact if and only if P is projective.

Proof. Suppose P is projective. We showed last time that $Hom_R(M, -)$ is always left exact. It then suffices to show that if $M \xrightarrow{f} N \to 0$ is exact, then $Hom_R(P, M) \xrightarrow{f_*} Hom_R(P, N) \to 0$ is also exact.

That is, it suffices to show that f_* is surjective. Let $g \in Hom_R(P, N)$. That is, $g : P \to N$ is an R-module homomorphism. Since P is projective, then by the definition of projective, there exists an $h : P \to M$ such that $fh = g$. Thus $g = f_*(h)$, so f_* is onto. Thus $Hom_R(P, -)$ is exact.

Conversely, suppose $Hom_R(P, -)$ is exact. Choose a free module F and a surjective R-module homomorphism $\phi : F \to P$. Then

$$0 \to K \xrightarrow{i} F \xrightarrow{\phi} P \to 0$$

is exact, where $K = \ker \phi$. Apply the functor $Hom_R(P-)$ to this whole thing. Then we get that

$$0 \to Hom_R(P, K) \xrightarrow{i_*} Hom_R(P, F) \xrightarrow{\phi_*} Hom_R(P, P) \to 0$$

is also exact. As ϕ_* is onto and $1_P \in Hom_R(P, P)$, there exists a $g : P \to F$ such that $\phi g = \phi_*(g) = 1_P$. Therefore $F \cong P \oplus K$. Since P is the summand of a free module, it is projective. ☐

Recall that a right R-module F is *flat* if $F \otimes_R -$ is an exact functor.

Remark 104. Consider a commutative diagram

$$\begin{tikzcd} A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[d] \\ D \arrow[r] & E \arrow[r] & F \end{tikzcd}$$

where the vertical arrows are isomorphisms. Then the top row is exact if and only if the bottom row is exact.

The proof of this is left as an exercise for the reader, but is fairly simple diagram chasing.

Proposition 75. Let R be a commutative ring, and S be a multiplicatively closed set. Then R_S is a flat R-module (so in particular, R is a flat R-module).

Proof. Let $A \xrightarrow{f} B \xrightarrow{C}$ be exact. Then

$$\begin{tikzcd} R_S \otimes_R A \arrow[r, "1 \otimes f"] \arrow[d] & R_S \otimes_R B \arrow[r, "1 \otimes g"] \arrow[d] & R_S \otimes_R C \arrow[d] \\ A_S \arrow[r, "\frac{f}{1}"] & B_S \arrow[r, "\frac{g}{1}"] & C_S \end{tikzcd}$$

is a commutative diagram. Furthermore, we showed that the bottom row is exact. By the homework [edit: see immediately below], the vertical arrows are isomorphisms. Then by the remark, the top row is also exact. Thus R_S is a flat R-module. $\square$

Homework Problem 9. *Let R be a commutative ring, let S be a multiplicatively closed set in R, and let M be an R-module. Then $M_S \cong M \otimes_R R_S$.*

Proposition 76. Let $\{A_i\}_{i \in I}$ be a set of right R-modules. Then $\oplus A_i$ is flat if and only if each A_i is flat.

Proof. Let $L \xrightarrow{f} M \xrightarrow{g} N$ be exact. Let $(*)_i$ denote the exact sequence

$$A_i \otimes_R L \stackrel{1_i \otimes f}{\to} A_i \otimes_R M \stackrel{1_i \otimes g}{\to} A_i \otimes_R N$$

for each $i \in I$. Let $(\#)$ denote the exact sequence

$$\oplus(A_i \otimes_R L) \stackrel{\oplus(1_i \otimes f)}{\to} \oplus(A_i \otimes_R M) \stackrel{\oplus(1_i \otimes g)}{\to} \oplus(A_i \otimes_R N)$$

Note that $(\#)$ is exact if and only if $(*)_i$ is exact for all i.

$$\begin{tikzcd} (\#) \oplus (A_i \otimes_R L) \arrow[r, "\oplus(1_i \otimes f)"] \arrow[d, "\cong"'] & \oplus(A_i \otimes_R M) \arrow[r, "\oplus(1_i \otimes g)"] \arrow[d, "\cong"'] & \oplus(A_i \otimes_R N) \arrow[d, "\cong"'] \\ (\#\#) \oplus (A_i) \otimes_R L \arrow[r, "\oplus(1_i \otimes f)"] & \oplus(A_i) \otimes_R M \arrow[r, "\oplus(1_i \otimes g)"] & \oplus(A_i) \otimes_R N \end{tikzcd}$$

This diagram commutes because it is so natural it would be weird if it didn't. Therefore $\oplus A_i$ is flat if and only if $(\#\#)$ is exact. By the lemma, this is the case if and only if $(\#)$ is exact. But this s the case if and only if $(*)_i$ is exact for all i. $\square$

Corollary 35. All free modules F are flat.

Proof. Recall that R is flat. Then $F \cong \bigoplus_i R$, so by the previous proposition, F is flat. $\square$

Corollary 36. All projective modules P are flat.

Proof. Since P is projective, it is the summand of a free module. That is, $F \cong P \oplus K$ for some module K and free module F. But F is flat by the previous corollary. Then by the proposition, P is flat. $\square$

Lemma 29. (Five Lemma) Consider the following commutative diagram of left R-modules:

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 & \xrightarrow{\alpha_4} & A_5 \\ \gamma_1\downarrow & & \gamma_2\downarrow & & \gamma_3\downarrow & & \gamma_4\downarrow & & \gamma_5\downarrow \\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 & \xrightarrow{\beta_4} & B_5 \end{array}$$

Suppose that each row is exact,and that $\gamma_1, \gamma_2, \gamma_4$, and γ_5 are all isomorphisms. Then γ_3 is an isomorphism.

Proof. (We proceed by diagram chasing.) We will first show that γ_3 is injective. Suppose $\gamma_3(a_3) = 0$. Then $\gamma_4\alpha_3(a_3) = \beta_3(\gamma_3(a_3)) = 0$. As γ_4 is injective, then $\alpha_3(a_3) = 0$. Therefore there exists an $a_2 \in A_2$ such that $\alpha_2(a_2) = a_3$. Then $\beta_2(\gamma_2(a_2)) = 0$, so there exists a $b_1 \in B_1$ such that $\beta_1(b_1) = \gamma_2(a_2)$. Since γ_1 is an isomorphism, we can choose $a_1 \in A_1$ such that $\gamma_1(a_1) = b_1$. Then $\gamma_2(\alpha_1(a_1)) = \gamma_2(a_2)$. Since γ_2 is injective, then $a_2 = \alpha(a_1)$. Then $a_3 = \alpha_2(a_2) = \alpha_2(\alpha_1(a_1)) = 0$, since the top row is exact. Therefore γ_3 is injective.

One does something similar for surjective. □

Proposition 77. We get a special case of the five lemma with a smaller commutative diagram:

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ \phi\downarrow & & \psi\downarrow & & & & \\ L & \xrightarrow{h} & M & \xrightarrow{i} & N & \longrightarrow & 0 \end{array}$$

where the top row and bottom row are exact, and ϕ and ψ are isomorphisms.

Then there exists an isomorphism $\epsilon : C \to N$ making the diagram commute.

Proof. It suffices to show that a map $\epsilon : C \to N$ exists. Then by the 5-lemma on

$$\begin{array}{ccccccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 & \longrightarrow & 0 \\ \phi\downarrow & & \psi\downarrow & & \epsilon\downarrow & & \downarrow & & \downarrow \\ L & \xrightarrow{h} & M & \xrightarrow{i} & N & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

this epsilon would be an isomorphism.

For $c \in C$, choose $b \in B$ such that $g(b) = c$. Define $\epsilon : C \to N$ by $\epsilon(c) = i\psi(b)$. It then suffices to show that ϵ is well-defined.

Suppose $b, b' \in B$ satisfies $g(b') = c$. Then $g(b - b') = 0$, so $b - b' = f(a)$ for some $a \in A$. So $b = f(a) + b'$. Then

$$\begin{aligned} i\psi(b) &= i\psi(f(a)) + i(\psi(b') \\ &= ih\phi 9) + i\psi(b') \\ &= i\psi(b') \end{aligned}$$

since $ih = 0$. It can easily be shown that ϵ is R-linear and makes the diagram commute. Therefore, by the 5-Lemma, ϵ is an isomorphism. □

Definition 101. A left R-module M is called *finitely presented* if there exists an exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

5.4 Day 20 - February 26

Let's talk about the relation between Hom and the tensor product.

Theorem 80 (*Hom*$-\otimes$ **Adjointness/Adjunction).** Let R, S, and T be rings. Let A be an $R-T$ bimodule, B be an $S-R$ bimodule, and C be a left S-module. Then the map $Hom_R(A, Hom_S(B,C)) \to Hom_S(B \otimes_R A, C)$ (which lives in the set of T-module homomorphisms) given by $\phi \mapsto \left(g_\phi : \begin{cases} B \otimes_R A \to C \\ b \otimes a \mapsto \phi(a)(b) \end{cases} \right)$ is a well-defined left T-module isomorphism.

Proof. Many of the details of this proof will be omitted.

We will first show that this map is well-defined.

Fix a $\phi \in Hom_R(A, Hom_S(B,C))$. Define $\tilde{g}_\phi : B \times A \to C$ by $(b,a) \mapsto \phi(b)(a)$.

One can check that $\tilde{g}_\phi$ is R-biadditive. Then by the universal property, there exists a unique g_ϕ which is a well-defined group homomorphism. Thus this map is well-defined.

One can then check that g_ϕ is S-linear.

We will now show that the map $\phi \mapsto g_\phi$ is T-linear. Define a map $Hom_S(B \otimes_R A, C) \to Hom_R(A, Hom_S(B,C))$ by $\psi \mapsto \left(f_\psi : \begin{cases} f_\psi : B \to C \\ b \mapsto \psi(b \otimes a) \end{cases} \right)$. By the previous part, this map is well-defined.

One can then check that

- For any $a \in A$, $f_\psi(a)$ is S-linear.
- f_ψ is R-linear.
- The map $\psi \mapsto f_\psi$ is T-linear.

We then wish to show that $f_{g_\phi} = \phi$. Fix an $a \in A$. Then $f_{g_\phi}(a)(b) = g_\phi(b \otimes a) = \phi(a)(b)$ for all $b \in B$. Thus $f_{g_\phi}(a) = \phi(a)$ for all $a \in A$.

Thus $f_{g_\phi} = \phi$. Similarly, $g_{f_\psi} = \psi$ for all ψ. Thus this map is an isomorphism of T-modules. $\square$

Remark 105. This map is a bit stronger than being simply an isomorphism. It is a *natural isomorphism*, meaning $Hom_R(-, Hom_S(B,C)) \to Hom_S(B \otimes_R -, C)$ is a functor. It is also a functor if you replace any other component with a dash.

Remark 106. Let R be a commutative ring, $x \in R$, let M and N be R-modules, and suppose that $xM = 0$ but x is a non-zero-divisor on N. Then $Hom_R(M,N) \cong Hom_R(M \otimes_R (R/(x)), N) \cong Hom_R(M, Hom_R(R/(x), N))$. But $Hom_R(R/(x), N) \cong (0 :_N X) = 0$, so $Hom_R(M,N) = 0$.

Definition 102. We say an R-module M is *finitely presented* if there exists an exact sequence of the form $R^m \to R^n \to M \to 0$.

Theorem 81. Let R be a commutative ring and let T be a flat R-algebra (that is, there is a ring homomorphism $\phi : R \to T$). Suppose M is a finitely presented R-module, and let N be an R-module. Then $\psi : T \otimes_R Hom_R(M,N) \to Hom_T(T \otimes_R M, T)$ given by $t \otimes f \mapsto \mu_t \otimes f$ is an isomorphism of T-modules.

Proof. We break the problem into several cases.

First, suppose $M = R$. Then $Hom_R(R,N) \cong N$, so $T \otimes_R Hom_R(R,N) \cong T \otimes_R (N) \cong Hom_T(T, T \otimes_R N) \cong Hom_T(T \otimes_R R, T \otimes_R N)$. If we follow an element through this chain of equivalences, we get that $t \otimes f \mapsto t \otimes f(1) \mapsto g_t : \begin{cases} T \to T \otimes_R N \\ 1 \mapsto t \otimes f(1) \end{cases} \mapsto \mu_t \otimes f$. (The last mapping, sending g_t to $\mu_t \otimes f$, is something we should check.) Therefore ψ_R is an isomorphism.

Suppose instead that $M = F = R^n$. Then by using direct sums, we get much the same results. Therefore ψ_F is an isomorphism.

Finally, consider the general case. Since M is finitely presented, there exists an exact sequence $F \to G \to M \to 0$, where F and G are free modules.

Now apply $T \otimes_R -$ to the entire sequence. Since T is flat, the resulting sequence is still exact. That is,

$$T \otimes_R F \to T \otimes_R G \to T \otimes_R M \to 0 \tag{2.1}$$

is exact. Now we apply $Hom_T(-, T \otimes_R N)$ to the equation. This functor is contravariant, so we get a backwards exact sequence. However, by applying $Hom_T(-, N)$ and $T \otimes_R -$ in the opposite order, we get the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, "\cong"'] & 0 \arrow[r] \arrow[d, "\cong"'] & T \otimes_R Hom_R(M,N) \arrow[r] & T \otimes_R Hom_R(G,N) \arrow[r] \arrow[d, "\cong"'] & T \otimes_R Hom_R(F,N) \arrow[d, "\cong"'] \\
0 \arrow[r] & 0 \arrow[r] & Hom_T(T \otimes_R M, T \otimes_R N) \arrow[r] & Hom_T(T \otimes_R G, T \otimes_R N) \arrow[r] & Hom_T(T \otimes_R F, T \otimes_R N)
\end{tikzcd} \tag{2.2}$$

Since T is flat and Hom preserves exactness, then both the top and the bottom are exact. Also, the vertical arrows are isomorphisms, by the previous parts. Furthermore, this is a commutative diagram, since these maps are natural. Finally, you can define the middle arrow in the same way as before.

Then, by the 5-Lemma, there is an isomorphism between $T \otimes_R Hom_R(M,N)$ and $Hom_T(T \otimes_R M, T \otimes_R N)$. $\square$

6 Projective Modules

6.1 Day 21 - February 29

Let R be a commutative ring. Recall that a finitely generated projective module over a quasi-local ring is in fact a free module. What about a converse?

Theorem 82. Let M be a finitely presented R-module. Then the following are equivalent:

1. M is projective.
2. $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module for all $\mathfrak{p} \in \operatorname{Spec} R$.
3. $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$.

Proof. We have already proven that (1) implies (2). Furthermore, (2) implies (3) follows instantly from definitions, as every maximal ideal is prime.

It then suffices to show that (3) implies (1). To this end, suppose M is a finitely presented R-module, and suppose that $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$.

Recall that a module is projective if and only if $Hom_R(M, -)$ is exact. Let $A \xrightarrow{f} B \to$ be exact. Then $Hom_R(M, A) \xrightarrow{f_*} Hom_R(M, B) \to C \to 0$ is exact (where $C = coker(f_*)$). We wish to show that f_* is surjective, and this is equivalent to showing that $C = 0$.

Let's localize at a maximal ideal $\mathfrak{m}$. Then

$$\begin{tikzcd}
Hom_R(M,A)_{\mathfrak{m}} \arrow[r, "\frac{f_*}{1}"] \arrow[d, "\cong"'] & Hom_R(M,B)_{\mathfrak{m}} \arrow[r] \arrow[d, "\cong"'] & C_{\mathfrak{m}} \arrow[r] \arrow[d] & 0 \\
Hom_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, A_{\mathfrak{m}}) \arrow[r, "(\frac{f}{1})_*"] & Hom_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, B_{\mathfrak{m}}) \arrow[r] & 0 &
\end{tikzcd}$$

Since $M_{\mathfrak{m}}$ is free, then it is projective, so the bottom row is exact. The vertical maps are isomorphisms since M is finitely presented. Also, the diagram commutes because the maps are natural. Therefore, by the 5-lemma, $C_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$. But the only such module is 0, so $C = 0$. Since C was the cokernel of f_*, then f_* is surjective. Thus M is projective, by an equivalent condition we proved before. $\square$

Remark 107. If M is a projective module, it is finitely presented. Therefore, in the previous theorem we need not check finitely presented if M is projective.

Let's now make an example to show that finitely presented was a necessary condition in the statement of the previous condition.

Definition 103. Let R be a (not necessarily commutative) ring with unit. We say R is *von Neumann regular* if, for all $a \in R$, there exists $x \in R$ such that $a = axa$.

Example 109. Any division ring is von Neumann regular.

Example 110. Any product of division rings (infinite or finite) is von Neumann regular.

Exercise 30. Let R be a commutative von Neumann regular ring. Then R_S is von Neumann regular for any multiplicatively closed set S.

Proposition 78. Let $(R, \mathfrak{m})$ be a commutative, quasi-local, von Neumann regular ring. Then R is a field.

Proof. We know that commutative ring is a field if and only if its only maximal ideal is (0).

Fix some $a \in \mathfrak{m}$. Then there exists $x \in R$ such that $a = axa = a^2x$. Then $a(1 - ax) = 0$. If $1 - ax \in \mathfrak{m}$, then $1 = (1 - ax) + ax \in \mathfrak{m}$, and this is a contradiction. Thus $a(1 - ax) \notin \mathfrak{m}$. Since R is semi-local, then $(1 - ax)$ is a unit. Thus $a = 0$, so $\mathfrak{m} = (0)$. Thus R is a field. $\square$

Example 111. Let $R = \prod_{i=1}^{\infty} \mathbb{C}$. Then R is von Neumann regular, but not semisimple.

Recall one characterization of a semisimple ring is that every ideal is a direct summand of the ring. Since R is no semisimple, there exists an ideal I of R such that R/I is not projective.

Let $M = R/I$, which is finitely generated. But $R_{\mathfrak{m}}$ is a field for all maximal ideals $\mathfrak{m}$. Therefore $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for all $\mathfrak{m}$, and M is not projective.

7 Injective Modules

Definition 104. Let R be a ring and let E be a left R-module. Then E is called *injective* if, for every diagram $0 \to M \xrightarrow{g} N$, and $f : M \to E$, there exists an $h : N \to E$ such that $hg = f$.

Theorem 83 (Baer's Criterion). Let R be a ring, and let E be a left R-module. Then E is injective if and only if, for all left ideals I of R, if $i : I \to R$ is the inclusion map, and $f : I \to E$ is an R-module homomorphism, then there exists an $h : R \to E$ such that $hi = f$.

(That is, every homomorphism $f : I \to E$ can be extended onto all of R.)

Proof. Certainly, if E is injective, then the map i has such an h.

Conversely, suppose $0 \to M \xrightarrow{i} N$ is exact, and $f : M \to E$ is any R-module homomorphism. Without loss of generality, we can assume $M \subset N$, and that i is the inclusion map.

We now use Zorn's Lemma. Let $\Lambda = \{(k, h_k) | M \subset K \subset N, h_K : K \to E \text{ such that } h_K\Big|_M = f\}$.

Partially order Λ by $(K, h_K) \leq (K', h_{K'})$ if and only if $K \subset K'$ and $h_{K'}\Big|_{K'} = h_k$.

One can verify that Zorn's Lemma applies, so there exists a maximal element in Λ. Let (K, h_K) be such a maximal element.

We then wish to show that $K = N$. Suppose for the sake of contradiction that $K \subsetneq N$. Let $x \in N \setminus K$, and let $I = (K :_R x) = \{r \in R | rx \in K\}$.

Define $\tilde{g} : I \to E$ by $i \mapsto h_K(ix)$. One can verify that $\tilde{g}$ is a homomorphism of R-modules. By hypothesis, we can extend $\tilde{g}$ to g. That is, there exists $g : R \to E$ such that g and $\tilde{g}$ agree on I.

Let $L = K + Rx$. "Define" $h_L : L \to E$ by $k + rx \mapsto h_K(k) + g(r)$. We need to show that h_L is well-defined. Suppose $k + rx = k' + r'x$. Then $(r - r')x = k' - k \in K$. Therefore, $r - r' \in I = (K :_R X)$.

Therefore,

$$\begin{aligned} g(r-r') &= \tilde{g}(r-r') \\ &= h_K((r-r')x) \\ &= h_K(k'-k) \end{aligned}$$

Therefore, $h_K(k)+g(r) = h_K(k')+g(r')$, so $h_L(k+rx) = h_L(k'+r'x)$. That is, h_L is well-defined. But then $(K, h_K) < (L, h_L)$. This contradricts the maximality of K, so $K = N$.

□

7.1 Day 22 - March 2

Recall the following exercise:

Exercise 31. If R is a ring and E is an R-module, then E is injective if and only if $Hom_R(-, E)$ is exact.

Recall also Baer's Criterion:

Theorem 84. Checking the criterion for injective modules is equivalent to checking the same criterion only for ideals of R.

Now we get a new exercise!

Exercise 32. Let $\{E_i\}_{i \in I}$ be a collection of left R-modules. Then $\prod_{i \in I} E_i$ is injective if and only if each E_i is injective.

From this we get that the direct sum of finitely many injective modules is injective.

Remark 108. The direct sum of an arbitrary family of injectives is injective if and only if R is left Noetherian.

Definition 105. We say an R-module M is *divisible* if, for every $u \in M$ and non-zero-divisor $r \in R$, there exists a $u' \in M$ such that $ru' = u$.

Example 112. If R is a field, every R-vector space is divisible.

If R is a domain, then Q, the field of fractions of R, is a divisible R-module. (More generally, if R is a commutative ring, and $S = \{\text{non-zero-divisors in } R\}$, then R_S is a divisible R-module. We call R_S the *total ring of fractions* of R.)

Sums, products, and quotients of divisible modules are divisible. In particular, $\mathbb{Q}/\mathbb{Z}$ is a divisible $\mathbb{Z}$-module.

Proposition 79. Let R be a commutative ring, and let E be an injective left R-module. Then E is divisible.

Proof. Let $u \in E$, and $r \in R$. Suppose r is a non-zero-divisor. Then consider the diagram $0 \to R \xrightarrow{r} R$. Define $f : R \to E$ by $1 \mapsto u$.

Since E is injective, then there exists an $h \in H$ such that $hr = f$. Then $u = f(1) = hr(1) = rh(1)$. Thus $u' = h(1)$ satisfies the definition of divisibility. □

Proposition 80. Let R be a PID. Then every divisible module is injective.

Proof. Let E be a divisible module over R. Using Baer's criterion, it suffices to check the injectivity condition on ideals of R. Let I be an ideal in R. If $I = 0$, there is nothing to check, so suppose $I \neq 0$.

Since R is a PID, then $I = (a)$ for some $a \in R$. Let $f : (a) \to E$ be an R-module homomorphism. We need to find $h : R \to E$ such that $h\Big|_{(a)} = f$. Let $u = f(a)$.

Note that since $a \neq 0$ and R is a PID, then a is a non-zero-divisor. Since E is divisible, and a is a non-zero-divisor, then there exists $u' \in E$ such that $au' = u$. Define $h : R \to E$ by $h(x) = xu'$. Then $h(ra) = rau' = ru = rf(a) = f(ra)$.

Thus we have extended f to an $h : R \to E$. Thus E is injective.

$\square$

Example 113. Since $\mathbb{Z}$ is a domain, then $\mathbb{Q}$, the field of fractions of $\mathbb{Z}$, is divisible as a $\mathbb{Z}$-module.
Therefore $\mathbb{Q}/\mathbb{Z}$ is divisible as a $\mathbb{Z}$-module as well.

Lemma 30. Every $\mathbb{Z}$-module M can be embedded into an injective $\mathbb{Z}$-module. That is, there exists an exact sequence $0 \to M \to E$, where E is injective.

Proof. Choose a free module F which surjects onto M. That is, choose a free module F and a surjective $\mathbb{Z}$-homomorphism $\phi : F \to M$. Let $K = \ker \phi$. Then $M \cong F/K$. However, $K \subset F = \bigoplus \mathbb{Z} \subset \bigoplus \mathbb{Q} = I$. Therefore $M \cong F/K \subset I/K$, so M embeds into I/K.

As $\mathbb{Q}$ is divisible, then I is divisible. Thus I/K is divisble. However, $\mathbb{Z}$ is a PID, so by the proposition, I/K is injective.

$\square$

Proposition 81. Let $\phi : R \to S$ be a ring homomorphism. Let E be an injective left R-module. Then $Hom_R(S, E)$ is an injective left S-module.

Proof. Recall that a left S-module M is injective if and only if $Hom_S(-, M)$ is exact. However $Hom_S(-, M)$ is always left exact. It then suffices to show right exactness.

Suppose $0 \to M \xrightarrow{f} N$ is exact in $\langle\langle S - mod\rangle\rangle$. Then by tensoring with S, we get

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{f} & N \\ & & \cong\downarrow & & \cong\downarrow \\ 0 & \longrightarrow & S \otimes_S M & \xrightarrow{1\otimes f} & S \otimes_S N \end{array}$$

is an exact sequence of R-modules.

Then applying $Hom_R(-, E)$, we get that

$$\begin{array}{ccccc} Hom_R(S \otimes_S N, E) & \xrightarrow{(1\otimes f)^*} & Hom_R(S \otimes_S M, E) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ Hom_S(N, Hom_R(S, E)) & \longrightarrow & Hom_S(M, Hom_R(S, E) & \longrightarrow & 0 \end{array}$$

But the bottom is exact since E is injective. Therefore $Hom_R(S, E)$ is injective as an S-module.

$\square$

Theorem 85. Let R be a ring, and M be a left R-module. Then M embeds into an injective left R-module.

Proof. We know that M is a $\mathbb{Z}$-module, so it imbeds into some E which is an injective $\mathbb{Z}$-module. Let $f : M \to E$ be such an embedding. Also, there exists a ring homomorphism from $\mathbb{Z} \to R$.

By the previous proposition, $Hom_{\mathbb{Z}}(R, E)$ is an injective left R-module. Define $\phi : M \to Hom_{\mathbb{Z}}(R, E)$ by $m \mapsto \begin{cases} \phi(m) : & R \to E \\ & r \mapsto f(rm) \end{cases}$.

Then one can verify that ϕ is an injective R-module homomorphism. $\square$

7.2 Day 23 - March 4

Lemma 31. Suppose E is an injective module, and that A is a direct summand of E. Then A is injective.

Proof. Since A is a direct summand of E, there exists a module B such that $E = A \oplus B$. Let $\phi : A \to E$ be the inclusion taking $a \mapsto (a, 0)$ and let $\pi : E \to A$ be the projection $(a, b) \mapsto a$.

Suppose $0 \to M \xrightarrow{g} N$ is an exact sequence and that $f : M \to A$ is any map. Then ϕf is an injection into E. Since E is an injective, there exists $h_1 : N \to E$ such that $h_1 g = f\phi$. Then $\pi h_1 g = \pi\phi f = f$ (as $\pi\phi = 1$. Let $h = \pi h_1$. Then $hg = f$, so A is injective. $\square$

Proposition 82. Let R be a ring, and let E be a left R-module. Then E is injective if and only if every short exact sequence of the form $0 \to E \xrightarrow{f} M \xrightarrow{g} N \to 0$ splits.

Proof. Suppose E is an injective. Then $0 \to E \xrightarrow{f} M$ is exact, and $1_E : E \to E$, so since E is injective, there exists an $h : M \to E$ such that $hf = 1_E$. In other words, the sequence splits.

Conversely, by the last theorem from last class, we know we can imbed E into an injective I. That is, we can make a short exact sequence of the form $0 \to E \xrightarrow{f} I \xrightarrow{g} M \to 0$, where I is injective. This splits, so $I \cong E \oplus M$. Since I is injective and E is a summand of I, then by the lemma, E is also an injective. $\square$

Definition 106. Let M be an R-module. A *projective resolution* of M is an exact sequence $... \to P_i \to P_{i-1} \to ... \to P_0 \to M \to 0$, where each P_i is projective.

We similarly define a *free resolution* of M to be an exact sequence $... \to F_i \to F_{i-1} \to ... \to F_0 \to M \to 0$, where each F_i is free.

The definition of an *injective resolution* is slightly different. An injective resolution is an exact sequence of the form $0 \to M \to I^0 \to I^1 \to I^2 \to ...$, where each I_j is injective.

Remark 109. Homological algebra is the study of a module and its resolutions. Namely, it attempts to understand a module based on its resolutions (for instance, the projective dimension or injective dimension).

8 Integral Extensions

Let's now change gears and talk about integral extensions. All rings in this case will be commutative.

Definition 107. Let $R \subset S$ be rings. An element $u \in S$ is *integral* over R if there exists an equation of the form $u^n + r_1 u^{n-1} + ... + r_{n-1} u + r_n = 0$, with each $r_i \in R$.

That is, we say $u \in S$ is integral if it is the root of some monic polynomial in $R[x]$.

Remark 110. If each R_i is a field, then $u \in S$ is integral over R if and only if u is algebraic over R.

Example 114. If $R = \mathbb{Z}$, then $\sqrt{5}$ is integral over $\mathbb{Z}$. However, $\frac{1}{2}$ is not integral over $\mathbb{Z}$.

Proposition 83. Let $R \subset S$ be rings, and let $u \in S$. The following are equivalent:

1. u is integral over R.
2. $R[u]$ is a finitely generated R-module.
3. There exists a finitely generated R-submodule M of S, such that $1 \in M$ and $uM \subset M$.
4. There exists a faithful $R[u]$-module M such that M is finitely generated as an R-module. (Recall that a module is faithful if $\operatorname{Ann}_{R[u]} M = 0$.)

Proof. Suppose (1). Then there exists an equation of the form $u^n + r_1 u^{n-1} + ... + r_0 = 0$. Then one can show that $R[u] = R \cdot 1 + Ru + ... + Ru^{n-1}$, so $R[u]$ is finitely generated as an R-module. Thus (1) implies (2).

Suppose (2). Then let $M = R[u]$. Note that $R[u]$ is a finitely generated R-submodule of S such that $1 \in R[u]$ and $uR[u] \subset R[u]$. Thus (2) implies (3).

Suppose (3). Let M be the finitely generated R-submodule M of S such that $1 \in M$ and $uM \subset M$. By assumption, M is finitely generated as an R-module, so it suffices to show that M is a faithful $R[u]$-module. Since $uM \subset M$, then M is an $R[u]$-module. Furthermore, since $1 \in M$, if $x \in \operatorname{Ann}_{R[u]}(M)$, then $1 \cdot x = 0$, so $x = 0$. Thus M is faithful. That is, (3) implies (4).

Suppose (4). We use "the determinant trick". Let $m = Rx_1 + ...Rx_n$ be the given finitely generated R-module. since M is an $R[u]$ module, then $uM \subset M$. For $j = 1, ..., n$, we can write $ux_j = \displaystyle\sum_{i=1}^{n} a_{i,j} u_i$ for some $a_{i,j} \in R$. Let $A = [a_{i,j}]$.

In matrix form, we have that

$$\begin{pmatrix} u & & 0 \\ & \ddots & \\ 0 & & u \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Thus $(uI_n - A)\overline{x} = 0$. Multiplying by $adj(uI_n - A)$, we get on the left that $det(uI_n - A)I_n\overline{x} = 0$. Thus $det(uI_n - A) \cdot x_i = 0$ for all i. Thus $det(uI_n - A) \in \mathrm{Ann}_R(M)$, but since M is faithful, then $\mathrm{Ann}_R(M) = 0$, so $det(uI_n - A) = 0$. But $det(uI_n - A)$ is a monic polynomial in $R[u]$! Thus u is the root of a monic polynomial in $R[x]$, so u is integral. □

8.1 Day 24 - March 7

Recall from last class an integral extension:

Definition 108. Let $R \subset S$ be rings. An element $u \in S$ is *integral* over R if there exists an equation of the form $u^n + r_1u^{n-1} + ... + r_{n-1}u + r_n = 0$, with each $r_i \in R$.

That is, we say $u \in S$ is integral if it is the root of some monic polynomial in $R[x]$.

We actually proved that u being integral is equivalent to three other things. Let us not define another related notion:

Definition 109. Let $R \subset S$ be rings. We say S is an *integral extension* or simply *integral* if every element $s \in S$ is integral over R.

This leads to the following criterion:

Corollary 37. Let $R \subset S$ be rings, and let $u \in S$. Then the following are equivalent:

1. u is integral over R.

2. $R[u]$ is a finitely generated R-module.

3. $R[u]$ is integral over R.

Proof. Last time, we showed that (1) implies (2).

Suppose (2). Let $\alpha \in R[u]$. Let $M = R[u]$, which by assumption is a finitely generated submodule of S. Furthermore, $1 \in M$ and $\alpha M \subset M$. Then by criterion (3) of the conditions from last class, we know that α is integral over R. Since α was arbitrary, then $R[u]$ is integral over R. Thus (2) implies (3).

Suppose (3). Since $u \in R[u]$, then u is integral over S.

□

We can use induction to prove the following corollary:

Corollary 38. Let $R \subset S$ be rings. Let $u_1, ..., u_n \in S$. Then the following are equivalent:

1. $u_1, ..., u_n$ are integral over R.

2. $R[u_1, ..., u_n]$ is a finitely generated R-module.

3. $R[u_1, ..., u_n]$ is integral over R

This gives us a neat fact:

Corollary 39. Let $R \subset S$ be an integral extension. Then S is finitely generated as an R-algebra if and only if S is finitely generated as an R-module.

Proof. If S is finitely generated as an R-module, then $S = Ru_1 + ... + Ru_n$ for some $u_1, ..., u_n \in S$. Thus $S = R[u_1, ..., u_n]$.

Conversely, if S is finitely generated as an R-algebra, then $S = R[v_1, ..., v_n]$. But then by the previous corollary, S is finitely generated as an R-module. $\square$

Definition 110. Let $R \subset S$ be rings. We say the *integral closure* of R over S is $T = \{u \in S | u \text{ is integral over } R\}$. If $R = T$, then we say R is *integrally closed*.

Proposition 84. Let $R \subset S$ be rings, and let T be the integral closure of R over S. Then T is a subring of S containing R.

Proof. For all $r \in R$, r is the root of $x - r \in R[x]$. Thus r is integral over R, so $R \subset T$.

We must now show that T is a subring of S. It suffices to show that T is closed under addition, subtraction, and multiplication. Let $\alpha, \beta \in T$. Then $\alpha + \beta, \alpha - \beta, \alpha\beta \in R[\alpha, \beta]$. Since α and β are integral, then by the lemma, $R[\alpha, \beta]$ is an integral extension of R. Thus $\alpha + \beta, \alpha - \beta$, and $\alpha\beta$ are integral. That is, $\alpha + \beta, \alpha - \beta, \alpha\beta \in T$. Thus T is closed under addition, subtraction, and multiplication, so T is a subring of S. $\square$

Definition 111. If R is a domain, then we say R is *integrally closed* (not in the context of any other ring) if R is integrally closed in its field of fractions.

Proposition 85. Let R be a unique factorization domain. Then R is integrally closed.

Proof. Let F be the field of fractions of R. Let $\alpha \in F$ be integral over R. Write $\alpha = \frac{r}{s}$ where $\gcd(r, s) = 1$ and $r, s \in R$.

Then since α is integral over R, there exists a monic polynomial $f(x) = x^n + c_1x^{n-1} + ... + c_n \in R[x]$ such that $f(\alpha) = 0$.

Then $(\frac{r}{s})^n + c_1(\frac{r}{s})^{n-1} + ... + c_n = 0$, so $r^n + c_1sr^{n-1} + ... + c_ns^n = 0$. Thus $r^n = s(-c_1r^{n-1} - ... - c_ns^{n-1})$, so $s | r^n$ in R. But $\gcd(r, s) = 1 = \gcd(r^n, s)$.

Thus s is a unit, so $\alpha \in R$. In other words, R is its integral closure over F, so R is integrally closed. $\square$

Proposition 86. Let $R \subset S$ be rings, and let T be the integral closure of R over S. Let W be a multiplicatively closed set of R. Then $R_W \subset S_W$. Furthermore, the integral closure of R_W in S_W is T_W.

Proof. We will first show that T_W is the integral closure of R_W in S_W.

Let $\frac{t}{w} \in T_W$, so $t \in T$ and $w \in W$. Then since T is the integral closure of R in S, then there exits $c_i \in R$ such that $t^n + c_1t^{n-1} + ... + c_n = 0$.

Then, dividing by w^n, we get that $(\frac{t}{w})^n + \frac{c_1}{w}(\frac{t}{w})^{n-1} + ... + \frac{c_n}{w^n} = 0$. But each $\frac{c_i}{w^i} \in R_i$, so $\frac{t}{w}$ is integral over R_W.

Thus the integral closure of R_W over S_W contains T_W.

Conversely, suppose $\frac{u}{w} \in S_W$ and suppose $\frac{u}{w}$ is integral over R_w. Then there exist coefficients $\frac{c_i}{v}$ (note that we can combine to make a common denominator) such that $(\frac{u}{w})^n + \frac{c_1}{v}(\frac{u}{w})^{n-1} + ... + \frac{c_{n-1}}{v}\frac{u}{w} + \frac{c_n}{v} = 0$.

Multiplying by $(wv)^n$, we get that $\dfrac{(uv)^n + r_1(uv)^{n-1} + ... + r_{n-1}(uv) + r_n}{1} = \dfrac{0}{1}$, where $r_i = c_iw^iv^{i-1} \in R$. Therefore, there exist $w' \in W$ such that $w'[(uv)^n + r_1(uv)^{n-1} + ... + r_{n-1}(uv) + r_n] = 0$.

Therefore $(w'^n)[(uv)^n + r_1(uv)^{n-1} + ... + r_{n-1}(uv) + r_n] = 0 = (uvw')^n + r_1'(uvw')^{n-1} + ... + r_n'$, where $r_i' = r_i(w')^i \in R$.

Thus $w'uv \in T$. Let $t = w'uv$. Then $\frac{u}{1} = \frac{t}{vw'} \in T_W$, so $\frac{u}{w} = \frac{t}{vww'} \in T_W$.

Therefore, T_W is the integral closure of R_W over S_W. $\square$

Corollary 40. Let $R \subset S$ be rings, and let T be the integral closure of R over S. Let W be a multiplicatively closed subset of R. Then,

1. If S is integral over R, then S_W is integral over R_W.

2. If R is integrally closed over S, then R_W is integrally closed in S_W.

3. If R is an integrally closed domain, then so is R_W.

Proposition 87. Let $R \subset S$ be an integral extension, and let I be an ideal of S. Then $I \cap R$ is an ideal of R. Furthermore, the map $R/(I \cap R) \to S/I$ by $r + I \cap R \to r + I$ is a well-defined injective ring map.

Finally, S/I is integral over (the canonical image of) $R/(I \cap R)$.

Proof. We will first show that this map is a well-defined injective ring map. First, note that this map is well-defined since $I \cap R \subset I$. Also, it is easy to see that it preserves addition, subtraction, and multiplication.

It then suffices to show that this map is injective. Suppose $r + I = 0$. Then $r \in I$. Also, $r \in R$, so $r \in I \cap R$. Thus $r + I \cap R = I \cap R$, so this map is injective.

Now let us show that we have integrality (is that a word?). Let $\overline{s} \in S/I$. Since S is an integral extension of R, then $s^n + r_1 s^{n-1} + ... + r_n = 0$, then $\overline{s}^n + \overline{r}_1 \overline{s}^{n-1} + ... + \overline{r}_n = \overline{0}$, so $\overline{s}$ is integral over R. Thus S/I is integral over the canonical image of $R/(I \cap R)$.

$\square$

8.2 Day 25 - March 9

Let's continue with integral extensions.

Corollary 41. Let $R \subset S$ be an integral extensions. Let $p \in \operatorname{Spec} S$. Then $\mathfrak{p}$ is maximal if and only if $\mathfrak{p} \cap R$ is maximal.

Proof. If $\mathfrak{p} \in \operatorname{Spec} S$, then $S/\mathfrak{p}$ is an integral extension of $R/(\mathfrak{p} \cap R)$. Then $S/\mathfrak{p}$ is a field if and only if $R/(\mathfrak{p} \cap R)$ is a field. $\square$

Lemma 32. Let $N_1, ..., N_t$ be R-submodules of M. Let W be a multiplicatively closed set. Then $\bigcap_{i=1}^t (N_i)_W = (\cap_{i=1}^t N_i)_W$.

Proof. We use induction. It then suffices to show the case that $t = 2$.

Suppose $\alpha \in (N_1)_W \cap (N_2)_W$. Then $\alpha = \frac{n_1}{w_1} = \frac{n_2}{w_2}$, where $n_1 \in N_1$, $n_2 \in N_2$, and $w_1, w_2 \in W$.

Then there exists $w_3 \in W$ such that $\beta = w_3 w_2 n_1 = w_3 w_1 n_2$. But then $\beta \in N_1 \cap N_2$. Thus $\alpha = \frac{beta}{w_1 w_2 w_3} \in (N_1 \cap N_2)_W$.

Conversely, suppose $\gamma \in (N_1 \cap N_2)_W$. Then $\gamma = \frac{n}{w}$ for some $n \in N_1 \cap N_2$ and $w \in W$. Then $\gamma = \frac{n}{w}$ is a representation of γ as an element of both $(N_1)_W$ and $(N_2)_W$.

Thus $(N_1 \cap N_2)_W = (N_1)_W \cap (N_2)_W$. $\square$

Theorem 86 (Lying Over Theorem). Let $R \subset S$ be an integral extensions. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then there exists $\mathfrak{q} \in \operatorname{Spec} S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$. (We say "$\mathfrak{q}$ lies over $\mathfrak{p}$".)

Proof. We first will consider a special case: suppose $(R, \mathfrak{m})$ is a quasi-local ring and suppose that $\mathfrak{p} = \mathfrak{m}$. Then let $\mathfrak{n}$ be any maximal ideal of S. Then $\mathfrak{n} \cap R$ is a maximal ideal in R, so $\mathfrak{n} \cap R = \mathfrak{m}$, as desired.

We now move to the general case. Let $W = R \backslash \mathfrak{p}$. Then S_W is integral over R_W. Also, R_W is quasi-local, with maximal ideal $\mathfrak{p}_W$. Then, by the special case, there exists $\mathfrak{q}_W \in \operatorname{Spec} S_W$ such that $\mathfrak{q}_W \cap R_W = \mathfrak{p}_W$. But by the lemma, $\mathfrak{q}_W \cap R_W = (\mathfrak{q} \cap R)_W$. Thus $(\mathfrak{q} \cap R)_W = \mathfrak{p}_W$, so $\mathfrak{q} \cap R = \mathfrak{p}$. Also, $\mathfrak{q}$ is prime since $\mathfrak{q}_W$ is prime. $\square$

Theorem 87 (Incomparable). Let $R \subset S$ be an integral extension. Let $\mathfrak{p} \in \operatorname{Spec} R$. Suppose $\mathfrak{q}_1 \neq \mathfrak{q}_2 \in \operatorname{Spec} S$ lie over $\mathfrak{p}$. Then $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ and $\mathfrak{q}_2 \subsetneq \mathfrak{q}_1$.

Proof. We again get a special case: suppose $(R, \mathfrak{m})$ is quasi-local and that $\mathfrak{p} = \mathfrak{m}$. Then since $\mathfrak{q}_1 \cap R = \mathfrak{m}$ is maximal, then by the corollary, $\mathfrak{q}_1$ is maximal. Similarly, $\mathfrak{q}_2$ is maximal. Then, since distinct maximal ideals are incomparable, then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are incomparable, as desired.

We now move to the general case. Again, let $W = R \backslash \mathfrak{p}$. Then S_W is an integral extension over R_W. Note that $(\mathfrak{q}_1)_W \cap R_W = (\mathfrak{q}_1 \cap R)_W = \mathfrak{p}_W = (\mathfrak{q}_2)_W \cap R_W$. By the special case, since $(R_W, \mathfrak{p}_W)$ is a quasi-local ring, then $(\mathfrak{q}_1)_W$ and $(\mathfrak{q}_2)_W$ are incomparable. Thus $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are incomparable. $\square$

Theorem 88 (Going Up Theorem). Let $R \subset S$ be an integral extension. Suppose $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ are primes in $\operatorname{Spec} R$. Let $\mathfrak{q}_1 \in \operatorname{Spec} S$ lie over $\mathfrak{p}_1$. Then there exists $\mathfrak{q}_2 \supsetneq \mathfrak{q}_1$ such that $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$.

Proof. We once again get a special case: suppose $(R, \mathfrak{m})$ is quasi-local, and $\mathfrak{p}_2 = \mathfrak{m}$. Then from the Lying Over Theorem, there exists a maximal ideal $\mathfrak{n}$ containing $\mathfrak{q}_1$. Then $n \cap R = \mathfrak{m}$. Since $\mathfrak{p}_1$ was not maximal, then $\mathfrak{q}_1$ isn't either. Then since $\mathfrak{q}_2$ is maximal, we get that $\mathfrak{q}_2 \subsetneq \mathfrak{q}_1$.

In the general case, let $W = R \setminus \mathfrak{p}_2$. Observer that $(\mathfrak{q}_1)_W \cap R_W = (\mathfrak{p}_1)_W$. Then R_W is a quasi-local ring with maximal ideal $(\mathfrak{p}_2)_W$. Then by the special case, there exists $(\mathfrak{q}_2)_W \in \operatorname{Spec} S_W$ such that $\mathfrak{q}_2 \supset (\mathfrak{q}_1)_W$ and $(\mathfrak{q}_2)_W \cap R_W = (\mathfrak{p}_2)_W$. Therefore $\mathfrak{q}_w \supsetneq \mathfrak{q}_1$ and $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$. $\square$

Theorem 89. Let $R \subset S$ be an integral extension. Then $\dim R = \dim S$.

Proof. We'll show that for every $n \geq 0$, $\dim R \geq n$ if and only if $\dim S \geq n$.

($\Rightarrow$) Suppose $\dim R \geq n$. Then there is a prime chain in $\operatorname{Spec} R$ of the form $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_n$. By the Lying Over Theorem, there exists $\mathfrak{q}_0 \in \operatorname{Spec} S$ such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$. By repeated use of the Going Up theorem, we get that there exist $\mathfrak{q}_1 \supsetneq \mathfrak{q}_0$, $\mathfrak{q}_2 \supsetneq \mathfrak{q}_1$, etc. Thus $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq ... \subsetneq \mathfrak{q}_n$ is a strictly ascending chain in $\operatorname{Spec} S$. Thus $\dim S \geq n$.

($\Leftarrow$) Suppose $\dim S \geq n$. Then there exists a chain of prime ideals of the form $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq ... \subsetneq \mathfrak{q}_n$ lying in S. Then $\mathfrak{q}_0 \cap R \subsetneq \mathfrak{q}_1 \cap R \subsetneq ... \subsetneq ...\mathfrak{q}_n \cap R$ is a chain of prime ideals in $\operatorname{Spec} R$. By the incomparability theorem, the containments are strict. Thus $\dim R \geq n$.

Thus $\dim R = \dim S$. $\square$

Example 115. Let F be a subfield of $\mathbb{C}$ which is algebraic over $\mathbb{Q}$. Let R be the integral closure of $\mathbb{Z}$ in F. (Such an R is called an *algebraic number field*.) Then $\dim R = \dim \mathbb{Z} = 1$.

Example 116. Let $V = \{(z^3, z^4, z^5) \in \mathbb{C}^3 | z \in \mathbb{C}\}$. Consider $I(V) = \{f(x, y, z) \in \mathbb{C}[x, y, z] | f(p) = 0 \text{ for all } p \in V\}$.

The coordinate ring of V is defined to be $\mathbb{C}[x, y, z]/I(V)$. Note that $_1 = x^3 - yz \in I(V)$, $f_2 = z^2 - x^2y \in I(V)$, and $f_3 = y^2 - xz \in I(V)$. Then it turns out that $I(V) = (f_1, f_2, f_3)$.

Consider $\phi : \mathbb{C}[x, y, z] \to \mathbb{C}[t]$ given by $f(x, y, z) \to f(t^3, t^4, t^5)$. Then $\ker \phi = I(V)$. Therefore $\mathbb{C}[x, y, z]/I(V) \cong \operatorname{im} \phi = \mathbb{C}[t^3, t^4, t^5]$. Note that $\mathbb{C}[t]$ is an integral extension over $\mathbb{C}[t^3, t^4, t^5]$. Then, by the theorem, $1 = \mathbb{C}[t] = \dim \mathbb{C}[t^3, t^4, t^5] = \dim \mathbb{C}[x, y, z]/I(V)$.

This is a good thing! After all, the dimension should correspond to the intuitive sense of the dimension of the curve, and V is certainly dimension 1!

8.3 Day 26 - March 11

Last time we proved the Going Up Theorem. Today we will prove the Going Down Theorem, but before we can do that, we need some lemmas.

Lemma 33. (Division algorithm in polynomial rings) Let R be a ring, and let $f(x) \in R[x]$ be a monic polynomial. Then for all $g(x) \in R[x]$, there exist unique $q(x), r(x) \in R[x]$ such that $g = fq + r$ and $\deg r < \deg f$.

This is such a classical result, we will not prove it.

Corollary 42. Let $R \subset S$ be rings, and let $f(x), g(x) \in R[x]$, where $f(x)$ is monic. Then $f|g$ in $R[x]$ if and only if $f|g$ in $S[x]$.

Proof. Certainly, if $f|g$ in $R[x]$, then $f|g$ in $S[x]$.

Conversely, if $f|g$ in $S[x]$, then by the division algorithm, $g = fq_R + r_R$ in $R[x]$ and $g = fq_S + r_S$ in $S[x]$. But both of these lie in $R[x]$, so $r_R = r_S$ and $q_R = q_S$. Since $g = fq_S + r_S$ and $f|g$ in $S[x]$, then $r_S = 0$. Thus $g = fq_S = fq_R$. Since $q_R \in R[x]$, then $f|g$ in $R[x]$. $\square$

Proposition 88. Let $R \subset S$ be an extension of domains. Let $K = Q(R) \subset L = Q(S)$. Suppose R is integrally closed in K. Let $\alpha \in S$ be integral over R. Then α is algebraic over K. Furthermore, if $f(x) = Min(\alpha, K)$, $f(x) \in R[x]$.

Proof. Since $\alpha \in S$ is integral over R, then there exists a polynomial $h(x) \in R[x]$ such that $h(\alpha) = 0$. But $h \in R[x]$, so $h \in K[x]$. Thus α is algebraic over K.

Let $f(x) = Min(\alpha, K)$. Then, by the definition of the minimal polynomial, $f(x)|h(x)$ in $K[x]$. Let $\overline{L}$ be an algebraic closure of L. Then every root of $h(x)$ in $\overline{L}$ is integral over R (since, by definition, they all are the roots of a monic polynomial with coefficients in R).

Then, write $f(x) = x^n + c_1x^{n-1} + ... + c_n \in K[x]$, and also write $f(x) = (x - \alpha_1)...(x - \alpha_n)$, where each $\alpha_i \in \overline{L}$. Note that all α_i's are integral over R. But each c_j is the product and sum of the α_is, so the c_js are integral over R as well. Also, $c_j \in K$, so since R is integrally closed in K, then $c_j \in R$ for all j. Hence $f(x) \in R[x]$. □

Remark 111. Let $R \subset S$ be an extension of domains. Let $K = Q(R) \subset L = Q(S)$. Suppose R is integrally closed in K. Let $\alpha \in S$ be integral over R. By the previous proposition, α is algebraic over K, and $f(x) = Min(\alpha, K) \in R[x]$.

Then, if $g(x) \in R[x]$ is monic such that $g(\alpha) = 0$, then $f(x)|g(x)$ in $R[x]$.

Proposition 89. Let $R \subset S$ be an integral extension, and let I be an ideal of R. Suppose $u \in IS$. Then u is a root of a polynomial of the form $x^n + i_1x^{n-1} + ... + i_n$ where each $i_j \in I$. In fact, $i_j \in I^j$.

Proof. We again use the "determinant trick".

Since $u \in IS$, then there exist $i_j \in I_S$ and $s_j \in S$ such that $u = i_1s_1+...+i_rs_r$. Let $T = R[s_1, ..., s-r] \subset S$. Note that T is integral over R.

Since T is finitely generated as an algebra over R, then T is finitely generated as an R-module. Then $T = Ry_1 + ...Ry_l$ for some $y_i \in T$.

Furthermore, $u \in IT$. Then $uy_j \in ITy_j \subset IT = Iy_1 + ... + Iy_l$. Thus there exists $a_{i,j} \in I$ such that $uy_j = \displaystyle\sum_{i=1}^{l} a_{i,j}y_i$ for all j. Let $A = (a_{i,j})$, and let $\overline{y} = (y_1, ..., y_l)^T$. Then $A\overline{y} = u\overline{y}$, so $(A - uI)(\overline{y}) = 0$. Therefore $\det(A - uI) = 0$. But $\det(A - xI)$ is a monic polynomial of the form $x^n + i_1x^{n-1} + ... + i_n$. In fact, each $i_j \in I^j$, as desired. □

We can now prove the Going Down Theorem:

Theorem 90 (Going Down Theorem). Let $R \subset S$ be an integral extension of domains. Suppose that R is integrally closed in $Q(R)$. Suppose also that $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ are primes in $\operatorname{Spec} R$, with $\mathfrak{q}_1 \in \operatorname{Spec} S$ a prime ideal such that $R \cap \mathfrak{q}_1 = \mathfrak{p}_1$. Then there exists $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$.

Proof. Let $W = R \setminus \mathfrak{p}_0$, and let $T = S \setminus q_1$. Then $TW = \{wt | w \in W, t \in T\}$ is a multiplicatively closed subset of S.

We now wish to show that $p_0S \cap WT = \emptyset$. Suppose for the sake of contradiction that $wt \in \mathfrak{p}_0S$. Then, by the previous proposition, wt is the root of a monic polynomial of the form $g(x) = x^n + a_1x^{n-1} + ... + a_n$, where each $a_j \in \mathfrak{p}_0$.

Let $h(x) = g(wx)$. Then $h(x) = w^nx^n + w^{n-1}a_1x^{n-1} + ... + a_n$. Note that $h(t) = g(wt) = 0$. Let $f(x) = Min(t, K)$, where $K = Q(R)$. By the first Proposition, since R is integrally closed, then $f(x) \in R[x]$. But since $h(t) = 0$, then by the remark, $f(x)|h(x)$ in $R[x]$. That is, there exists $q(x) \in R[x]$ such that $h(x) = f(x)q(x)$.

Then, in $R/\mathfrak{p}_0[x]$, we have that $\overline{h}(x) = \overline{f}(x)\overline{q}(x) = \overline{w}^nx^n$ since the $a_j \in \mathfrak{p}_0$.

Recall that $R/\mathfrak{p}_0$ is a domain since $\mathfrak{p}_0$ is a prime ideal. Recall also that $f(x)$ was monic, so $\overline{f}(x) = x^r$ for some r. Therefore $f(x) = x^r + c_1x^{r-1} + ... + c_r$, where each $c_i \in \mathfrak{p}_0$. Thus $0 = f(t) = t^r + c_1t^{r-1} + ... + c_r$.

Rearranging, we get that $t^r = -c_1t^{r-1} - ... - c_r \in \mathfrak{p}_0S \subset \mathfrak{p}_1S \subset \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is prime, then $t \in \mathfrak{q}_1$. However, we defined $T = S \setminus \mathfrak{q}_1$, and $t \in T$, so this is a contradiction.

[Proof will be completed later.] □

8.4 Day 27 - March 14

We ended last class halfway through the proof of the Going Down Theorem:

Theorem 91. (Going Down Theorem) Let $R \subset S$ be an integral extension of domains. Suppose that R is integrally closed in $Q(R)$. Suppose also that $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ are primes in $\operatorname{Spec} R$, with $\mathfrak{q}_1 \in \operatorname{Spec} S$ a prime ideal such that $R \cap \mathfrak{q}_1 = \mathfrak{p}_1$. Then there exists $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$.

Proof. Let $W = R \setminus \mathfrak{p}_0$, and let $T = S \setminus q_1$. Then $TW = \{wt | w \in W, t \in T\}$ is a multiplicatively closed subset of S.

We showed last time that $\mathfrak{p}_0 S \cap WT = \emptyset$.

Now, let $\Lambda = \{I | I \text{ ideal of } S,\ I \supset \mathfrak{p}_0 S,\ I \cap WT = \emptyset\}$. Then $\mathfrak{p}_0 S \in \Lambda$, so Λ is nonempty. Also, any chain in Λ has an upper bound which is their union.

Thus by Zorn's Lemma, Λ has a maximal element, $\mathfrak{q}_0$. It must be the case that $\mathfrak{q}_0$ is prime [why?]. Then $\mathfrak{q}_0 \in \operatorname{Spec} S$.

Also, $W \subset WT$, so $\mathfrak{q}_0 \cap W \subset \mathfrak{q}_0 \cap WT = \emptyset$, so $\mathfrak{q}_0 \cap R \subset \mathfrak{p}_0$. But $\mathfrak{q}_0 \supset \mathfrak{p}_0 S \supset \mathfrak{p}_0$, so $\mathfrak{q}_0 \cap R \supset \mathfrak{p}_0$. Thus $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$.

Furthermore, since $\mathfrak{q}_0 \cap T = \emptyset$, then $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$. $\square$

Since we can "go down" one step, we can actually "go down" chains of primes:

Corollary 43. Let $R \subset S$ be an integral extension of domains, and suppose R is integrally closed. Suppose $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ is a chain of ideals in $\operatorname{Spec} R$. Suppose also that there exists $\mathfrak{q}_n \in \operatorname{Spec} S$ such that $\mathfrak{q}_n \cap R = \mathfrak{p}_n$. Then there exists $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq q_{n-1} \subsetneq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all i.

Corollary 44. Let $R \subset S$ be an integral extension of domains. Suppose R is integrally closed, and let $\mathfrak{q} \in \operatorname{Spec} S$. Then $ht(\mathfrak{q}) = ht(\mathfrak{q} \cap R)$.

Proof. We will first show that $ht(\mathfrak{q} \cap R) \geq ht(\mathfrak{q})$ for all integral extensions.

Let $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \ldots \subsetneq \mathfrak{q}_n = \mathfrak{q}$ be a chain of primes in S. Then, contracting to R, we get that $\mathfrak{q}_0 \cap R \subsetneq \mathfrak{q}_1 \cap R \subsetneq \ldots \subsetneq \ldots \mathfrak{q}_n \cap R = \mathfrak{q} \cap R$ (note that we get strict inequalities by the incomparability theorem). Hence, $ht(\mathfrak{q} \cap R) \geq n$.

It then suffices to show that $ht(\mathfrak{q}) \geq ht(\mathfrak{q} \cap R)$. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p} = \mathfrak{q} \cap R$. By the previous corollary, there exists $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_n = \mathfrak{q}$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all i. Thus $ht(\mathfrak{q}) \geq n$. $\square$

Remark 112. Let $R = K[x_1, \ldots, x_n]$, where each x_i is an indeterminant, and K is a field. Consider a monomial $dx_1^{\alpha_1} \ldots x_n^{\alpha_n}$, where each $\alpha_i \geq 0$, and $d \in K \setminus \{0\}$. Let $a_1, \ldots, a_{n-1}$ be positive integers.

For $i = 1, \ldots, n-1$, let $y_i = x_i - x_n^{a_i}$, and let $y_n = x_n$. Note that $K[x_1, \ldots, x_n] = k[y_1, \ldots, y_n] = R[y_n]$. Then, $dx_1^{\alpha_1} \ldots x_n^{\alpha_n} = d(y_1 + y_n^{a_1})^{\alpha_1} \ldots (y_{n-1} + y_n^{a_{n-1}})^{\alpha_{n-1}} y_n^{\alpha_n}$.

Note that the highest degree term in y_n is $dy_n^{\alpha_1 a_1 + \ldots + \alpha_{n-1} a_{n-1} + \alpha_n}$ (and there are other terms as well). Note that this is "monic" in y_n, in the sense that y_n has no y_i coefficients in front of it.

Let $\underline{\alpha} = \alpha_1, \ldots, \alpha_n$. Suppose $F(x_1, \ldots, x_n) = \sum_{\text{finite}} d_{\underline{\alpha}} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, and that $F(x_1, \ldots, x_n) \neq 0$.

We wish to do a change of variables such that this polynomial becomes "monic" in y_n . We already can make each monomial be monic, but this could backfire if the monomials have the same exponents and add up to a leading coefficient of 0.

However, we can make a choice of the a_i so that this doesn't happen. Since $F(x_1, \ldots, x_n)$ is a finite sum, then we can choose an integer c which is larger than any α_i appearing in a nonzero term in F. Let $a_i = c^i$ for $i = 1, \ldots, n-1$.

Then, with $y_i = x_i - x_n^{c_i}$ for $i = 1, \ldots, n-1$, and $y_n = x_n$, we get, as before, terms of the form $d_{\underline{\alpha}} y_n^{\alpha_n c^0 + \alpha_1 c + \ldots \alpha_{n-1} c^{n-1}}$.

But note $\alpha_n c^0 + \alpha_1 c + \ldots + \alpha_{n-1} c^{n-1} = \beta_n c^0 + \ldots + \beta_{n-1} c^{n-1}$ with $\beta_i < c$ for all i if and only if $\alpha_i = \beta_i$. (Because these are essentially base-c expansions for numbers, and these are distinct.)

Thus, each nonzero term of F becomes "monic" in y_n of distinct degrees in y_n. Hence, F becomes "monic" in y_n.

9 Affine Rings

Definition 112. Let K be a field. An *affine ring* (or an *affine K-algebra*) is a finitely generated K-algebra. That is, an affine ring is a ring of the form $K[u_1, ..., u_n]$, where the u_is may be either indeterminant or algebraic.

Remark 113. If $K[u_1, ..., u_n]$ is an affine ring, then define $\phi : K[x_1, ..., x_n] \to K[u_1, ..., u_n]$ by $f(x_1, ..., x_n) \to f(u_1, ..., u_n)$. Therefore $K[u_1, ..., u_n] \cong K[x_1, ..., x_n]/I$, where $I = \ker \phi$.

Thus, an equivalent definition of an affine ring is one which is the homomorphic image of a polynomial ring.

Lemma 34. (Noether Normalization Lemma) Let $A = K[u_1, ..., u_n]$ be an affine K-algebra. Then there exists $y_1, ..., y_r \in A$ which are algebraically independent over K, such that A is integral over the polynomial ring $R = K[y_1, ..., y_r]$.

We will prove the Noether Normalization Lemma next class.

Remark 114. Let A, K, and R be as in the Noether Normalization Lemma. Then, since A is finitely generated as a ring over $K \subset R$, then A is finitely generated as a ring over R. Then, since A is also integral over R, then A is finitely generated as an R-module.

Remark 115. Let $A = K[u_1, ..., u_n]$ be an affine K-algebra. Let $y_1, .., y_r$ be the algebraically independent elements over K guaranteed by the Noether Normalization Lemma. Then $\dim A = \dim R = r$.

9.1 Day 28 - March 16

We are about to prove the Noether Normalization Lemma.

However, we need an exercise first.

Exercise 33. Let $C \subset B \subset A$ be rings. Suppose B is integral over C, and A is integral over B. Then A is integral over C.

Lemma 35. (Noether Normalization Lemma) Let $A = K[u_1, ..., u_n]$ be an affine K-algebra. Then there exists $y_1, ..., y_r \in A$ which are algebraically independent over K, such that A is integral over the polynomial ring $R = K[y_1, ..., y_r]$.

Proof. Choose a set of $y_1, .., y_r \in A$ such that A is integral over $R = K[y_1, .., y_r]$ and such that r is the least possible. (Note that since $u_1, ..., u_n$ is such a set, then a "least possible" set exists, and $r \leq n$).

It then suffices to show that $\{y_1, ..., y_r\}$ is algebraically independent over K.

Suppose for the sake of contradiction that $\{y_1, ..., y_r\}$ is algebraically depended over K. Then there exists $f(T_1, ..., T_r) \in K[T_1, .., T_r] \setminus \{0\}$ such that $f(y_1, ..., y_r) = 0$.

But by the hideous lemma last class, there exists a change of variables of the form $X_1 = T_1 - T_r^{a_1}, ..., X_{r-1} = T_{r-1} - T_r^{a_{r-1}}, X_r = T_r$ such that $g(X_1, ..., X_r) := f(X_1 + X_r^{a_1}, ..., X_r) = cX_r^N + ... +$[lower order terms in X_r] is monic in terms of X_r.

Then let $z_1 = y_1 - y_r a^1, ... z_{r-1} = y_{r-1} - y_r^{a_{r-1}}, z_r = y_r$. Note that $g(z_1, ..., z_r) = f(z_1 + z_r^{a_1}, ..., z_r) = f(y_1, ..., y_r) = 0$. But also observe that $K[z_1, ..., z_r] = K[y_1, ..., y_r]$. Since z_r is a root of $\frac{g(z_1, ..., z_{r-1}, X_r)}{c}$, then z_r is integral over $K[z_1, ..., z_{r-1}]$.

But, by the exercise, integral extensions are transitive, so A is integral over $K[z_1, ..., z_{r-1}]$. Thus our choice of r was not minimal, and this is a contradiction. Thus $\{y_1, ..., y_r\}$ are algebraically independent over K. ☐

Definition 113. If $A = K[u_1, ..., u_n]$ is an affine K-algebra, and $y_1, ..., y_r$ are a set of algebraically independent elements guaranteed by the Noether Normalization Lemma, then we say that $R = K[y_1, ..., y_r]$ is called a *Noether normalization* for A.

Remark 116. Suppose A is an affine K-domain, and let $K[y_1, ..., y_r]$ be a normalization.

Then $Q(A)$ is algebraic over $k(y_1, ..., y_r)$, so $\{y_1, ..., y_r\}$ is a transcendence base for $Q(A)/K$. Therefore r is the transcendence degree of $Q(A)/K$.

Remark 117. In general, $\dim A = \dim K[y_1, ..., y_r]$. It is a fact that $\dim K[y_1, ..., y_r] = r$, so by transitivity, $\dim A = r$.

Theorem 92 (Nullstellensatz - Strong Form). Let A be an affine K-algebra which is a field. Then A is algebraic over K.

Proof. By the Noether Normalization Lemma, there exists a normalization $R = k[y_1, ..., y_r]$ of A.

Then $R \subset A$ is an integral extension. We showed that, in an integral extension, the top ring is a field if and only if the bottom ring is a field. Therefore $K[y_1, ..., y_r]$ is a field. However, the y_i are transcendental over K, so $K[y_1, ..., y_r$ is isomorphic to a polynomial ring.

Recall that polynomial rings are fields if and only if they have 0 variables. Thus $r = 0$, and $R = K$. Then A is integral over K, so A is algebraic over K.

$\square$

Corollary 45. Let K be an algebraically closed field, and let $R = K[x_1, ..., x_n]$ be a polynomial ring. Then $\mathfrak{m}$ is a maximal ideal of R if and only if $\mathfrak{m} = (x_1 - c_1, ..., c_n - c_n)$, where $c_1, ..., c_n \in K$.

Proof. Note that $(x_1 - c_1, ..., x_n - c_n)$ is the kernel of the ring surjection $K[x_1, ..., x_n] \to K$ given by $f \mapsto f(c_1, ..., c_n)$. Thus $\mathfrak{m}$ is always maximal, regardless of the structure of K.

Conversely, suppose $\mathfrak{m}$ is a maximal ideal of R. Note that there is a ring map $K \to R \to R/\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, then $\mathfrak{m} \cap K = (0)$, so this map is injective.

Consider $K \subset R/\mathfrak{m} = K[\overline{x}_1, ..., \overline{x}_n]$. Since $R/\mathfrak{m}$ is a field and finitely generated as a K-algebra, then by the Strong Form of the Nullstellensatz, $R/\mathfrak{m}$ is an algebraic extension of K. Since K is algebraically closed, then $R/\mathfrak{m} \cong K$. Therefore the map $K \to K[x_1, ..., x_n]/\mathfrak{m}$ is an isomorphism. Therefore, for each x_i, there exists $c_i \in K$ such that $\overline{x}_i = x_i + \mathfrak{m} = c_i + \mathfrak{m}$. Thus $x_i - c_i \in \mathfrak{m}$ for all i. Thus $\mathfrak{m} \supset (x_1 - c_1, ..., x_n - c_n)$. Since these ideals are both maximal, they are equal. Thus $\mathfrak{m} = (x_1 - c_1, ..., x_n - c_n)$. $\square$

9.2 Day 29 - March 18

Theorem 93 ("Trick of Rabinowitsch"). Let R be a commutative ring, and I be an ideal of R, and let x be an indeterminant over R. Then $\sqrt{I} = \bigcap\limits_{\substack{\mathfrak{m} \text{ maximal in } R[x] \\ \mathfrak{m} \supset I}} (\mathfrak{m} \cap R)$.

Proof. Certainly, $I \subset \bigcap\limits_{\substack{\mathfrak{m} \text{ maximal in } R[x] \\ \mathfrak{m} \supset I}} (\mathfrak{m} \cap R)$. Also, this is a radical ideal, so $\sqrt{I} \subset \bigcap\limits_{\substack{\mathfrak{m} \text{ maximal in } R[x] \\ \mathfrak{m} \supset I}} (\mathfrak{m} \cap R)$.

Let $f \in \bigcap\limits_{\substack{\mathfrak{m} \text{ maximal in } R[x] \\ \mathfrak{m} \supset I}} (\mathfrak{m} \cap R)$, and consider $J = (I, fx - 1) \subset R[x]$.

We wish to show that $J = R[x]$. Suppose for the sake of contradiction that $J \neq R$. Then let $\mathfrak{m}$ be a maximal ideal in $R[x]$ such that $J \subset \mathfrak{m}$. Therefore $I \subset \mathfrak{m}$, so $f \in \mathfrak{m}$. But $fx - 1 \in \mathfrak{m}$, so $1 \in \mathfrak{m}$. This contradicts the maximality of $\mathfrak{m}$. Thus $R = J$.

Therefore we can write $1 = i_1 g_1 + ... + i_n g_n + (fx - 1)g_{n+1}$, where $g_i \in R[x]$ and $i_j \in I$ for all j. If f is nilpotent, then $f \in \sqrt{I}$, so we're done. If f is not nilpotent, then $R_f \neq 0$.

Consider the ring homomorphism $\phi : R[x] \to R_f$ given by $h(x) \mapsto h(\frac{1}{f})$. Now let's apply ϕ to the earlier equation.

Then $1 = \frac{i_1 g_1'}{f^\alpha} + \frac{i_2 g_2'}{f^\alpha} + ... + \frac{i_n g_n'}{f^\alpha}$ in R_f. That is, there exists an f^s such that $f^{s+\alpha} = i_1 f^s g_1' + ... + i_n f^s g_n' \in I$. Thus $f \in \sqrt{I}$.

Thus $\sqrt{I} = \bigcap\limits_{\substack{\mathfrak{m} \text{ maximal in } R[x] \\ \mathfrak{m} \supset I}} (\mathfrak{m} \cap R)$.

$\square$

Proposition 90. Let A be an affine K-algebra. Let x be an indeterminant. Then every maximal ideal of $A[x]$ contracts to a maximal ideal of A.

Proof. Since A is an affine K-algebra, then so is $A[x]$. Let $\mathfrak{m}$ be a maximal ideal of $A[x]$.

Then $A[x]/\mathfrak{m}$ is algebraic over K by Hilbert's Nullstellensatz. Therefore we get the containment chain $K \subset A/(\mathfrak{m} \cap A) \subset A[x]/\mathfrak{m}$. Since the total extension is algebraic, then $A/(\mathfrak{m} \cap A)$ is integral over K. Also, $A/(\mathfrak{m} \cap A)$ is a domain. Since integral domain extensions over a field are still fields, then $A/(\mathfrak{m} \cap A)$ is a field.

Thus $\mathfrak{m} \cap A$ is a maximal ideal in A. $\square$

Theorem 94. Let A be an affine K-algebra, and let I be an ideal of A. Then $\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{m} \supset I}} \mathfrak{m}$.

Proof. By the Trick of Rabinowitsch, $\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \text{ maximal in } R[x] \\ \mathfrak{m} \supset I}} (\mathfrak{m} \cap R)$. Then by the previous proposition, if $\mathfrak{m}$ is maximal in $R[x]$, then $\mathfrak{m} \cap R$ is maximal in R. Thus $\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{m} \supset I}} \mathfrak{m}$.

$\square$

Remark 118. Suppose $K = \overline{K}$. Let $R = K[x_1, ..., x_n]$. Then every maximal ideal is of the form $\mathfrak{m}_p = (x_1 - c_1, ..., c_n - c_n)$ where $p = (c_1, ..., c_n) \in K^n$. Therefore $f \in \mathfrak{m}_p$ if and only if $f(p) = 0$. Then $I \subset \mathfrak{m}_p$ if and only if $f(p) = 0$ for all $f \in I$.

10 Algebraic Geometry

10.1 Day 30 - March 28

We're back from break!

Definition 114. Let K be a field, and let $n \geq 1$. Let $\mathbb{A}^n_K = K^n = \{(a_1, ..., a_n) | a_i \in K\}$. Then $\mathbb{A}^n_K$ is called *affine n-space over* K. The elements of $\mathbb{A}^n_K$ are called *points*.

Definition 115. Let $R = K[x_1, ..., x_n]$, and let $S \subset R$. The *zero set of* S is $Z(S) = \{p \in \mathbb{A}^n_K | f(p) = 0 \text{ for all } f \in S\}$. Then $Z(S)$ is called an (affine) *algebraic K-variety*.

Remark 119. Other people have other terms for varieties. Hartshorne and followers reserve the term "variety" for irreducible varieties. They use the term *algebraic set* for a not-necessarily-irreducible algebraic variety.

Example 117. Let $K = \mathbb{R}$. Let $f = y - x^2 \in \mathbb{R}[x, y]$. Then $Z(f)$ is the graph of the curve $y = x^2$.

Example 118. Let $K = \mathbb{R}$. Let $f = x - 1^2$ and $g = y^2 - y$ as elements of $\mathbb{R}[x, y]$. Let $S = \{f, g\}$. Then $Z(S) = \{(1, 0), (1, 1)\}$.

Remark 120. By generalizing the previous example, one can construct any finite set as an algebraic variety.

Example 119. Let $K = \mathbb{R}$. Let $f = z^2 - x^2 - y^2$ and let $g = z - 1$ as elements of $\mathbb{R}[x, y]$. Let $S = \{f, g\}$. Then $Z(S)$ is the circle of radius 1 lying in the plane $z = 1$.

Remark 121. Let K be a field, and let $R = K[x_1, ..., x_n]$. Let $S \subset T \subset R$. Then observe that $Z(T) \subset Z(S)$.

Proposition 91. Let K be the field, and let $R = k[x_1, ..., x_n]$. Then,

1. Let $\{S_\alpha\}_{\alpha \in I}$, where $S_\alpha \subset R$ for all α. Then $Z(\bigcup_\alpha S_\alpha) = \bigcap_\alpha Z(S_\alpha)$.
2. Let $S, T \subset R$. Then $Z(ST) = Z(S) \cup Z(T)$.
3. Let $S \subset R$. Then $Z(S) = Z((S))$, where (S) is the ideal generated by S.

4. Let $I \subset R$ be an ideal. Then $Z(I) = Z(\sqrt{I})$.
5. $\mathbb{A}^n_K = Z((0)) = Z(\emptyset)$ and $\emptyset = Z(1)$.

Proof. It is very easy to prove (1), so we will omit the proof.

Let us now prove (2). Certainly, $Z(ST) \subset Z(S) \cup Z(T)$. Conversely, suppose $p \in Z(ST)$ by $p \notin Z(S)$. Then there exists an $f \in S$ such that $f(p) \neq 0$.

Then, for all $g \in T$, $fg \in ST$, so $fg(p) = f(p)g(p) = 0$ as $p \in Z(ST)$. Since $f(p) \neq 0$ and this multiplication is taking place in k, then $g(p) = 0$. Since g was arbitrary, then $g(p) = 0$ for all $g \in T$. Thus $p \in Z(T)$, so $Z(ST) = Z(S) \cup Z(T)$, as desired.

Let us now prove (3). Since $S \subset (S)$, then $Z((S)) \subset Z(S)$. Let $p \in Z(S)$. Then, for all $f_i \in Z(S)$, $f_i(p) = 0$. Let $f \in (S)$. Then $f = g_1f_1 + ... + g_tf_t$ for some $g_i \in R$, so $f(p) = g_1(p)f_1(p) + ... + g_t(p)f_t(p) = 0$. Thus $f(p) = 0$ for all $f \in (S)$, so $p \in Z((S))$. Thus $Z(S) = Z((S))$, as desired.

Let us now prove (4). If $I \subset R$ is an ideal, then $I \subset \sqrt{I}$. Therefore, $Z(\sqrt{I}) \subset Z(I)$.

Let $p \in Z(I)$, and let $f \in \sqrt{I}$. Then there exists a t such that $f^t \in I$, so $f^t(p) = 0$. But this exponentiation is taking place in K, so $f(p) = 0$. Thus $p \in Z(\sqrt{I})$, so $Z(\sqrt{I}) = Z(I)$, as desired.

It is easy to verify (5) on your own. □

Corollary 46. The collection of zero sets satisfy the axioms of the closed sets of a topology on $\mathbb{A}^n_K$.

Definition 116. The *Zariski Topology* on $\mathbb{A}^n_K$ is the topology whose closed sets are the zero sets of polynomials.

Remark 122. The Zariski topology on $\mathbb{R}^n$ is strictly coarser than the Euclidean topology.

Corollary 47. Let $V = Z(S)$ be an affine K-variety. Then there exists $f_1, ..., f_t \in R = k[x_1, ..., x_n]$ such that $V = Z(f_1) \cap ... \cap Z(f_t)$. (In fact, one can choose $t \leq n$, but this result is hard.)

Proof. Recall that $V = Z(S) = Z((S))$. Since $R = k[x_1, .., x_n]$ is Noetherian, then each ideal is finitely generated. In particular, $(S) = (f_1, ..., f_t)$ for some $f_i \in R$.

Then, $V = Z(S) = Z((S)) = Z((f_1, ..., f_t)) = Z(f_1, ..., f_t) = Z(f_1) \cap ... \cap Z(f_t)$. □

Definition 117. Let $U \subset \mathbb{A}^n_K$. Define the *vanishing ideal* of U to be $I(U) = \{f \in R | f(p) = 0 \text{ for all } p \in U\}$.

Remark 123. Vanishing ideals are, in fact, ideals. Also, $0 \in I(U)$.

Proposition 92. Let $U \subset \mathbb{A}^n_K$. Then, $I(U)$ is a radical ideal.

Proof. Suppose $f \in \sqrt{I(U)}$. Then $f^r \in I(U)$ for some r, so $f^r(p) = 0$ for all $p \in U$. This exponentiation is taking place inside of K, a field, so $f(p) = 0$. Thus $f \in I(U)$. Since f was arbitrary, then $\sqrt{I(U)} = I(U)$. Thus $I(U)$ is a radical ideal. □

Remark 124. We have a correspondence between the set of affine K-varieties, and the set of radical ideals in $K[x_1, ..., x_n]$.

Proposition 93. For any variety V of $\mathbb{A}^n_K$, we have that $V = Z(I(V))$.

[proof omitted]

10.2 Day 31 - March 30

Recall from last class the following results:

Remark 125. We have a correspondence between the set of affine K-varieties, and the set of radical ideals in $K[x_1, ..., x_n]$.

Proposition 94. For any variety V of $\mathbb{A}^n_K$, we have that $V = Z(I(V))$.

However, the $I(Z(J)) \neq \sqrt{J}$ for an ideal J. Let's look at an example.

Example 120. Let $k = \mathbb{R}$, and $n = 1$. Let $J = (x^2+1) \subset \mathbb{R}[x]$. Then $Z(J) = \emptyset$. Therefore $I(Z(J)) = I(\emptyset) = \mathbb{R}[x]$. However, $\sqrt{(x^2+1)} \neq \mathbb{R}[x]$.

Theorem 95 (Nullstellensatz - geometric version). Let $K = \overline{K}$, and let J be an ideal of $K[x_1, ..., x_n]$. Then $I(Z(J)) = \sqrt{J}$.

Proof. If $p = (a_1, ..., a_n) \in \mathbb{A}^n_K$, then let $\mathfrak{m}_p = (x_1 - a_1, ..., x_n - a_n)$.

Recall that $f \in \mathfrak{m}_p$ if and only if $f(p) = 0$.

Therefore, for an ideal J, recall that $J \subset \mathfrak{m}_p$ if and only if $f(p) = 0$ for all $f \in J$, which is the case if and only if $p \in Z(J)$.

Recall that, as $K = \overline{K}$, then every maximal ideal is of the form $\mathfrak{m}_p$ for some $p \in \mathbb{A}^n_K$.

Now we are ready to show that $I(Z(J)) = \sqrt{J}$. Note that

$$\begin{aligned} f \in I(Z(J)) &\iff f(p) = 0 \text{ for all } p \in Z(J) \\ &\iff f \in \mathfrak{m}_p \text{ for all } p \in Z(J) \\ &\iff f \in \mathfrak{m}_p \text{ for all } \mathfrak{m}_p supset Z(J) \\ &\iff f \in \bigcap_{p \in Z(J)} \mathfrak{m}_p \end{aligned}$$

However, $\bigcap_{p \in Z(J)} \mathfrak{m}_p = \bigcap_{\substack{\mathfrak{m} \text{ maximal} \\ \mathfrak{m} \supset J}} \mathfrak{m} = \sqrt{J}$.

Thus $f \in I(Z(J))$ if and only if $f \in \sqrt{J}$. □

Corollary 48. If $K = \overline{K}$, then there exists a bijective, inclusion-reversing correspondence between subvarieties of $\mathbb{A}^n_K$ and radical ideals of $K[x_1, ..., x_n]$.

And that's everything we need to know about algebraic geometry!

11 Invariant Theory

Now we get to just talk about a random grabbag of topics! Let's start with invariant theory.

Let K be a field, and let $R = K[x_1, ..., x_n]$. Let S_n act on R by $\sigma(f(x_1, ..., x_n)) = f(x_{\sigma(1)}, ..., x_{\sigma(n)})$. (Really, what we are doing is defining a $\tilde{\sigma} : R \to R$ for all $\sigma \in S_n$. Then each $\tilde{\sigma}$ is an automorphism of R fixing K, so S_n is (isomorphic to) a subgroup of $Aut_K(R)$.)

Definition 118. Let $R^{S_n} := \{f \in R | \sigma(f) = f \text{ for all } \sigma \in S_n\}$. Then we call R^{S_n} the *fixed subring* of R or an *invariant subring* of R.

Way back when, we showed that $R^{S_n} = K[s_1, ..., s_n]$, where the s_is are the elementary symmetric functions in $x_1, ..., x_n$.

Remark 126. The "first problem of Invariant Theory" is the following: If $R = K[x_1, ..., x_n]$, and G is a finite subgroup of $Aut_K(R)$, then is R^G a finitely generated K-algebra?

Hilbert proved the answer was yes in 1890. Later, he showed (in some cases), what the generators would be.

Noether gave a cool proof in the 1920s, so let's look at that.

Theorem 96. Let R be a finitely generated K-algebra, and let G be a finite subgroup of $Aut_K(R)$. Then R^G is a finitely generated K-algebra.

Proof. Let $R = K[u_1, ..., u_n]$, let $r = |G|$, and let t be an indeterminant. For each $1 \leq i \leq n$, consider $f_i(t) = \prod_{\sigma \in G} (t - \sigma(u_i)) = t^r + c_{i,1}t^{r-1} + ... + c_{i,r}$.

Note that $f_i^{\sigma}(t) = f_i(t)$ for all $\sigma \in G$. Therefore, $\sigma(c_{i,j}) = c_{i,j}$ for all i, j, so $f_i(t) \in R^G[t]$.

Let $S = K[c_{i,j}]_{\substack{1 \leq i \leq n \\ 1 \leq j \leq r}} \subset R^G$.

Note that $f_i(u_i) = 0$ for all i, so each u_i is integral over S. Therefore, $R = K[u_1, ..., u_n]$ is integral over S. However, R is a finitely generated S-algebra (in particular, $R = S[u_1, ..., u_n]$), so R is a finitely generated S-module.

But since S is a finitely generated K-algebra, then by the Hilbert basis theorem, S is Noetherian.

Therefore, R is a Noetherian S-module, so R^G is an S-submodule of R. Hence, R^G is a finitely generated S-module. Therefore, R^G is a finitely generated S-algebra. Since S is a finitely generated K-algebra, then by the transitivity of finitely-generatedness, R^G is a finitely generated K-algebra.

$\square$

Corollary 49. With R and G as above, then by the Noether Normalization Lemma, there exists $y_1, ..., y_l \in R^G$ which are algebraically independent, such that R is a finitely generated $K[y_1, ..., y_l]$-module.

Note that this is a bit weaker than what happened when $G = S_n$, where $K[y_1, ..., y_l] = R^G$, instead of the latter only being finitely generated as a module over the former.

Question 3. Let R be a Noetherian domain, and let $K = Q(R)$. Let $\overline{R}$ denote the integral closure of R in K. Is $\overline{R}$ a finitely-generated R-module?

Question 4. Let R be a Noetherian, integrally closed domain. Let L be a finite algebraic field extension of $K = Q(R)$. Let S be the integral closure of R in L. Is S a finitely generated R-module?

The answer to Question 3 is yes, in the case that R is a finitely generated k-algebra with *char* $k = 0$.

12 Extensions Of A Field of Fractions

12.1 Day 32 - April 1

Our final will be on Monday May 2, 10-12. It will be open note, but not open laptop.

Remark 127. Recall the following results about separable extensions: Let E/F be a finite separable extension of fields. Since E/F is finite, it is automatically algebraic.

Let $\sigma_1, ..., \sigma_r$ be the distinct field embeddings of E into $\overline{E}$ fixing F. Recall that $\text{Tr}_F^E = \sigma_1 + ... + \sigma_r : E \to F$ is an F-linear functional. Furthermore, recall that since E/F is separable, then $\text{Tr}_F^E \neq 0$.

Theorem 97. Let E/F be a finite separable extension of fields. Let $\{\alpha_1, ..., \alpha_r\}$ be an F-basis for E. Then there exists a basis $\{\beta_1, ..., \beta_r\}$ of E such that $\text{Tr}_F^E(\beta_i \alpha_j) = \delta_{i,j}$ for all i, j.

Proof. Let $E^* = Hom_F(E, F)$. Then $\dim_F E^* = \dim_F(E) \cdot \dim_F(F) = \dim_F E$. Define $\alpha_j^* : E \to F$ by $\alpha_j^* : \alpha_i \mapsto \begin{cases} 0 \text{ if } i \neq j \\ 1 \text{ if } i = j \end{cases}$. That is, $\alpha_j^*(\alpha_i) = \delta_{i,j}$.

(Vocabulary lesson: we say that $\{\alpha_1^*, ..., \alpha_r*\}$ is the dual basis for E^* corresponding to $\{\alpha_1, ..., \alpha_r\}$.)

For each $\beta \in E$, define $f_\beta : E \to F$ by $\gamma \to \text{Tr}_F^E(\beta\gamma)$. One can verify that f_β is F-linear, so $f_\beta \in E^*$.

Thus the map $\phi : E \to E^*$ by $\beta \mapsto f_\beta$ is F-linear. We now wish to show that ϕ is injective. Suppose $\phi(\beta) = 0$ for some $\beta \in E$. Then, for all $\gamma \in E$, $0 = \phi(\beta)(\gamma) = f_\beta(\gamma) = \text{Tr}_F^E(\beta\gamma)$. If $\beta \neq 0$, then $\beta E = E$, so it must be that $\text{Tr}_F^E = 0$, which is nonsense. Therefore, $\beta = 0$, so ϕ is injective.

Since $\dim_F(E) = \dim_F(E^*)$, then ϕ is also surjective, so ϕ is an isomorphism.

Let $\beta_i = \phi^{-1}(\alpha_i^*)$ for all i. Then

$$\begin{aligned}\mathrm{Tr}_F^E(\beta_i\alpha_j) &= f_{\beta_i}(\alpha_j) \\ &= \phi(\beta_i)(\alpha_j) \\ &= \phi(\phi^{-1}(\alpha_i^*))(\alpha_j) \\ &= \alpha_i^*(\alpha_j) \\ &= \delta_{i,j}\end{aligned}$$

as desired.

□

Lemma 36. Let R be a Noetherian integrally closed domain. Let K be the field of fractions of R. Let L be a finite separable extension of K. Let S be the integral closure of R in L. Let $W = R \setminus \{0\}$. Then $S_W = L$ (and in particular, $Q(S) = L$).

Proof. Certainly, $S_W \subset L$.

Conversely, let $\alpha \in L$. Then α is algebraic over $K = Q(R)$, so there exists $c_i, d \in R$ such that $\alpha^n + \frac{c_{n-1}}{d}\alpha^{n-1} + ... + \frac{c_0}{d} = 0$. Multiplying by d^n, we get that $(d\alpha)^n + c_{n-1}(d\alpha)^{n-1} + ... + c_1 d^{n-2}(d\alpha) + c_0 d^{n-1} = 0$. Thus, d_α is integral over R, so $d\alpha = f \in S$. Then $\alpha = \frac{f}{d} \in S_W$.

Thus $L \subset S_W$, so $L = S_W$, as desired. □

Lemma 37. Let R be a Noetherian integrally closed domain. Let K be the field of fractions of R. Let L be a finite separable extension of K. Let S be the integral closure of R in L. Then $\mathrm{Tr}_K^L(S) \subset R$.

Proof. Let $u \in S$. Then u is a root of a monic polynomial $f(x) \in R[x]$. Let $\sigma : L \to \overline{L}$ be an embedding fixing K. Since $R \subset K$, then σ fixes the coefficients of $f(x)$. Thus $\sigma(u)$ is a root of $f(x)$. Therefore $\sigma(u) \in \overline{L}$ is integral over R. Therefore $\mathrm{Tr}_K^L(u) = \sigma_1(u) + ... + \sigma_r(u)$ is integral over R and is in K. Since R is integrally closed in K, then $\mathrm{Tr}_K^L(u) \in R$, as desired.

□

Theorem 98. Let R be a Noetherian integrally closed domain. Let K be the field of fractions of R. Let L be a finite separable extension of K. Let S be the integral closure of R in L. Then S is finitely generated as an R-module.

Proof. Let $\alpha_1, ...\alpha_r\}$ be a K-basis for L. By the first lemma, there exist $\alpha_i' \in S$ and a $d \in R$ such that $\alpha_i = \frac{\alpha_i'}{d}$ for $i = 1, ..., r$. Then $\{\alpha_1', ..., \alpha_r'\}$ is also a K-basis for L¡ so we can assume $\{\alpha_1, ..., \alpha_r\} \subset S$.

By the previous theorem, there exists a K-basis for L $\{\beta_1, ..., \beta_r\}$ such that $\mathrm{Tr}_K^L(\beta_i\alpha_j) = \delta_{i,j}$.

We now wish to show that $S \subset R\beta_1 + ... + R\beta_r$.

Let $u \in S$. We already know that $S \subset K\beta_1 + ... + K\beta_r$, so there exists $c_i \in K$ such that $u = c_1\beta_1 + ... + c_r\beta_r$. Then, $u\alpha_i = c_1\beta_1\alpha_i + ... + c_r\beta_r\alpha_i$, so $\mathrm{Tr}_K^L(u\alpha_i) = c_i$. Since $u\alpha_i \in S$, then by the second lemma, $\mathrm{Tr}_K^L(u\alpha_i) \in R$. Thus $c_i \in R$ for all i, so $u \in R\beta_1 + ... + R\beta_r$.

Then, since R is Noetherian, $M = R\beta_1 + ... + R\beta_r$ is a Noetherian R-module. Therefore, S is an R-submodule of M, so S is finitely generated as an R-module. □

Theorem 99. Let K be a field with *char* $K = 0$, and let R be an affine K-domain. Then the integral closure of R in its field of fractions is a finitely generated R-module (and is therefore Noetherian).

Proof. By the Noether Normalization Lemma, there exists algebraically independent elements $y_1, ..., y_d \in R$ such that R is a finitely generated module over the subring $T = k[y_1, ..., y_d]$ (so the extension $T \subset R$ is integral).

Let E be the field of fractions of R, and let S be the integral closure of R in E. Note that S is also the integral closure of T in E.

Let F be the field of fractions of T. Since R is a finitely generated T-module, then E is a finitely generated F-module. As *char* $K = 0$, then E/F is separable.

Therefore, by the previous theorem, S is a finitely generated T-module. Since $T \subset R \subset S$, then S is also finitely generated as an R-module. □

12.2 Day 33 - April 4

Recall the following theorems from last class:

Theorem 100. Let R be a Noetherian integrally closed domain. Let $F = Q(R)$, and let E be a finite separable extension of F, and let S be the integral closure of R in E. Then S is finitely generated as an R-module.

Theorem 101. Let K be a field of characteristic 0, and let R be an affine K-domain. Let $E = Q(R)$, and let S be the integral closure of R in E. Then S is a finitely-generated R-module.

Let's also talk about some old definitions.

Remark 128. Let F be a field of characteristic $\mathfrak{p}$, and let E/F be a field extension. Recall the following:

1. We say $\alpha \in E$ is purely inseparable over F if $\alpha^{p^n} \in F$ for some p^n.

2. We say E/F is purely insepable if each $\alpha \in E$ is purely inseparable over F.

3. If E/F is finite, then E/F is purely inseparable if and only if $E^{p^n} \subset F$ for some n.

4. Let $F^{p.i.} = \{\alpha \in E | \alpha \text{ is purely inseparable over } F\}$. We called $F^{p.i.}$ the purely inseparable closure of F in E, andit is a subfield of E containing F.

5. If E/F is normal, then $E/F^{p.i.}$ is separable and $F^{p.i.}/F$ is purely inseparable.

Remark 129. Let R be a domain of characteristic $\mathfrak{p}$. Let K be an algebraic closure of $Q(R)$. For any $c \in R$ and $n \geq 1$, then the polynomial $x^{p^n} - c \in R[x] \subset K[x]$ has a unique root in K. (In particular, if α is a root, then $x^{p^n} - c = (x - \alpha)^{p^n}$.)

We will denote this root by $c^{\frac{1}{p^n}}$.

Furthermore, for $c, d \in R$, we have that $c^{\frac{1}{p^n}} + d^{\frac{1}{p^n}} = (c + d)^{\frac{1}{p^n}}$ and $c^{\frac{1}{p^n}} \cdot d^{\frac{1}{p^n}} = (c \cdot d)^{\frac{1}{p^n}}$

Let $R^{\frac{1}{p^n}} = \{c^{\frac{1}{p^n}} | c \in R\}$. Then $R^{\frac{1}{p^n}}$ is a subring of K containing R. Also, $R \subsetneq R^{\frac{1}{p}} \subsetneq R^{\frac{1}{p^2}} \subsetneq ... \subset K$.

However, note that, for all $n \geq 1$, $R \cong R^{\frac{1}{p^n}}$ by the isomorphism $c \mapsto c^{\frac{1}{p^n}}$.

Theorem 102. Let E/F be a field extension, and let *char* $F = p$. Suppose $\{y_1, ..., y_d\} \subset E$ is algebraically independent over F. Let $n \geq 1$. For any algebraic extension L/F, then $\{y^{\frac{1}{p^n}}, ..., y^{\frac{1}{p^n}}\}$ is algebraically independent over L.

Proof. Recall that $\{y_1, ..., y_d\}$ is algebraically independent over F if and only if $\operatorname{Tr}.\ deg.\ (F(y_1, ..., y_d)/F) = d$. It then suffices to show that $\operatorname{Tr}.\ deg.\ (L(y_1^{\frac{1}{p^n}}, ..., y_d^{\frac{1}{p^n}})/L) = d$. However, we can do so by a big complicated picture. $\square$

From this, we can conclude that the p-th root of an indeterminant will still be an indeterminant.

Lemma 38. Let F be a field of characteristic $p > 0$. Let $x_1, ..., x_d$ be indeterminants over F, and let L be a finite field extension of F. Then $L[x^{\frac{1}{p^n}}, ..., x^{\frac{1}{p^n}}]$ is a finitely generated $F[x_1, ..., x_d]$-module.

[Proof omitted.]

12.3 Day 34 - April 8

(There was no class on Wednesday.)

Hint for a homework problem: Let $\alpha \in \bigcap_{\mathfrak{m} \text{ maximal}} R_{\mathfrak{m}}$. Then let $\alpha = \frac{a}{b}$. We want to show that $((b) :_R a) = R$.

Recall this theorem:

Theorem 103. Let R be a Noetherian integrally closed domain. Let K be the field of fractions of R. Let L be a finite separable extension of K. Let S be the integral closure of R in L. Then S is finitely generated as an R-module.

Proof. $\square$

Theorem 104. Let K be a field, and let $A = K[x_1, ..., x_d]$ be a polynomial ring over K. Let $F = Q(A) = K(x_1, ..., x_d)$. Let E be a finite field extension of F, and let B be the integral closure of A in E. Then B is finitely generated as an A-module.

Proof. We will first show the theorem when E/F is separable or purely inseparable.

By the recalled theorem, if E/F is separable, then the theorem is true.

If E/F is purely inseparable, let *char* $K = p$, and write $E = F(\alpha_1, ..., \alpha_l)$ where $\alpha_i^{p^n} \in F$ for a fixed n and for all i. Since F is the field of fractions of $A = K[x_1, ..., x_n]$, then $\alpha_i^{p^n} = \frac{f_i(x_1,...,x_d)}{g_i(x_1,...,x_d)}$ for some $f_i, g_i \in K[x_1, ..., x_d]$. Note that we can in fact commonize the denominators and assume $g_i(x_1, ..., x_d) = g(x_1, ..., x_d)$ for some $g \in K[x_1, ..., x_d]$.

Then, $\alpha_i = \frac{f_i(x_1,...,x_d)^{\frac{1}{p^n}}}{g(x_1,...,x_d)^{\frac{1}{p^n}}} = \frac{\tilde{f}_i(x_1^{\frac{1}{p^n}},...x_d^{\frac{1}{p^n}})}{\tilde{g}(x_1^{\frac{1}{p^n}},...x_d^{\frac{1}{p^n}})}$, where $\tilde{f}_i, \tilde{g} \in K^{\frac{1}{p^n}}[x_1^{\frac{1}{p^n}}, ..., x_d^{\frac{1}{p^n}}]$.

Let S be the set of all the p^nth roots of all the coefficients of the f_is and g. Let $K' = K(S) = K[S]$. Then K'/K is finite and purely inseparable. Also, $\tilde{f}_i, \tilde{g} \in K'[x_1^{\frac{1}{p^n}}, ..., x_1^{\frac{1}{p^n}}] = T$. Let $L = Q(T) = K'(x_1^{\frac{1}{p^n}}, ..., x_1^{\frac{1}{p^n}})$. Note that all $\alpha_i \in L$.

Then, let C denote the integral closure of A in L. We wish to show that $C = T$. Certainly, T is integral over A since $(x_i^{\frac{1}{p^n}})^{p^n} = x_i \in A$ for all i and $K'^{p^s} \subset K$ for some s. Thus $T \subset C$. However, T is integrally closed in $Q(T) = L$. Thus $T = C$.

Recall that $C = K'[x_1^{\frac{1}{p^n}}, ..., x_1^{\frac{1}{p^n}}] = T$ is finitely generated as a module over $K'[x_1, .., x_d]$, which in turn is finitely generated as a module over A (since $[K' : K] < \infty$). Then, by transitivity of finitely-generated-ness, C is a finitely-generated A-module. Since B is an A-submodule of C, and A is Noetherian, then B is finitely generated as an A-module. This completes the proof in the purely inseparable case.

If E/F is neither separable nor purely inseparable, then we proceed as follows. First, we will show that we can assume without loss of generality that E/F is normal.

To this end, let $\tilde{E}$ be the normal closure of E/F. Let $\tilde{B}$ be the integral closure of A in $\tilde{E}$. Suppose $\tilde{B}$ is a finitely generated A-module. If we can show that $\tilde{B}$ is a Noetherian A-module, then since B is an A-submodule of $\tilde{B}$, then B is a finitely generated A-module.

Therefore, it suffices to show the case where E/F is finite and normal. Let $E' = F^{p.i}$. Then E'/F is purely inseparable, and E/E' is separable. Let B' be the integral closure of A in E'. By the purely-inseparable case, B' is finitely generated as an A-module. Then B' is a Noetherian, integrally closed domain (since $Q(B') = E'$). Therefore B is the integral closure of B' in E.

By the separable case, B is a finitely generated B'-module. Since we assumed that B' is a finitely generated A-module, then by transitivity of finitely-generated-ness, B is a finitely generated A-module. $\square$

13 Representation Theory Revisited

13.1 Day 35 - April 11

Recall the following things about group-rings.

Remark 130. If G is a finite group, and $\mathbb{C}$ is the field of complex numbers, then

$$\begin{aligned} \mathbb{C}[G] &= B(I_1) \times ... \times B(I_t) \\ &\cong n_1 I_1 \oplus ... \oplus n_t I_t \end{aligned}$$

, where $I_1, ..., I_t$ represent all the simple left ideals of $\mathbb{C}[G]$ up to isomorphism, and $B(I_j)$ is the sum of all the left ideals of $\mathbb{C}[G]$ which are isomorphic to I_j.

We then have the following results

1. t is equal to the number of conjugacy classes of G.

2. $n_i = \dim_{\mathbb{C}} I_i$ for $1 \leq i \leq t$.

3. $B(I_i) \cong M_{n_i}(\mathbb{C})$ for $1 \leq i \leq t$.

Remark 131. Let R be a commutative ring, and let G be a finite group. Then $Z(R[G]) = Rz_1 \oplus ... \oplus Rz_t$, where $z_i = \sum_{g \in C_i}$, where $C_1, ..., C_t$ are the distinct conjugacy classes of G.

In particular, $Z(\mathbb{Z}[G]) = \mathbb{Z}z_1 \oplus ... \oplus \mathbb{Z}z_t \subset \mathbb{C}z_1 \oplus ... \oplus \mathbb{C}z_t = Z(\mathbb{C}[G])$.

For the rest of today, let A be the integral closure of $\mathbb{Z}$ in $\mathbb{C}$. That is, A denotes the set of algebraic integers.

We will now build up to the fact that $n_i \Big| |G|$ for all i.

Proposition 95. For each i, let $e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g$. Then $z_i \in Ae_1 + ... + Ae_t$.

Proof. Recall that $Z(\mathbb{C}[G]) \cong \mathbb{C}e_1 \times ... \times \mathbb{C}e_t$ (as an internal direct product).

Since $z_i \in Z(\mathbb{C}[G]) = \mathbb{C}e_1 \times ... \times \mathbb{C}e_t$., then there exist $\alpha_i \in \mathbb{C}$ such that $z_i = \alpha_1 e_1 + ... + \alpha_t e_t$. Note that $z_i \in Z(\mathbb{Z}[G]) = \mathbb{Z}z_1 + ...\mathbb{Z}z_t$.

As $Z(\mathbb{Z}[G])$ is a commutative ring, and is finitely generated as a $\mathbb{Z}$-module, then $Z(\mathbb{Z}[G])$ is integral over $\mathbb{Z}$. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $f(z_i) = 0$. Then $f(\alpha_1 e_1 + ...\alpha_t e_t) = 0$.

That is,

$$\begin{aligned} 0 &= f(\alpha_1 e_1 + ...\alpha_t e_t) \\ &= f(\alpha_1 e_1) + ... + f(\alpha_t e_t) \\ &= f(\alpha_1)e_1 + ...f(\alpha_t)e_t \end{aligned}$$

Note that the second equality is because $e_i e_j = 0$ for $i \neq j$, and the third equality is because $e_i e_i = e_i$.

But since $e_1, ...e_t$ is linearly independent over $\mathbb{C}$, then each $f(\alpha_j) = 0$ for all j. Thus $\alpha_j \in A$ for all j, so $z_i \in Ae_1 + ... + Ae_t$. ☐

Lemma 39. Let χ be any character for G and let $g \in G$. Then $\chi(g) \in A$ for all $g \in G$.

Proof. Recall the definition of $\chi(g)$: $\chi(g) = \mathrm{Tr}(\rho(g))$ where $\rho : G \to GL_{\mathbb{C}}(V)$ is a representation. Since $g^n = 1$ for some n, then $\rho(g)^n = 1_V$. Thus every eigenvalue of $\rho(g)$ is an n-th root of unity.

But each n-th root of unity is an algebraic integer! Also, the trace of a matrix is the sum of its eigenvalues (with some multiplicities), so $\chi(g) = \mathrm{Tr}(\rho(g))$ is the sum of some algebraic integers. Since A is closed under addition (because it is a ring), then $\chi(g) \in A$. ☐

Theorem 105. For each $i = 1, ..., t$, $n_i \Big| |G|$.

Proof. Recall that $\frac{|G|}{n_i} e_i = \sum_{g \in G} \chi_i(g^{-1})g = \sum_{j=1}^{t} \chi_i(g_j^{-1})z_j$, where each $g_j \in C_j$.

But this is in $Az_1 + ... + Az_t$ since $\chi_i(g_j^{-1}) \in A$ by the Lemma. By the proposition, $Az_1 + ... + Az_t \subset Ae_1 + ... + Ae_t$. Thus $\frac{|G|}{n_i} \in A$. However, we can see that $\frac{|G|}{n_i} \in \mathbb{Q}$, so $\frac{|G|}{n_i} \in A \cap \mathbb{Q} = \mathbb{Z}$. In other words, $n_i \Big| |G|$. ☐

Now let's talk about the representations of products of groups.

Definition 119. Let $\rho_1 : G_1 \to GL_{\mathbb{C}}(V_1)$ and let $\rho_2 : G_2 \to GL_{\mathbb{C}}(V_2)$ be representations of some groups G_1 and G_2.

Define $\rho_1 \otimes \rho_2 : G_1 \times G_2 \to GL_{\mathbb{C}}(V_1 \otimes_{\mathbb{C}} V_2)$ by $(g_1, g_2) \mapsto \rho_1(g_1) \otimes \rho_2(g_2)$.

Remark 132. One can verify that $\rho_1 \otimes \rho_2$ is a group homomorphism.

Exercise 34. Show that $\mathrm{Tr}(\phi \otimes \psi) = \mathrm{Tr}(\phi) \cdot \mathrm{Tr}(\psi)$.

From this, one gets that $\chi_{\rho_1 \otimes \rho_2}((g_1, g_2)) = \chi_{\rho_1}(g_1) \cdot \chi_{\rho_2}(g_2)$.

Corollary 50. The following are equivalent:

1. $\rho_1 \otimes \rho_2$ is irreducible as a representation
2. $\chi_{\rho_1 \otimes \rho_2}$ is irreducible as a character
3. $\langle \chi_{\rho_1 \otimes \rho_2}, \chi_{\rho_1 \otimes \rho_2} \rangle = 1$
4. $\langle \chi_{\rho_1}, \chi_{\rho_1} \rangle = 1$ and $\langle \chi_{\rho_2}, \chi_{\rho_2} \rangle = 1$
5. ρ_1 and ρ_2 are irreducible as representations.

Proposition 96. If $\{\rho_1, ...\rho_t\}$ and $\{\phi_1, ..., \phi_s\}$ are the irreducible representations for G_1 and G respectively, then $\{\rho_i \otimes \phi_j | 1 \leq i \leq t, 1 \leq j \leq s\}$ is the set of irreducible representations for $G_1 \otimes G_2$.

Lemma 40. Let $\phi : G \to GL_{\mathbb{C}}(V)$ be an irreducible representation. Let $g \in Z(G)$. Then $\rho(g) = \lambda I$ for some root of unity λ. In particular, $|\chi(g)| = \chi(1)$

Proof. Recall that $Z(\mathbb{C}[G]) = \mathbb{C}e_1 \times ... \times \mathbb{C}e_t$ (as an internal direct product). Then, we can write $g = (\alpha_1, ..., \alpha_t)$ to represent $g = \alpha_1 e_1 + ... + \alpha_t e_t$.

Since V is a simple $\mathbb{C}[G]$-module, and $\mathbb{C}[G] = B(I_1) \times ... \times B(I_t)$, then $V \cong I_j$ as $\mathbb{C}[G]$-modules, for some j. Without loss of generality, let $V \cong I_j$.

Then $e_1 = (1, 0, ..., 0)$ acts as the identity on V, so $e_j V = 0$ for all $j \neq 1$. Let $u \in V$. Then $gu = (\alpha_1, ..., \alpha_t)u = (\alpha_1 u, 0, ..., 0)$. Thus $\rho(g_i) = \alpha_1 I_V$. Since $|G|$ is finite, then g has finite order, so α_i must be a $|G|$-th root of unity. ☐

13.2 Day 36 - April 13

Proposition 97. Let R be a Noetherian ring, and let S be a domain containing R. Let $u \in S$ and suppose there exists a nonzero $r \in R$ such that $ru^n \in R$ for all $n \geq 1$. Then u is integral over R.

Proof. Recall that u is integral over R if and only if $R[u]$ is finitely generated as an R-module.

Consider $R \cdot \frac{1}{r}$ as an R-submodule of $Q(R)$. Since $u^n \in R \cdot \frac{1}{r}$ for all n, then $R[u] \subset R \cdot \frac{1}{r}$.

Recall that, since R is Noetherian, then any submodule of a finitely generated R-module is also finitely generated.

But $R \cdot \frac{1}{r}$ is a finitely generated R-module (namely, it is generated by $\frac{1}{r}$), so $R[u]$ is a finitely-generated R-module. Thus u is integral over R.

☐

Theorem 106 (Schur). With the usual notation for a character χ, then $n_i \Big| [G : Z(G)]$ for all i.

Proof. For all integers $m \geq 1$, let $G_m = G \times G \times ... \times G$ (m times). Let χ be an irreducible character, and let $n = \deg \chi = \chi(1)$. Then there exists a representation $\rho : G \to GL_{\mathbb{C}}(V)$ such that $\mathrm{Tr}(\rho) = \chi$. We then wish to show that $n \Big| [G : Z(G)]$.

Let $\rho_m = \rho \otimes \rho ... \otimes \rho : G_m \to GL_{\mathbb{C}}(V \otimes_{\mathbb{C}} ... \otimes_{\mathbb{C}} V)$ (where both tensor products occur m times).

Since ρ is irreducible, then ρ_m is an irreducible representation for G_m. Also, $\deg(\rho_m) = \chi_{\rho_m}(1) = \mathrm{Tr}(\rho_m(1)) = \mathrm{Tr}(\rho(1))^m = n^m$.

Recall from last class that if $g \in Z(G)$, then $\rho(g) = \lambda_g I$ for some root of unity λ. Define $\gamma : Z(G) \to \mathbb{C}^*$ by $g \mapsto \lambda_g$.

Let $H = \ker \gamma = \{g \in Z(G) | \rho(g) = I\} = \ker \rho \cap Z(G)$. Let $D = \{(g_1, ..., g_m) \in Z(G_m) = Z(G) \times ... \times Z(G) | \gamma(g_1, ..., g_m) = 1\}$.

One can check (should check) that $D \lhd G_m$. Moreover, $D \subset \ker \rho_m$ since if $\rho_m(g_1...g_m) = 1$ implis that $\rho_m(g_1, ..., g_m) = \rho(g_1) \otimes ... \otimes \rho(g_m) = \lambda_{g_1} I_V \otimes ... \otimes \lambda_{g_m} I_V = \lambda_{g_1}...\lambda_{g_m} I = \lambda_{g_1...g_m} I = I$.

But recall that normal subgroups induce representations (and irreducible subgroups induce irreducible representations). Thus $D \lhd G_m$ gives an induced irreducible representation on G_m/D, with $\overline{\rho}_m : G_m/D \to GL_{\mathbb{C}}(V \otimes_{\mathbb{C}} ... \otimes_{\mathbb{C}} V)$ such that $\deg \overline{\rho}_m = n^m$. But by the previous theorem, $\deg \overline{\rho}_m \Big| |G_m/D|$, so $n^m \Big| |G_m/D|$.

We now wish to show that $|D| = |Z(G)|^{m-1} \cdot |H|$. In order to do so, let $\alpha = (g_1, ..., g_m) \in Z(G_m) = Z(G) \times ... \times Z(G)$. Then $\alpha \in D$ if and only if $g_1...g_m \in H$, which is the case if and only if $g_m \in (g_1...g_{m-1})^{-1} H$. We therefore have a bijective correspondance between D and $Z(G)^{m-1} \times H$ by $\alpha = (g_1, ..., g_m) \to ((g_1, ..., g_{m-1}), g_1...g_m)$ and $(g_1, ..., g_{m-1}, (g_1...g_m)^{-1}h) \leftarrow ((g_1, ..., g_{m-1}, h)$.

Thus $|D| = |Z(G)|^{m-1} \cdot |H|$.

Therefore, $n^m \Big| \frac{|G|^m}{|Z(G)|^{m-1} \cdot |H|}$. That is, $\frac{|G|^m}{|Z(G)|^{m-1} \cdot |H| n^m} = \frac{|Z(G)|}{|H|} \cdot \left(\frac{|G|}{n|Z(G)|}^m \right) \in \mathbb{Z}$ for all $m \geq 1$. Then, by the previous proposition, $\frac{|G|}{n|Z(G)|}$ is integral over $\mathbb{Z}$. But it is also a rational number, and the only integral rational numbers are integers! Thus $\frac{|G|}{n|Z(G)|} \in \mathbb{Z}$. In other words, $n|Z(G)| \Big| |G|$, so $n \Big| \frac{|G|}{|Z(G)|} = [G : Z(G)]$.

□

Lemma 41. Let G be a finite group and let χ be an irreducible (complex) character of G. Suppose C is a conjugacy class of G such that $\gcd(|C|, n) = 1$, where $n = \deg \chi$. Then for all $g \in C$, $\chi(g) = 0$ or $|\chi(g)| = n$.

Proof. Let $m = |C|$, and let $z = \sum_{g \in C} g$. Recall that $z \in Ae_1 \oplus ... \oplus Ze_t$ (were A is the integral closure of $\mathbb{Z}$ in $\mathbb{C}$).

By one of the formulas about characters, $\frac{m\chi(g)}{n} \in A$ for all $g \in C$. Since $\gcd(m, n) = 1$, then there exists $r, s \in \mathbb{Z}$ such that $1 = rm + sn$. If we multiply this equation by $\frac{\chi(g)}{n}$, then we get that $\frac{\chi(g)}{n} = r \cdot (\frac{m\chi(g)}{n}) + s(\chi(g))$. Since $r, s \in \mathbb{Z} \subset A$, and $\frac{m\chi(g)}{n}, \chi(g) \in A$, then $\frac{\chi(g)}{n} \in A$.

However, $\chi(g) = \lambda_1 + ... + \lambda_n$ for some kth roots of unity $\lambda_1, ..., \lambda_n$.

Let $\alpha = \frac{\chi(g)}{n} = \frac{\lambda_1 + ... + \lambda_n}{n} \in A$. Then $|\alpha| = |\frac{\lambda_1 + ... + \lambda_n}{n}| \leq \frac{|\lambda_1| + ... + |\lambda_n|}{n} \leq 1$. Furthermore, note that we have $|\alpha| = 1$ if and only if $\lambda_i = \lambda_j$ for all i and j, which is equivalent to $|\chi(g)| = n$.

Let ω be a primitive kth root of unity, and let $E = \mathbb{Q}(\omega)$. Then let $H = Gal(E/\mathbb{Q})$, and let $\sigma \in H$. Note $\sigma(\alpha \in A)$ since σ takes integral elements to integral elements.

Furthermore, for all i, $\sigma(\lambda_i = \lambda_i'$ for some k-th root of unity λ_i'. Therefore, $\sigma(\alpha) = \frac{\lambda_1' + ... + \lambda_n'}{n}$.

Let $N = N_{\mathbb{Q}}^E : E \to \mathbb{Q}$. Then, $N(\alpha) = \prod_{\sigma \in H} \sigma(\alpha) \in \mathbb{Q} \cap A = \mathbb{Z}$. Therefore, $N(\alpha) = \prod_{\sigma \in H} |\sigma(\alpha)| \leq 1$. Thus either $N(\alpha) = 0$, so $\alpha = 0$ and $\chi(g) = 0$, or $N(\alpha) = 1$, so $|\sigma(\alpha)| = 1$ for all σ. Namely, this is true $\sigma = \text{id}$, so $|\alpha| = 1$. Thus $|\chi(\alpha)| = n$

□

13.3 Day 37 - April 15

Recall this theorem from last class:

Lemma 42. Let G be a finite group, and let χ be an irreducible $\mathbb{C}$-character of G. Let $n = \deg \chi$. Suppose C is a conjugacy class of G such that $\gcd(|C|, n) = 1$. Then, for all $g \in C$, $\chi(g) = 0$ or $|\chi(g)| = n$.

Proposition 98. Let G be a finite simple group. Then there does not exist a conjugacy class C such that $|C| = p^a$ for some prime p and integer $a > 0$.

Proof. Let $\chi_1, ..., \chi_t$ be the irreducible (complex) characters of G, and let $\rho_1, ..., \rho_t$ be their associated representations. Let n_i denote the degree of χ_i. That is, $n_i = \chi_i(1)$. Without loss of generality, assume that ρ_1 is the trivial representation.

Suppose for the sake of contradiction that $|C| = p^a$ for some prime p and integer $a > 0$.

First, we will show that if $p \nmid n_i$ for some $i > 1$, then $\chi_i(g) = 0$ for all $g \in C$.

Let $G_i = \{g \in G | \rho_i(g) = \lambda I \text{ for some } \lambda \in \mathbb{C}\}$. Note that $G_i \lhd G$. But by assumption, G is normal, so either $G_i = \{1\}$ or $G_i = G$. Suppose for the sake of contradiction that $G_i = G$. Since $i > 1$, then ρ_i is not the constant (trivial) homomorphism. Also, since G is simple, then $\ker \rho_i = \{1\}$. Then $G \cong \rho_i(G) = \rho_i(G_i) = \{\lambda I | g \in G\}$. Thus G is abelian, so this contradicts the fact that $|C| > 1$. Therefore $G_i = \{1\}$.

That is, for all $g \neq 1$, $|\chi_i(g)| < n_i$. As $p \nmid n_i$, then $\gcd(|C|, n_i) = 1$. Then, by the lemma, $\chi_i(g) = 0$ or $|\chi_i(g)| = n_i$ for all $g \in C$. Since $|\chi_i(g)| < n_i$ for all $g \neq 1$, and $1 \notin C$, then $\chi_i(g) = 0$ for all $g \in C$, as desired.

Recall one of the formulae about characters was that, for all $g \neq 1$, $\sum_{i=1}^{t} \chi_i(1)\chi_i(g) = 0$. In particular, this is true for some $g \in C$. But $\chi_i(1) = n_i$, so $\sum_{i=1}^{t} n_i\chi_i(g) = 0$. Recall that $n_1 = 1$ and $\chi_1(g) = 1$, so $1 + \sum_{i=2}^{t} n_i\chi_i(g) = 0$. By the previous part of the proof, $p \nmid n_i$ for all $i > 1$, so $\chi_i(g) = 0$ for this $g \in C$. Thus $1 = 0$, a contradiction! Thus there is no conjugacy class of size p^a. [this is flawed]

□

Let's now do one application of character theory. It is Burnside's Theorem.

Theorem 107. Let G be a group of order $p^a q^b$, with p and q primes. Then G is solvable.

Proof. Several cases of this are easy. First, if G is abelian, then it is solvable. Also, if $a = 0$ or $b = 0$, then G is, respectively, a p-group or a q-group, and we have already proven such groups are solvable. If $a = b = 1$, then either it has a unique Sylow p-group or a unique Sylow q-group, which must be normal.

We will now proceed by induction on $a + b$. If $a + b = 2$, then $a = b = 1$ which case we have already discussed.

Suppose $a + b > 2$. It then suffices to show that G has a nontrivial normal subgroup. Suppose for the sake of contradiction that G is simple. Let P be a Sylow p-subgroup. Then, by classical results, $Z(p) \neq \{1\}$, so let $x \in Z(P) \setminus \{1\}$.

Let $C_G(x) = \{y \in G | yx = xy\}$ (the centralizer of x in G), and note that $P \subset C_G(x)$. Let C denote the conjugacy class of x. Then $|C| = [G : C_G(x)] = q^l$ for some $l \leq b$. But by the previous proposition, $l = 0$. Therefore, $|C| = 1$, so $C = \{x\}$. In other words, $x \in Z(G)$. Thus $Z(G) \neq 1$, so $Z(G)$ is a nontrivial subgroup. However, it is a proper subgroup as well, since we already dealt with the case that G is abelian. Thus $Z(G)$ is a proper nontrivial normal subgroup, so by the inductive hypothesis, G is solvable. □

And now, a word on Frobenius reciprocity:

Remark 133. Let G be a group, and let $H \leq G$. Let $\chi \in char(H)$. Then, χ^G induced up to G, so for all $\phi \in char(G)$, $\phi_H \in char(H)$, and $\langle \chi^G, \phi \rangle = \langle \chi, \phi_H \rangle$.

This is hard to do normally, but with commutative algebra, this ends up being just $Hom - \otimes$ adjunction!

14 Primary Decompositions

Let's now talk about primary decompositions.

Definition 120. Let R be a commutative ring. Let $N \subsetneq M$ be R-modules. For any $a \in R$ and any module L, let $a_L : L \to L$ be the R-module homomorphism given by $l \mapsto al$.

We say that N is a *primary submodule of* M if, for all $a \in R$, $a_{M/N} : M/N \to M/N$ is either injective or nilpotent (i.e. $a^n_{M/N} = 0$ for some n).

Remark 134. If $L \subset N \subsetneq M$, then N is primary in M if and only if N/L is primary in M/L. This follows directly from the fact that $(M/L)/(N/L) \cong M/N$. In particular, N is primary in M if and only if (0) is primary in M/N.

Proposition 99. Let $I \subsetneq R$ be an ideal. Then I is primary (as an R-module) if and only if, whenever $ab \in I$, either $a \in I$ or $b \in \sqrt{I}$.

Proof. Suppose I is a primary ideal of R, and suppose $ab \in I$. Then, for all $a \in R$, $a_{R/I}$ is either injective or nilpotent.

Either $a \in I$ or $a \notin I$. In the former case, we have nothing to show. In the latter case, then $\overline{a} \neq \overline{0}$ in R/I, but $b_{R/I}(\overline{a}) = \overline{ba} = \overline{0}$, so $b_{R/I}$ is not injective. Therefore $b_{R/I}$ is nilpotent, so there exists an $n \in \mathbb{N}$ such that $0 = b^n(\overline{1}) = \overline{b}^n$. Thus $b^n \in I$, or in other words $b \in \sqrt{I}$. Thus either $a \in I$ or $b \in \sqrt{I}$.

Conversely, suppose whenever $ab \in I$, then either $a \in I$ or $b \in \sqrt{I}$. Let $a \in R$ and suppose $a_{R/I}$ is not injective. Then there exists a $b \notin I$ such that $a_{R/I}(\overline{b}) = \overline{0} = \overline{ab}$. Thus $ba = ab \in I$. Since $b \notin I$, then $a \in \sqrt{I}$. That is, $a^n \in I$ for some $n \in \mathbb{N}$. Thus $a^n_{R/I} = 0$, so $a_{R/I}$ is nilpotent.

□

14.1 Day 38 - April 18

Let's talk more about primary decompositions.

Proposition 100. Suppose N is a primary submodule of M. Then $\sqrt{\mathrm{Ann}_R(M/N)}$ is prime.

Before the proof, let's define a term.

Definition 121. If $\mathfrak{p} = \sqrt{\mathrm{Ann}_R(M/N)}$, then we say N is $\mathfrak{p}$-*primary*, or $\mathfrak{p}$ is the prime *prime associated to* M/N.

Proof. Since $N \neq M$, then $1 \notin \sqrt{\mathrm{Ann}_R(M/N)}$, so this ideal is not all of R.

Suppose $ab \in \sqrt{\mathrm{Ann}_R(M/N)}$, and suppose $a \notin \sqrt{\mathrm{Ann}_R(M/N)}$. Recall that $\sqrt{\mathrm{Ann}_R(M/N)} = \{r \in R | r_{M/N} \text{ is nilpotent}\}$.

Since N is primary, and $a \notin \sqrt{\mathrm{Ann}_R(M/N)}$, then $a_{M/N}$ is injective. Since $ab \in \sqrt{\mathrm{Ann}_R(M/N)}$, then there exists an $n \in \mathbb{N}$ such that $(ab)^n_{M/N} = a^n_{M/N} b^n_{M/N} = 0$ for some n. Since $a_{M/N}$ is injective, then so is $a^n_{M/N}$, so $b^n_{M/N} = 0$. Thus $b \in \sqrt{\mathrm{Ann}_R(M/N)}$.

That is, whenever $ab \in \sqrt{\mathrm{Ann}_R(M/N)}$ and $a \notin \sqrt{\mathrm{Ann}_R(M/N)}$, then $b \in \sqrt{\mathrm{Ann}_R(M/N)}$. Thus this ideal is prime. □

Let's look at a non-example of a primary ideal.

Example 121. Let k be a field, and let $R = k[x, y]$. Let $I = (x^2, xy)$. Then $\sqrt{I} = (X)$. However, $xy \in I$, by $x \notin I$ and $y \notin \sqrt{I} = (X)$. Thus I is not primary.

Proposition 101. Suppose $\sqrt{\mathrm{Ann}_R(M/N)} = \mathfrak{m}$ is a maximal ideal. Then N is a primary submodule of M.

Proof. Let $a \in R$, and suppose $a_{M/N}$ is not nilpotent. It then suffices to show that $a_{M/N}$ is injective.

Since $a \notin \sqrt{\mathrm{Ann}_R(M/N)} = \mathfrak{m}$, then $\mathrm{Ann}_R(M/N) + Ra = R$. Thus $1 = r + sa$ for some $r \in \mathrm{Ann}_R(M/N)$ and $s \in R$.

Now suppose $a_{M/N}(\overline{x}) = \overline{0}$ for some $\overline{x} \in M/N$. Then $ax \in N$. But $x = rx + sax$, and both $rx \in N$ since $r \in \mathrm{Ann}_R(M/N)$, and $sax \in N$ since $ax \in N$. Thus $x \in N$, so $\overline{x} = 0$. That is, $a_{M/N}$ is injectivve. Thus N is primary. □

Remark 135. Let R be a ring, and let $I \subset R$ be an ideal. Then $\mathrm{Ann}_R(R/I) = I$, and $\sqrt{\mathrm{Ann}_R(R/I)} = \sqrt{I}$. If I is a primary ideal, then $\sqrt{I}$ is prime. If $\sqrt{I}$ is maximal, then I is a primary ideal.

Proposition 102. Let R be a PID. Let I be an ideal of R. Then the following are equivalent:

1. I is primary in R.

2. $I = (0)$ or $I = (f^n)$ for some irreducible element f and $n \geq 1$.

3. $I = (0)$ or $I = \mathfrak{m}^n$ for some maximal ideal $\mathfrak{m}$ and $n \geq 1$.

Proof. Let's first show that (2) implies (1). Certainly, (0) is prime in R (since it is a principal ideal domain), so it is primary. On the other hand, if $I = (f^n)$ for some irreducible element f, then $\sqrt{I} = \sqrt{(f^n)} \supset (f)$. But since f is irreducible, then (f) is maximal, so either $\sqrt{I} = (f)$ or $\sqrt{I} = R$. The latter is not the case because $1 \notin \sqrt{I}$, so $\sqrt{I} = (f)$. Then, by the previous proposition and remark, since $\sqrt{I}$ is maximal, then I is primary.

Thus (2) implies (1).

Now let us show that (1) implies (2). Let I be primary, and suppose $I \neq (0)$. Therefore, by the previous remark, $\sqrt{I}$ is prime. Recall that the prime ideals in a PID are either 0 or generated by irreducible elements. Since $I \neq 0$, then $\sqrt{I} \neq 0$, so $\sqrt{I} = (f)$ for some irreducible $f \in R$. Let n be the least number such that $f^n \in I$.

We now wish to show that $I = (f^n)$. Suppose $g \in I$. Write $g = f^l h$ where $\gcd(f, h) = 1$. Then $f^l h = g \in I$, so since I is primary, eiether $f^l \in I$ or $h \in \sqrt{I} = (f)$.

But $gcd(f, h) = 1$, so $h \notin (f)$. Thus $f^l \in I$. We chose n to be the least element so that $f^n \in I$, so so $l \geq n$. Thus $g = f^l h \in (f^n)$. Therefore $I = (f^n)$.

Thus (1) implies (2).

The proof of the equivalence of (2) and (3) is left to the reader. □

Corollary 51. If $R = \mathbb{Z}$, then I is primary if and only if $I = (0)$ or $I = (p^n)$ for some prime p and $n \geq 1$.

Remark 136. People were very interested in generalizing unique prime factorization from $\mathbb{Z}$ to other rings. In $\mathbb{Z}$, the statement for ideals goes as follows.

Let $R = \mathbb{Z}$, and let $I \subsetneq R$ be a nonzero ideal. Then $I = (n)$ for some $n \neq -1, 0, 1$.

Then, we can write $n = p_1^{m_1} ... p_k^{m_k}$, where each p_i is prime and $m_i \geq 1$. Then $I = (p_1^{m_1} ... p_k^{m_k}) = (p_1^{m_1}) \cap ... \cap (p_k^{m_k}) = (p_1)^{m_1} \cap ... \cap (p_k)^{m_k}$.

However, in order to prove this, you need the fact that $\mathbb{Z}$ is height 1, so the chinese remainder theorem applies nicely. Thus this exact statement of unique prime factorization doesn't generalize totally.

Example 122. Let k be a field and let $R = k[x, y]$. Let $I = (x^2, y)$. Then $\sqrt{I} = (x, y)$. Since $\sqrt{I}$ is maximal, then I is primary. Note that I is not a power of a prime ideal, since it could only be a power of (x, y), and it is not.

Also, powers of prime ideals need not be primary!

Example 123. Let k be a field, and let $f = x^2 - yz \in k[x, y, z]$. Let $R = k[x, y, z]/(f)$, and let Let $\mathfrak{p} = (\overline{x}, \overline{z})R = (x, y)/(f)$. Then $\mathfrak{p}$ is prime, and $p^2 = (\overline{x}^2, \overline{xz}, \overline{z}^2) = (x^2, xz, z^2, yz)/(f)$. Thus $\overline{zy} \in \mathfrak{p}^2$, but $\overline{z} \notin \mathfrak{p}^2$ and $\overline{y} \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p} = (\overline{x}, \overline{z})$. Thus $\mathfrak{p}^2$ is not prime!

Definition 122. Let M be an R-module, and let $N \subsetneq M$ be a submodule. Then N is called *irreducible in* M if, whenever $N = L_1 \cap L_2$ for some submodules $L_1, L_2 \subset M$, then $N = L_1$ or $N = L_2$.

Remark 137. If $A \subset N \subsetneq M$, then N is irreducible in M if and only if N/A is irreducible in M/A, which is the case if and only if $(\overline{0})$ is irreducible in M/N.

14.2 Day 39 - April 20

Recall the definition of primary. We will prove some equivalent conditions about it.

Remark 138. Let M be an R-module, and let $Q \subsetneq M$ be a submodule. Then the following are equivalent:

1. Q is primary. (That is, for all $a \in R$, $a_{M/Q} : M/Q \to M/Q$ is either injective as a function, or nilpotent as a function.)

2. For all $a \in R$ $(Q :_M a) = Q$ (meaning a is a non-zero-divisor on M/Q) or $a^n M \subset Q$ for some n.

If $M = R$ is $Q = I$, an ideal, then we get a further equivalence that

3. For all $a \in R$, $a \in \sqrt{I}$ (and $\sqrt{I}$ is a prime ideal), or $(I :_R: a) = I$.

We get a simpler statement if we assume $Q = (0)$.

Remark 139. For any module M, (0) is primary in M if and only if for all $a \in R$, either $a^n M = 0$ for some n, or $(0 :_M a) = 0$ (that is, a is a non-zero-divisor on M).

Now let us return to the topic from last class, irreducible submodules of a Noetherian module.

Theorem 108. Let M be a Noetherian R-module, and let Q be an irreducible submodule of M. Then Q is primary.

Proof. By the remark from last class, Q is primary in M if and only if (0) is primary in M/Q. Since M is Noetherian, then M/Q is Noetherian as well. Also, since Q is irreducible in M, then (0) is irreducible in M/Q.

Therefore, we will assume without loss of generality that $Q = (0)$. By the previous remark, it suffices to show that if $a \in R$ and $a^n M \neq 0$ for all n, then a is a non-zero-divisor on M.

Suppose for the sake of contradiction that $0 \neq (0 :_M a)$. Then consider the ascending chain $0 \subsetneq (0 :_M a) \subset (0 :_M a^2) \subset (0 :_M a^3) \subset ....$

Since M is Noetherian, then this chain eventually stabilizes. That is, $(0 :_M a^n) = (0 :_M a^{n+j}$ for some n and all j. Suppose for the sake of contradiction that there exists some $u \in R \setminus (0 :_M a^n)$ [other choice of u?].

We then wish to show that $Ru \cap a^n M = (0)$.

Let $x = ru = a^n y$ for some $r \in R, y \in M$. Then $ax = rau = a^{n+1} y$. But $rau = 0$ since [???]. Thus $a^{n+1} y = 0$. Thus $y \in (0 :_M a^{n+1}) = (0 :_M a^n)$, so $a^n y = 0$, so $x = 0$. Thus $Ru \cap a^n M = (0)$.

Since (0) is an irreducible submodule, then $Ru = 0$ or $a^n M = 0$. Since $Ru \neq 0$, then $a^n M = 0$. □

Definition 123. Let N be a proper submodule of M. A *primary decomposition* for N (in M) is an equation $N = Q_1 \cap ... \cap Q_s$, where each Q_i are primary submodules of M.

Theorem 109. Let $M \neq 0$ be a Noetherian module. Then every proper submodule of M has a primary decomposition.

Proof. Let $\Lambda = \{N \subsetneq M | N \text{ does not have a primary decomposition}\}$. Then then suffices to show that $\Lambda = \emptyset$.

Suppose for the sake of contradiction that $\Lambda \neq \emptyset$. Then since M is Noetherian, we can choose $N \in \Lambda$ which is maximal. By the contrapositive of the previous theorem, N must be reducible.

That is, there must exist $L_1, L_2 \supsetneq N$ such that $N = L_1 \cap L_2$. But if $L_1 = M$, then $N = L_1 \cap L_2 = L_1$. Since this is not the case, then $L_1 \subsetneq M$. Similarly, $L_2 \subsetneq M$.

Therefore, $L_1, L_2 \in \Lambda$, so they each have a primary decomposition. Then, by intersecting their two primary decompositions, we get a primary decomposition for N. This contradicts the fact that $N \in \Lambda$, so $\Lambda = \emptyset$, as desired. □

Lemma 43. Let $Q_1, ...Q_n$ be $\mathfrak{p}$-primary submodules of M. Then $Q_1 \cap ... \cap Q_n$ is $\mathfrak{p}$-primary as well.

Proof. We must show that $Q_1 \cap ... \cap Q_n$ is primary, and that its associated prime is $\mathfrak{p}$.

For each Q_i, since Q_i is $\mathfrak{p}$-primary, then $\sqrt{\mathrm{Ann}_R(M/Q_i)} = \mathfrak{p}$. But note that $\mathrm{Ann}_R(M/(Q_1 \cap ... \cap Q_n)) = \mathrm{Ann}_R(M/Q_1) \cap ... \cap \mathrm{Ann}_R(M/Q_n)$.

Therefore, $\sqrt{\mathrm{Ann}_R(M/(Q_1 \cap ... \cap Q_n))} = \sqrt{\mathrm{Ann}_R(M/Q_1)} \cap ... \cap \sqrt{\mathrm{Ann}_R(M/Q_n)} = \mathfrak{p} \cap ... \cap \mathfrak{p} = \mathfrak{p}$. Thus, if $Q_1 \cap ... \cap Q_n$ is primary, it will have the right associated prime.

We must now show that $Q_1 \cap ... \cap Q_n$ is primary. Let $a \in R$. As we have just shown, if $a \in \mathfrak{p}$, then $a \in \sqrt{\mathrm{Ann}_R(M/(Q_1 \cap ... \cap Q_n))}$, so $a^n M \subset Q_1 \cap ... \cap Q_n$. On the other hand, if $a \notin \mathfrak{p}$, then $(Q_1 \cap ... \cap Q_n :_M a) = (Q_1 : a) \cap ... \cap (Q_n :_M a) = Q_1 \cap ... \cap Q_n$ (as each Q_i is $\mathfrak{p}$-primary).

Thus, by the remark above, $Q_1 \cap ... \cap Q_n$ is primary, and since it has the right associated prime, then $Q_1 \cap ... \cap Q_n$ is $\mathfrak{p}$-primary. □

Definition 124. Let $N \subsetneq M$. We say an *irredundant primary decomposition* for N is an equation where $N = Q_1 \cap ... \cap Q_s$ where

1. Each Q_i is $\mathfrak{p}_i$-primary.

2. $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$.

3. $N \subsetneq Q_1 \cap ... \cap \hat{Q}_i \cap ... \cap Q_n$ for all i.

Proposition 103. If N has a primary decomposition, it has an irredundant primary decomposition.

Proof. If some Q_i, Q_j violates the second criterion, then they can be combined by the Lemma.

If some Q_i violates the third criterion, then it can be dropped completely.

This eventually terminates, so we are done. $\square$

Example 124. Let k be a field, and let $R = k[x, y]$. Let $I = (x^2, xy)$. Note that $I = (x) \cap (x^2, y)$ is an irredundant primary decomposition. However, note that $I = (x) \cap (x^2, xy, y^2)$ is another irreducible primary decomposition.

That is, there are two irreducible primary decompostions for I! However, both i.p.d.s have the same collection of associated primes, namely $\{(x), (x, y)\}$. Note also that the number of primary components is the same in both decompositions, and (x) appears in both. We will formalize the reasons for this later.

Now let's talk about how localization plays with a primary decomposition.

Proposition 104. Let Q be a $\mathfrak{p}$-primary submodule of M, and let S be a multiplicatively closed set of R. Then

1. $Q_S = M_S$ if and only if $\mathfrak{p} \cap S \neq \emptyset$.

2. If $\mathfrak{p} \cap S = \emptyset$, then Q_S is $\mathfrak{p}_S$-primary.

Proof. Recall that localization commutes with quotienting. Therefore, it suffices to show the statement holds for (0) in M/Q. That is, we may assume without loss of generality that $Q = 0$.

Thus, (0) is primary in M and $\mathfrak{p} = \sqrt{\operatorname{Ann}_R(M)}$.

(Proof of 1). If $\mathfrak{p} \cap S \neq \emptyset$, let $t \in \mathfrak{p} \cap S$. Then $t^n M = 0$ for some n. Since $t \in S$, then $t^n = S$. Thus $M_S = 0 = Q_S$, as desired.

Conversely, suppose $Q_S = M_S$, and let $u \in M \setminus Q$. Then $\frac{u}{1} = \frac{q}{s}$ for some $q \in Q$ and $s \in S$. Then, there exists a $t \in S$ such that $tsu = tq$. Since $tq \in Q$, then $u \in (Q :_M ts) \setminus Q$. Therefore, $ts \in \mathfrak{p} \cap S$, so $\mathfrak{p} \cap S \neq \emptyset$. This completes the proof of (1).

We will prove (2) tomorrow. $\square$

14.3 Day 40 - April 22

Let's finish the proof of a proposition from last class.

Proposition 105. Let Q be a $\mathfrak{p}$-primary submodule of M, and let S be a multiplicatively closed set of R. Then

1. $Q_S = M_S$ if and only if $\mathfrak{p} \cap S \neq \emptyset$.

2. If $\mathfrak{p} \cap S = \emptyset$, then Q_S is $\mathfrak{p}_S$-primary.

Proof. Recall that localization commutes with quotienting. Therefore, it suffices to show the statement holds for (0) in M/Q. That is, we may assume without loss of generality that $Q = 0$.

Thus, (0) is primary in M and $\mathfrak{p} = \sqrt{\operatorname{Ann}_R(M)}$.

(Proof of 2). We wish to show that Q_S is $\mathfrak{p}_S$-primary. But $Q = 0$, so $Q_S = 0$. Let $\frac{r}{s} \in R_S$. Either $\frac{r}{s}$ is a non-zero-divisor on M_S or it is not.

If $\frac{r}{s}$ is a non-zero divisor on M_S, then multiplication by $\frac{r}{s}$ is injective on M_S.

On the other hand, if $\frac{r}{s} \cdot ut = 0$ for some $\frac{u}{t} \in M_S \setminus 0$, then $\frac{ru}{st} = 0$. That is, there exists an $s' \in S$ such that $s'ru = 0$. Since $\frac{u}{t} \neq 0$, then $u \neq 0$, so $s'r$ is a zero-divisor on M. Since M is $\mathfrak{p}$-primary, then all zero divisors are nilpotent. That is, there exists an n such that $(s'r)^n M = 0$. Then $(\frac{s'r}{1})^n M_S = 0$, so $(\frac{r}{s})^n M_S = 0$. That is, multiplication by $\frac{r}{s}$ is nilpotent on M_S.

Thus, multiplication by $\frac{r}{s}$ is either injective or nilpotent on M_S, so (0) is primary in M_S.

It then suffices to show that the prime associated to $Q_S = 0$ is $\mathfrak{p}$.

But note that $s'r \in \mathfrak{p}$ [why]? Thus, $\frac{r}{s} \in \mathfrak{p}_S$. Therefore, $\sqrt{\operatorname{Ann}_{R_S}(M_S)} \subset \mathfrak{p}_S$. Thus M_S is $\mathfrak{p}_S$-primary. □

Remark 140. Localization distributes across intersections of ideals. That is, $(Q_1 \cap ... \cap Q_t)_S = (Q_1)_S \cap ... \cap (Q_t)_S$ for any submodules $Q_S, ..., Q_t$ of M. (This is a good exercise to do.)

Suppose $N = Q_1 \cap ... \cap Q_t$ is a primary decomposition for N in M, where each Q_i is $\mathfrak{p}_i$-primary. Then $N_S = M)S$ if and only if $S \cap \mathfrak{p}_i \neq 0$ for all i, which is true if and only if $(Q_i)_S = (M_i)_S$ for all i.

Proposition 106. Let $N = Q_1 \cap ... Q_t$ be an irredundant primary decomposition for $N \subset M$. Let S be a multiplicatively closed set of R such that $N_S \neq M_S$. From the previous remark, this implies that $S \cap \mathfrak{p}_i = \emptyset$ for at least one i. Reorder the Q_i such that $S \cap \mathfrak{p}_i = \emptyset$ for $i = 1, ..., r$ and $S \cap \mathfrak{p}_i \neq 0$ for $i = r+1, ..., t$. Then $N_S = (Q_1)_S \cap ... \cap (Q_r)_S$ is an irredundant primary decomposition.

Proof. By the previous remark, since localization distributes over intersections, then

$$\begin{aligned} N_S &= (Q_1 \cap ... \cap Q_t)_S \\ &= (Q_1)_S \cap ... \cap (Q_r)_S \cap (Q_{r+1})_S \cap ... \cap (Q_t)_S \\ &= (Q_1)_S \cap ... \cap (Q_r)_S \cap M_S \cap ... \cap M_S \\ &= (Q_1)_S \cap ... \cap (Q_r)_S \end{aligned}$$

Note that the third equality is by part 1 of the previous decomposition.

Thus, $N_S = (Q_1)_S \cap ... \cap (Q_r)_S$ is a primary decomposition. We must now show that it is irredundant.

Because $N = Q_1 \cap ... \cap Q_t$ was an irredundant primary decomposition, then they have distinct associated primes $\mathfrak{p}_1, ... \mathfrak{p}_t$.. By the previous proposition, the associated prime of $(Q_i)_S$ is $(\mathfrak{p}_i)_S$ for $i = 1, ..., r$. Since the $\mathfrak{p}_i$ are distinct, then the $(\mathfrak{p}_i)_S$ are distinct.

It then suffices to show that we cannot do without any of the $(Q_i)_S$, for $i = 1, ..., r$.

Suppose for the sake of contradiction that $(Q_i)_S \supset (Q_1)_S \cap ... \cap (\hat{Q}_i)_S \cap ... \cap (Q_r)_S \cap (Q_{r+1})_S \cap ... \cap (Q_t)_S = (Q_1 \cap ... \cap \hat{Q}_i \cap Q_t)_S$. We know that $Q_i \not\supset Q_1 \cap ... \cap \hat{Q}_i \cap .. \cap Q_t$, since they formed an irredundant primary decomposition for N. Then, there must be a $u \in Q_1 \cap ... \cap \hat{Q}_i \cap .. \cap Q_t \setminus Q_i$, so $\frac{u}{1} \in$ [*something*].

Hence, w is a zero divisor on M/Q_i, so $w \in \mathfrak{p}_i \cap S$. This is a contradiction, so the primary decomposition is irredundant. □

Remark 141. In the proposition above, the set of associated primes of $N_S = Q_1 \cap ... \cap Q_t$ is

$$\{\mathfrak{p}_S | \mathfrak{p} \text{ is an associated prime of } N_S = (Q_1)_S \cap ... \cap (Q_t)_S \text{ and } \mathfrak{p} \cap S = \emptyset\}$$

Theorem 110 (First Uniqueness Theorem). Let R be a Noetherian ring, and let M be a finitely generated R-module. Let N be a proper submodule, and let $N = Q_1 \cap ... \cap Q_t$ be an irredundant primary decomposition. Let $\mathfrak{p}_i$ be the prime associated with Q_i. Then $\{\mathfrak{p}_1, ... \mathfrak{p}_t\} = \{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\}$.

Therefore, the set of primes only depends on N, and not on the irredundant primary decomposition. In partiuclar, every irreducible primary decomposition for N has the same number of primary components.

Proof. We can reduce to the case that $N = 0$.

Let $0 = Q_1 \cap ... \cap Q_t$ be an irredundant primary decompostion, where each Q_i is $\mathfrak{p}_i$-primary for $i = 1, ..., t$.

We will first show that $\mathfrak{p} \in \{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\}$ implies $\mathfrak{p} \in \{\mathfrak{p}_1, ...\mathfrak{p}_t\}$.

Choose some $x \in M$, and suppose $\mathfrak{p} = (0 :_R x)$ is prime. Then, $\mathfrak{p}R_\mathfrak{p} = (0 :_{R_\mathfrak{p}} \frac{x}{1})$. Since $\mathfrak{p}R_\mathfrak{p} \neq R_\mathfrak{p}$, then $\frac{x}{1} \neq 0$, so $M_\mathfrak{p} \neq 0$.

Then (rearranging the order of the irreducible primary decomposition), $0 = (Q_1)_\mathfrak{p} \cap ... \cap (Q_r)_\mathfrak{p}$ is an irreducible primary decomposition for (0) in $M_\mathfrak{p}$, and $(Q_i)_\mathfrak{p}$ is $\mathfrak{p}_i R_\mathfrak{p}$-primary.

Since $\mathfrak{p} \neq R$, then $x \neq 0$. Thus $x \notin Q_i$ for some i. But $\mathfrak{p}x = 0$ since $\mathfrak{p} = (0 :_R x)$. Thus $\mathfrak{p}$ consists of zero divisors on M/Q_i. Since Q_i is primary, then zero divisors on M/Q_i are nilpotent. Thus $\mathfrak{p} \subset \mathfrak{p}_i$. Therefore, $\mathfrak{p}R_\mathfrak{p} \subset \mathfrak{p}_i R_\mathfrak{p}$. But $\mathfrak{p}R_\mathfrak{p}$ is a maximal ideal and $\mathfrak{p}_i R_\mathfrak{p} \neq 0$, so $\mathfrak{p}R_\mathfrak{p} = \mathfrak{p}_i R_\mathfrak{p}$. Thus $\mathfrak{p} = \mathfrak{p}_i$.

That is, $\mathfrak{p} \in \{\mathfrak{p}_1, ..., \mathfrak{p}_t\}$. Thus $\{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\} \subset \{\mathfrak{p}_1, ...\mathfrak{p}_t\}$.

Conversely, we wish to show each $\mathfrak{p}_i \in \{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\}$. We will show that $\mathfrak{p}_1 \in \{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\}$, and an identical argument will apply to the other $\mathfrak{p}_i$.

We have two cases. The first case is that $(R, \mathfrak{m})$ is local, and $\mathfrak{p}_1 = \mathfrak{m}$. Let $\Lambda = \{(0 :_R x) | \sqrt{(0 :_R x)} = \mathfrak{m}\}$. We will first show that $\Lambda \neq \emptyset$.

Since our decomposition with irredundant, then $Q_2 \cap ... \cap Q_t \not\subset Q_1$. Thus there exists a $u \in Q_2 \cap ... \cap Q_t \setminus Q_1$.

Also, since $\mathfrak{m} = \mathfrak{p}_1$ is the prime associated to Q_1, then $\mathfrak{m} = \mathfrak{p}_1 = \sqrt{\operatorname{Ann}_R(M/Q_1)}$. Since R is Noetherian, then $\mathfrak{m}$ is finitely generated, so $\mathfrak{m}^n \subset \operatorname{Ann}_R M/Q_1$ for some n. Hence, $\mathfrak{m}^n u \subset Q_1$.

But since $\mathfrak{m}^n u \subset Q_2 \cap ... \cap Q_t$ as well, then $\mathfrak{m}^n u \subset Q_1 \cap ... \cap Q_r = 0$. Thus $\mathfrak{m}^n u = 0$, so $\mathfrak{m} \subset \sqrt{(0 :_R u)}$. Since $u \neq 0$, then $\sqrt{(0 :_R u)} \neq R$, so $\mathfrak{m} = \sqrt{(0 :_R u)}$. That is, $(0 :_R u) \in \Lambda$, so $\Lambda \neq 0$, as desired.

Since R is Noetherian, then there exists a maximal element of Λ. Let $(0 :_R x)$ be such an element. We wish to show that $(0 :_R x)$ is prime, and that $(0 :_R x) = \mathfrak{m}$.

Suppose $ab \in (0 :_R x)$ but that $b \notin (0 :_R x)$. Then $abx = 0$, but $bx \neq 0$. Also, $(0 :_R x) \subset (0 :_R bx)$. Thus $\mathfrak{m} = \sqrt{(0 :_R x)} \subset \sqrt{(0 :_R bx)}$. Since $bx \neq 0$, then $(0 :_R bx) \subsetneq R$, so $\sqrt{(0 :_R bx)} \subsetneq R$. But since $\mathfrak{m}$ is maximal, and $\mathfrak{m} \subset \sqrt{(0 :_R bx)} \subsetneq R$, then $\mathfrak{m} = \sqrt{(0 :_R bx)}$. Thus $(0 :_R bx) \in \Lambda$. Since $(0 :_R x)$ was maximal in Λ, and $(0 :_R x) \subset (0 :_R bx) \in \Lambda$, then $(0 :_R x) = (0 :_R bx)$. But $abx = 0$, so $a \in (0 :_R bx)$, so $a \in (0 :_R x)$. Thus $(0 :_R x)$ is prime.

Since $(0 :_R x)$ is prime, then it is radical. That is , $(0 :_R x) = \sqrt{(0 :_R x)} = \mathfrak{m}$. Thus $\mathfrak{p}_1 = \mathfrak{m} \in \{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\}$. This concludes the specific case.

In the other case, R is not necessarily semi-local. However, by localizing, we get that $\mathfrak{p}_1 R_{\mathfrak{p}_1}$ is an associated prime of the localized irredundant prime decompositon. Then, by the previous case, $\mathfrak{p}_1 R_{\mathfrak{p}_1} = (0 :_{R_{\mathfrak{p}_1}} \frac{x}{t})$, for some $\frac{x}{t} \in M_{\mathfrak{p}_1}$.

Since R is Noetherian, then $\mathfrak{p}_1$ is finitely generated. That is, $\mathfrak{p}_1 = (a_1, ..., a_n)$. Then for each i, $\frac{a_i}{1} \cdot \frac{x}{t} = \frac{0}{1}$, so there exists an $s_i \notin \mathfrak{p}_1$ such that $s_i a_i x = 0$ for $i = 1, ..., n$. Let $s = s_1 ... s_n$, and note that $s \notin \mathfrak{p}_1$. Then $a_i(sx) = 0$ for all $i = 1, ..., n$, so $\mathfrak{p}_1 \subset (0 :_R sx)$. Then $\mathfrak{p}_1 = (0 :_R sx)$ as $s \notin \mathfrak{p}_1$.

Thus $\mathfrak{p}_1 \in \{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\}$, so $\{\mathfrak{p}_1, ...\mathfrak{p}_t\} = \{\mathfrak{p} \in \operatorname{Spec} R | p = (N :_R x) \text{ for some } x \in M\}$, as desired. □

15 Associated Primes

15.1 Day 41 - April 25

We showed last class that, in nice cases, any primary decomposition of a specified submodule has the same set of associated prime ideals. This gives rise to the following definition.

Definition 125. Let R be a Noetherian ring, and $N \subsetneq M$ be finitely generated R-modules. Let $N = Q_1 \cap ... \cap Q_t$ be an irredunant primary decomposition. For each i, let $\mathfrak{p}_i = \sqrt{\operatorname{Ann}_R(M/Q_i)}$. Then $\{\mathfrak{p}_1, ..., \mathfrak{p}_t\}$ is the set of *associated primes* of N in M, or of M/N. We denote this set by $\operatorname{Ass}_R(M/N)$.

Remark 142. We proved lass class that $\operatorname{Ass}_R(M/N)$ is well-defined in this context, and that $Ass_R(M/N) = \{(N :_R x) \in \operatorname{Spec} R | x \in M\}$.

Remark 143. Assume again that Let R be a Noetherian ring, and $N \subsetneq M$ be finitely generated R-modules.

We have the following results:

1. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then the following are equivalent:
   (a) $\mathfrak{p} \in \operatorname{Ass}_R(M) = \operatorname{Ass}_R(M/0)$.
   (b) $\mathfrak{p} = (0 :_R x)$ for some $x \in M$.
   (c) There exists an injective R-module homomorphism $R/\mathfrak{p} \to M$ (given by $\overline{1} \mapsto x$).
   (d) $Hom_{R_\mathfrak{p}}(k(\mathfrak{p}), M_\mathfrak{p}) \neq 0$.
2. $M = 0$ if and only if $Ass_R M = \emptyset$.
3. If S is a multiplicatively closed set of R, then $Ass_{R_S} M_S = \{\mathfrak{p}_S | \mathfrak{p} \cap S = \emptyset \text{ and } \mathfrak{p} \in \operatorname{Spec} R\}$.
4. If $N \subset M$, then $Ass_R N \subset Ass_R M$.
5. Suppose $N \subset M$. Then $N = 0$ if and only if $N_\mathfrak{p} = 0$ for all $\mathfrak{p} \in Ass_R M$.

Let us prove this last item.

Proof. Suppose $N \subset M$. Certainly, if $N = 0$, then $N_\mathfrak{p} = 0$ for all primes $\mathfrak{p}$, including the ones in $\operatorname{Ass}_R M$.

If $N \neq 0$, then there exists some $\mathfrak{p} \in Ass_R N \subset Ass_R M$. But $\mathfrak{p} \in Ass_R N$. Therefore, by one of the remarks, we have that $Hom_{R_\mathfrak{p}}(k(p), N_\mathfrak{p}) \neq 0$. But certainly, if $N_\mathfrak{p} = 0$, then all homomorphisms into this would be 0. Since this is not the case, then $N_\mathfrak{p} \neq 0$. $\square$

Proposition 107. Let R be Noetherian, and let $M \neq 0$ be a finitely generated R-module. Then the set of zero divisors on M is the union of the associated primes. That is, $ZD_R(M) := \{r \in R | ru = 0 \text{ for some } u \in M \setminus \{0\} = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} \mathfrak{p}$.

Proof. Let $p \in Ass_R M$. Then $\mathfrak{p} = (0 :_R x)$ for some $x \in M$. Furthermore, $x \neq 0$, since $\mathfrak{p} \neq R$. Thus $\mathfrak{p}x = 0$, so $\mathfrak{p} \subset ZD_R(M)$. Thus $\bigcup_{\mathfrak{p} \in Ass_R M} \subset ZD_R(M)$.

Conversely, suppose $r \in ZD_R(M)$. Then $ru = 0$ for some $u \in M \setminus \{0\}$. Thus $r \in (0 :_R u)$. Let $\Lambda = \{(0 :_R v) | (0 :_R u) \subset (0 :_R v) \text{ for some } v \neq 0\}$. Since $(0 :_R u) \in \Lambda$, then Λ is nonzero. Also, R is Noetherian, so one can choose a $(0 :_R v)$ which is maximal in Λ.

One can show that $(0 :_R v)$ is prime [we made an identical argument previously], so $(0 :_R v) \in Ass_R M$. But since $r \in (0 :_R v)$, then $r \in \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} \mathfrak{p}$. Thus $ZD_R(M) \subset \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} \mathfrak{p}$.

Thus $ZD_R(M) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}_R(M)} \mathfrak{p}$. $\square$

Proposition 108. Let R be Noetherian, and let $M \neq 0$ be a finitely generated R-module. Then the radical of the annihilator is the intersection of the associated primes. That is, $\sqrt{\operatorname{Ann}_R M} = \bigcap_{\mathfrak{p} \in Ass_R M} \mathfrak{p}$.

Proof. Let $(0) = Q_1 \cap ... \cap Q_t$ be an irredundant primary decomposition for (0) in M. Then $\operatorname{Ann}_R M = \bigcap_{i=1}^t \operatorname{Ann}_R M/Q_i$. Thus, by elementary properties of radicals, $\sqrt{\operatorname{Ann}_R M} = \bigcap_{i=1}^t \sqrt{\operatorname{Ann}_R M/Q_i} = \bigcap_{\mathfrak{p} \in \operatorname{Ass}_R M} \mathfrak{p}$. $\square$

Recall that if M is a (finitely generated) R-module, then $Supp_R M = \{\mathfrak{p} \in \operatorname{Spec} R | M_\mathfrak{p} \neq 0\}$. Recall also that if M is finitely generated, then $Supp_R M = V(\operatorname{Ann}_R M)$.

Definition 126. Define the *minimal primes* of M to be the set of minimal primes in $Supp_R M$.

We use the following notation: $Min_R M = \{\mathfrak{p} \in Supp_R M | M_q = 0 \text{ for all } \mathfrak{q} \subset \mathfrak{p}\}$.

Remark 144. If M is finitely generated, then $Min_R M = \{\mathfrak{p} \in \operatorname{Spec} R | \mathfrak{p} \text{ is minimal over } \operatorname{Ann}_R M\}$.

Proposition 109. Let R be a Noetherian ring, and let M be a finitely generated R-module. Then $Min_R M \subset Ass_R M \subset Supp_R M$.

Proof. Let $\mathfrak{p} \in Min_R M$. Note that $\mathfrak{p} \in Ass_R M$ if and only if $\mathfrak{p}R_\mathfrak{p} \in Ass_{R_\mathfrak{p}} M_\mathfrak{p}$. But $Supp_{R_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\}$ since $\mathfrak{p} \in Min_R M$. Thus $Ass_{R_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{p}R_\mathfrak{p}\}$, so $\mathfrak{p} \in Ass_R M$.

Suppose now that $\mathfrak{p} \in Ass_R M$. Then $HoM_{R_\mathfrak{p}}(k(p), M_\mathfrak{p}) \neq 0$, so like we said above, $M_\mathfrak{p} \neq 0$. That is, $\mathfrak{p} \in Supp_R M$. $\square$

Lemma 44. Let R be a ring, let I be an ideal, and let M be a finitely generated R-module. If $IM = M$, then there exists an $s \in I$ such that $(1-s)M = 0$.

Proof. Suppose $\mathfrak{p} \in \operatorname{Spec} R$, and that $I \subset \mathfrak{p}$. Then $I_\mathfrak{p} M_\mathfrak{p} = M_\mathfrak{p}$. Since $I \subset \mathfrak{p}$, then $I_\mathfrak{p} \subset \mathfrak{p}R_\mathfrak{p}$, so $(\mathfrak{p}R_\mathfrak{p})M_\mathfrak{p} = M_\mathfrak{p}$. But $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal in the semi-local ring $R_\mathfrak{p}$, so by Nakayama's Lemma, we have that $M_\mathfrak{p} = 0$. Thus $\mathfrak{p} \notin \operatorname{Ann}_R M$.

Thus $I + \operatorname{Ann}_R M = R$ [why?]. In particular, there exists $s \in I$ and $t \in \operatorname{Ann}_R M$ such that $s + t = 1$. Then $t = 1 - s \in \operatorname{Ann}_R M$. $\square$

15.2 Day 42 - April 27

Recall the following Lemma, which we proved last class:

Lemma 45. Let R be a ring, and let $I \subset R$ be an ideal. Llet M be a finitely generated R-module, and suppose $IM = M$. Then there exists $s \in I$ such that $(1-s)M = 0$.

Last class, we stated Krull's Intersection Theorem:

Theorem 111 (Krull's Intersection Theorem). Let R be a Noetherian ring, and let M be a finitely generated R-module, and let I be an ideal of I. Then there exists an $s \in I$ such that $(1-s)(\bigcap_{n=1}^\infty I^n M) = 0$. In particular, if $I \subset Jac(R)$, then $1 - s$ is a unit and $\bigcap_{n=1}^\infty I^n M = 0$.

Let us now prove it.

Proof. Let $N = \bigcap_{n \geq 1} I^n M$. Note that $N = IM \cap IN$. We then wish to show that there exists an $s \in S$ such that $(1-s)N = 0$.

We have two cases: either $IM = M$, or $IM \subsetneq M$.

In the former case, by the Lemma there exists an $s \in I$ such that $(1-s)M = 0$. Therefore

$$\begin{aligned} (1-s)N &= (1-s)(IM \cap IN) \\ &= (1-s)IM \cap (1-s)IN \\ &= (1-s)M \cap (1-s)IN \\ &= 0 \cap (1-s)IN \\ &= 0 \end{aligned}$$

as desired.

If $IM \neq M$, then $IN \subset N \subsetneq M$, so $IN \subsetneq M$.

Therefore, there exists an irredundant primary decompostion $IN = Q_1 \cap ... \cap Q_t$ for IN in M.

Suppose for the sake of contradiction that $IN \neq N$. If not, then $IN \subsetneq N$, so $N \subsetneq Q_i$ for some I. But $IN \subset Q_i$, so I consists of zero divisors on M/Q_i. Since Q_i is primary, then $I \subset \sqrt{\operatorname{Ann}_R(M/Q_i)}$. Since I if finitely generated, then this implies that $I^n \subset \operatorname{Ann}_R(M/Q_i)$ for some n.

That is, $I^n M \subset Q_i$ for some n. But $N \subset I^n M \subset Q_i$, so this contradicts the fact that $N \subsetneq Q_i$. Thus $IN = N$.

Since R is Noetherian, and $N \subset M$, a finitely generated R-module, then by the Lemma, there exists some $s \in I$ such that $(1-s)N = 0$. $\square$

Corollary 52. If R is Noetherian, and either a domain or a quasi-local ring, and $I \neq R$, then $\bigcap_{n \geq 0} I^n = 0$.

Now, let us turn back to primary decompositions. Sometimes, it turns out that the primary ideals in an irredundant primary decomposition are unique. This is summed up in the second uniqueness theorem.

Theorem 112. Let R be a Noetherian ring, and let M be a finitely-generated R-module. Let $N \subsetneq M$. Let $N = Q_1 \cap ... \cap Q_t$ be an irredundant primary decomposition, and for $i = 1, ..., t$, let $\mathfrak{p}_i = \sqrt{\operatorname{Ann}_R(M/Q_i)}$. Then, if some $\mathfrak{p}_i \in Min_R(M/N)$, then $Q_i = \phi^{-1}(N_{\mathfrak{p}_i})$, where $\phi : M \to M_{\mathfrak{p}_i}$ is the natural localization map. Therefore, the $\mathfrak{p}_i$-primary component for N in M is unique.

Proof. Let $S = R \setminus \mathfrak{p}_i$. Note that $\mathfrak{p}_j \cap S \neq \emptyset$ for $j \neq i$. Therefore, $(Q_j)_S = M_S$ for all $j \neq i$.

Therefore,

$$\begin{aligned} N_{\mathfrak{p}_i} &= (Q_1 \cap ... \cap Q_t)_{\mathfrak{p}_i} \\ &= (Q_1)_{\mathfrak{p}_i} \cap ... \cap (Q_t)_{\mathfrak{p}_i} \\ &= (Q_i)_{\mathfrak{p}_i} \end{aligned}$$

Note also that $(Q_i)_{\mathfrak{p}_i}$ is $\mathfrak{p}_i R_{\mathfrak{p}_i}$-primary in $M_{\mathfrak{p}_i}$.

We now wish to show that $Q_i = \phi^{-1}((Q_i)_{\mathfrak{p}_i})$.

For simplicity, let $Q = Q_i$, and let $\mathfrak{p} = \mathfrak{p}_i$. Let $u \in Q$. Then $\frac{u}{1} \in Q_{\mathfrak{p}}$, so $u \in \phi^{-1}(Q_{\mathfrak{p}})$. Thus $Q \subset \phi^{-1}(Q_{\mathfrak{p}})$.

Conversely, let $u \in \phi^{-1}(Q_{\mathfrak{p}})$. Then $\frac{u}{1} = \frac{v}{s}$ for some $v \in Q$ and $s \notin \mathfrak{p}$. Therefore, there exists some $s' \notin \mathfrak{p}$ such that $s'u = v \in Q$. Since $s' \notin \mathfrak{p} = \sqrt{\operatorname{Ann}_R(M/Q)}$, then $(Q :_M s') = Q$. Since $u \in (Q :_M s') = Q$, then $Q = \phi^{-1}(Q_{\mathfrak{p}})$, as desired.

□

Theorem 113. Let R be Noetherian, and let $M \neq 0$ be a finitely generated R-module. Then there exists a filtration of submodules of M $0 \subset N_0 \subset ... \subset N_t = M$ such that $N_i/N_{i-1} \cong R_{\mathfrak{p}_i}$ for some $\mathfrak{p}_i \in \operatorname{Spec} R$.

Proof. Choose some $\mathfrak{p}_1 \in Ass_R M$. Then $\mathfrak{p}_1 = (0 :_R x_1)$ for some $x_1 \in M$. Therefore $Rx_1 \cong R/\mathfrak{p}_1$ (by the isomorphism $R/\mathfrak{p} \to Rx_1$ by $\overline{r} \mapsto rx_1$.

Let $N_1 = Rx_1 \subset M$. If $N_1 = M$, then we are done.

If $N_1 \ncong M$, then choose $\mathfrak{p}_2 \in Ass_R(M/N)$. Then $\mathfrak{p}_2 = (N_1 :_R x_2)$. Let $N_2 = N_1 + Rx_2 = Rx_1 + Rx_2$. Therefore, $N_2/N_1 \cong R\overline{x}_2 \cong R/\mathfrak{p}_2$. We now have a chain $0 = N_0 \subset N_1 \subset N_2$.

If $N_2 \neq M$, we repeat. Eventually, this must terminate by the ascending chain condition. □

Here's how we normally use this result.

Remark 145. Suppose you have a property that is true for domains, and that it is "preserved by exact sequences" (meaning if $0 \to A \to B \to C \to 0$ is exact, then the property is true for B whenever it is true for A and C.)

Then, by the previous theorem, there exists a nice filtration. This gives us a bunch of exact sequences $0 \to N_k \to N_{k+1} \to N_{k+1}/N_k \to 0$. Since N_{k+1}/N_k is isomorphic to a domain by the previous theorem, our hypothetical property is true for it. Also, by induction, the property is true for N_k. Thus it is true for N_{k+1}.

In this way, we can induct and show that this is true for any finitely generated R-module!

Thanks for reading! Good luck in your algebra endeavors!
-Robert

Chapter 3

Appendix

This appendix was originally my ultra-condensed notes for when I was studying for my comprehensive exam. It consists of raw theorems and results about central concepts (almost all ring/module theory) that I considered essential to know. You might find it useful too!

1 Projective Modules

Here R is a ring, and P is a projective left R-module.

Definition 127. An left R-module P is called *projective* if any of the following equivalent conditions are met:

1. If $M \xrightarrow{f} N \to 0$ is exact and $g : P \to N$, then there exists some $h : P \to M$ such that $fh = g$.
2. Every short exact sequence of the form $0 \to L \to M \to P \to 0$ splits.
3. P is the direct summand of a free module.
4. $Hom_R(P, -)$ is exact.
5. $P_{\mathfrak{p}}$ is free for all $\mathfrak{p} \in \operatorname{Spec} R$.
6. $P_{\mathfrak{m}}$ is free for all $\mathfrak{m} \in \operatorname{Maxspec} R$.

Theorem 114. If R is a polynomial ring, then every f.g. projective module over R is free.

Theorem 115. If R is a semilocal ring, then every f.g. projective module over R is free.

Theorem 116. If R is commutative, S is a multiplicatively closed subset of R, and P is a projective R-module, then P_S is a projective R_S module.

Theorem 117. If P is a finitely generated projective R-module, then the map $f : \operatorname{Spec} R \to \mathbb{N}_0$ given by $\mathfrak{q} \mapsto \operatorname{rk} P_{\mathfrak{q}}$ is continuous (with respect to the discrete topology on $\mathbb{N}_0$).

Theorem 118. Projective modules are flat.

Example 125. Free modules are projective. D^n is projective over $M_n(D)$ (where D is a division ring). Summands of free modules are projective. Direct sums of projective modules are projective.

2 Injective Modules

Here R is a ring and E is an injective R-module.

Definition 128. A left R-module E is called *injective* if any of the the following equivalent conditions are met:

1. If $0 \to M \xrightarrow{g} N$ is exact, and $f : M \to E$, then there exists an $H : N \to E$ such that $hg = f$.
2. (Baer's Criterion) For all left ideals I of R and $f : I \to E$, if $i : I \to R$ is the inclusion map, there exists an $h : R \to E$ such that $hi = f$.
3. $Hom_R(-, E)$ is exact.
4. Every short exact sequence of the form $0 \to E \to M \to N \to 0$ splits.

Theorem 119. Let $E = \prod_{i \in I} E_i$ be a product of left R-modules. Then E is injective if and only if each E_i is injective.

Theorem 120. E is divisible (i.e. for all non-zero-divisors $r \in R$, and all $u \in E$, there exists $u' \in E$ such that $u = ru'$.

Theorem 121. If R is a PID, then every divisible module is injective.

Example 126. Let R be a PID. Then $Q(R)$ is injective. $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module. $k[x]/x^2$ is an injective itself-module. If E is injective, and $\phi : R \to S$ is a ring homomorphism (so S is an R-module), then $Hom_R(S, E)$ is injective. Every module is contained in an injective hull. A direct summand of an injective module is injective.

3 Semisimple Modules

Definition 129. A (left) R-module M is called *semisimple* if any of the following conditions are met:

1. Every submodule of M is a direct summand of M.
2. M is the sum of simple submodules.
3. M is the direct sum of simple submodules.

Theorem 122. Any submodule of a semisimple module is semisimple.

Theorem 123. Any nonzero semisimple module contains a simple submodule.

Theorem 124. If M is semisimple, then the following are equivalent:

1. M is Artinian.
2. M is Noetherian.
3. M is finitely generated.
4. $\lambda(M) < \infty$.

4 Semisimple Rings

Definition 130. A ring R is called *semisimple* if any of the following conditions are met:

1. R is semisimple as a left- or right- R-module.
2. R is the direct sum of matrix rings over division rings.
3. $J(R) = 0$ and R is left Artinian.
4. Every R-module is projective.

Theorem 125. A module over a semisimple ring is semisimple.

Theorem 126. If R is semisimple, $J(R) = 0$.

Theorem 127. Let k be a field of characteristic p (possibly $p = 0$). Then $k[G]$ is semisimple if and only if $|G| < \infty$ and $p \nmid |G|$.

5 Localization

Here, R is a commutative ring, and S is a multiplicatively closed subset of R containing 1, and M is an R-module.

Theorem 128. If R is Noetherian (resp. Artinian), then so is R_S.

Theorem 129. If I is an ideal in R, then $I_S = R_S$ if and only if I intersects S.

Theorem 130. $\operatorname{Spec} R_S$ is in natural bijection with $\{\mathfrak{p} \in \operatorname{Spec} R | \mathfrak{p} \cap S = \emptyset\}$ (by $\mathfrak{p} \mapsto \mathfrak{p}_S$).

Theorem 131. $M_S \cong M \otimes_R R_S$.

Theorem 132. R_S is a flat R-module (i.e. localizing is exact).

Theorem 133. The following are equivalent:

1. $M = 0$.
2. $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec} R$.
3. $M_\mathfrak{m} = 0$ for all $\mathfrak{m} \in \operatorname{Maxspec} R$.

Theorem 134. If $Ann_R M$ intersects S, then $M_S = 0$. If M is finitely generated, then the converse holds (i.e. $M_S = 0$ implies $Ann_R(M)$ intersects S).

6 Hom Modules

Definition 131. Let F be an additive covariant functor on module categories. Then F is *left exact* if, whenever $0 \to A \to B \to C$ is exact at B, then $0 \to F(A) \to F(B) \to F(C)$ is exact at $F(B)$.

We say F is *right exact* if, whenever $A \to B \to C \to 0$ is exact at B, then $F(A) \to F(B) \to F(C) \xrightarrow{0}$ is exact at $F(B)$.

Theorem 135. For R a ring and M a module, $M \otimes_R -$ is right exact.

Definition 132. We say M is flat if $M \otimes_R -$ is exact.

Theorem 136. For any ring R, R and R_S are both flat as R-modules.

Theorem 137. If R is a ring, then any projective R-module is flat.

Theorem 138. The functors $Hom_R(M,-)$ and $Hom_R(-,N)$ are left exact.

Theorem 139. Hom in either coordinate distributes over direct sums.

Theorem 140. For any modules, $\oplus A_i$ is flat if and only if each A_i is flat.

Theorem 141. ($Hom - \otimes$ Adjointness/Adjunction) Let R, S, and T be rings. Let A be an $R-T$ bimodule, B be an $S-R$ bimodule, and C be a left S-module. Then the map $Hom_R(A, Hom_S(B,C)) \to Hom_S(B \otimes_R A, C)$ (which lives in the set of T-module homomorphisms) given by $\phi \mapsto \left(g_\phi : \begin{cases} B \otimes_R A \to C \\ b \otimes a \mapsto \phi(a)(b) \end{cases} \right)$ is a well-defined left T-module isomorphism.

7 Tensors and Flat Modules

Here R is a ring and M is an R-module.

Theorem 142. (Universal Property for Tensor Products) Let $h : M \times N \to M \otimes_R N$ be the natural map. For any abelian group A and R-biadditive map $f : M \times N \to A$, there exists a unique group homomorphism $g : A \to M \otimes_R N$ such that $f = g \circ h$.

Definition 133. We say M is flat if tensoring by M is exact.

Theorem 143. If I and J are ideals, then $R/I \otimes_R R/J \cong R/(I+J)$.

Theorem 144. Tensors distribute over arbitrary direct sums.

8 Primary Decompositions

Theorem 145. Suppose N is a primary submodule of M. Then $\sqrt{Ann_R(M/N)}$ is prime.

Theorem 146. If $I \subset R$ is primary, then $\sqrt{I}$ is prime. If $\sqrt{I}$ is maximal, then I is primary.

Theorem 147. Irreducible submodules of Noetherian modules are primary.

Theorem 148. If $M \neq 0$, then every proper submodule of M has an (irredundant) primary decomposition.

Theorem 149. Primary submodules play nicely with localization: if $Q \subset M$ is $\mathfrak{p}$-primary, then $Q_S = M_S$ if and only if $\mathfrak{p} \cap S \neq \emptyset$. Also, if $\mathfrak{p} \cap S = \emptyset$, then Q_S is $\mathfrak{p}_S$-[rimary.

Theorem 150 (First Uniqueness Theorem). If R is Noetherian, M is a finitely generated R-module, and N is a proper submodule, then the associated primes of an irredundant primary decomposition of N are independent of the primary decomposition, and denoted by $Ann_R(M/N)$.

Theorem 151 (Second Uniqueness Theorem). If M is a finitely generated module over a Noetherian ring, and $\mathfrak{p}_i \in Min(M/N)$, then the $\mathfrak{p}_i$-primary component of N is unique in any irredundant primary decomposition.

Theorem 152. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then the following are equivalent:

1. $\mathfrak{p} \in Ass_R(M)$
2. $\mathfrak{p} = \sqrt{Ann_R(M/Q_i)}$ for some primary component Q_i in any primary decomposition of 0.
3. $\mathfrak{p} = (0 :_R x)$ for some $x \in M$.
4. There exists an injective R-module homomorphism $R/\mathfrak{p} \to M$ given by $\overline{1} \mapsto x$.

5. $Hom_{R_\mathfrak{p}}(k(\mathfrak{p}), M_\mathfrak{p}) \neq 0$.

Theorem 153. We have the following other results:

1. $N = 0$ if and only if $Ass_R(M/N) = \emptyset$.
2. If S is multiplicatively closed, then $Ass_{R_S}(M_S) = \{\mathfrak{p}_S | \mathfrak{p} \cap S = \emptyset \text{ and } \mathfrak{p} \in \operatorname{Spec} R\}$.
3. If $N \subset M$, then $Ass_R N \subset Ass_R M$.
4. If $N \subset M$, then $N = 0$ if and only if $N_\mathfrak{p} = 0$ for all $\mathfrak{p} \in Ass_R(M)$.

Theorem 154 (Krull's Intersection Theorem). Let R be a Noetherian ring, and let M be a finitely generated R-module, and let I be an ideal of R. Then there exists an $s \in I$ such that $(1-s)(\bigcap I^n M) = 0$.

Corollary 53. If R is Noetherian and either a domain or a quasi-local ring, then for any proper ideal I, $\bigcap I^n = 0$.

9 Integral Extensions

Theorem 155 (Lying Over Theorem). Let S be an integral extension of R. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then there exists $\mathfrak{q} \in \operatorname{Spec} S$ such that $\mathfrak{p} = R \cap \mathfrak{q}$.

Theorem 156 (Incomparability Theorem). Let S be an integral extension of R. Let $\mathfrak{q}_1, \mathfrak{q}_2$ lie over $\mathfrak{p}$. Then $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are incomparable.

Theorem 157 (Going Up Theorem). Let S be an integral extension of R. Then one can "go up" chains of primes.

Theorem 158 (Going Down Theorem). Let S be an integral extension of R, and assume both R and S are domains. Suppose also that R is integrally closed in $Q(R)$. Then one can "go down" chains of primes.

10 Techniques For 0

Theorem 159. Let M be an R-module. Then the following are equivalent:

1. $M = 0$.
2. $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec} R$.
3. $M_\mathfrak{m} = 0$ for all $\mathfrak{m} \in \operatorname{Maxspec} R$.

If M is finitely generated, the following are also equivalent:

1. $M = 0$.
2. (Nakayama's Lemma) $M = JM$ (where J is the Jacobson radical).

If $N \subset M$ and R is Noetherian, then the following are equivalent:

1. $N = 0$
2. $Ass_R(M/N) = \emptyset$
3. $N_\mathfrak{p} = 0$ for all $\mathfrak{p} \in Ass_R(M)$.

Chapter 4

Index

Index