Math 210B Lecture Notes

Professor: Romyar Sharifi
Scribe: Daniel Raban

Contents

1 Free Modules

1.1 Free modules over rings

Let R be a commutative ring.

Definition 1.1. An R-module M is **free** on a subset X if for any R-module N and map $f : X \to N$, there exists a unique R-module homomorphism $\phi_f : M \to N$ such that $\phi_f|_X = f$.

Example 1.1. If X is a set, we can construct the free module on X: $F_X = \bigoplus_{x \in X} R \cdot x$.

We can think of this as a functor F from Set to R-mod. With this viewpoint, if $f : X \to Y$, then $F(f) : F_X \to F_Y$ is given by $F(f)(\sum_{i=1}^n a_i x_i) = \sum_{i=1}^n a_i f(x_i)$. So for $F : \text{Set} \to \text{R-mod}$,

$$\mathrm{Hom}_{\text{Set}}(X, N) \cong \mathrm{Hom}_{\text{R-mod}}(F_X, N),$$

where this isomorphism is natural. That is, F is left-adjoint to the forgetful functor from R-mod to Set.

Lemma 1.1. *An R-module M is free on X if and only if*

1. *X generates M as an R-module (i.e. for all $m \in M$, there exist $x_1, \ldots, x_n \in X$ and $a_1, \ldots, a_n \in R$ such that $m = \sum a_i x_i$)*
2. *X is R-linearly independent (i.e. if $\sum_{i=1}^n a_i x_i = 0$ with $s_1, \ldots, x_n \in X$ distinct, then $a_i = 0$ for all i).*

Proof. If M is free on X¡ then there exists a unique isomorphism from M to F_X, induced by the identity on X. F_X satisfies these two properties, so M does.

If M satisfies the two properties, then there exists a unique $\phi : F_X \to M$ sending $x \mapsto X$ (since $X \subseteq M$). Property 1 implies that ϕ is surjective, and property 2 implies that ϕ is injective. $\square$

1.2 Bases and vector spaces

Definition 1.2. If X generates the R-module M and is linearly independent, we call it a **basis** of the M.

Theorem 1.1. *Every vector space V over a field has a basis. In fact, every linearly independent set in V is contained in a basis, and every spanning set contains a basis.*

Proof. We will prove the first statement; the other two statements follow by a similar argument. Let V be an F-vector space, where F is a field. Conide the set S of subsets X of V that are F-linearly independent. $(S, \subseteq)$ is a partially ordered set (poset). If C is a chain, $\bigcup_{X \in C} X$ is linearly independent, so it is an upper bound on C. By Zorn's lemma, S has a maximal element B. Let $W = \mathrm{span}(B)$. If $v \in V \setminus W$, then $B \cup \{v\}$ is linearly independent, contradicting the maximality of B. Then $V = W$, so B is a basis. $\square$

Example 1.2. The field condition is very important; here are counterexamples for general rings. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}$. Then $2 \in \mathbb{Z}$, but 2 is not contained in a basis of $\mathbb{Z}$. The set $\{2, 3\}$ spans $\mathbb{Z}$, but does not contain a basis.

Proposition 1.1. *Let V be an F-vector space with a basis of n elements. Let $Y \subseteq W$.*

1. *If Y spans V, then $|Y| \geq n$.*

2. *If Y is linearly independent, then $|Y| \leq n$.*

3. *If $|Y| = n$, then Y is linearly independent iff Y spans V.*

Remark 1.1. The first two properties hold for free modules with a basis of n elements as well, but the 2nd property becomes harder to prove. For the third property, in the general case, we just have that if Y spans and $|Y| = n$, then Y is linearly independent.

Corollary 1.1. *If $\varphi : V \to W$ is an F-linear transformation of finite-dimensional vector spaces over F, then $\dim_F(V) = \dim_F(\ker(\varphi)) + \dim_F(\mathrm{im}(\varphi))$. In particular, if $\dim V = \dim W$, then φ is injective iff φ is surjective iff φ is an isomorphism.*

1.3 Cardinality of bases

Theorem 1.2. *If X and Y are sets and $F_X \cong F_Y$, then X and Y have the same cardinality.*

Proof. Suppose $|Y| \geq |X|$ and first suppose that X is infinite. It suffices to show F_X has no basis of cardinality $> |X|$. Suppose $B \subseteq F_X$ is a basis of F_X. Every $x \in X$ is a finite linear combination of some elements in B; let B_x be the set of these. Then $|\coprod_{x \in X} B_x| \geq |\bigcup_{x \in X} B|$ and it generates F_X, so we can get the upper bound on cardinality $|B| \leq |\mathbb{Z} \times X| = |X|$. Therefore, F_X has no basis of cardinality $> |X|$.

If Y is finite, let $\mathfrak{m}$ be a maximal ideal of R. Then $F = R/\mathfrak{m}$ is a field, and

$$F_X/\mathfrak{m}F_X \cong \left(\bigoplus_{x \in X} R\right) / \mathfrak{m} \left(\bigoplus_{x \in X} R\right) \cong \bigoplus_{x \in X} F.$$

The same is try for F_Y. The isomorphism $F_X \cong F_Y$ induces the isomorphism of F-vector spaces $F_X/\mathfrak{m}F_X \cong F_Y/\mathfrak{m}F_Y$, which then have bases of cardinality $|X|$ and $|Y|$. Y is finite, so X is finite and has cardinality $|X| = |Y|$. $\square$

2 Introduction to Field Theory

2.1 Field extensions

Definition 2.1. A field E is an **extension field** (or **extension**) of a field F if F is a subfield of E.

We often write E/F to denote that E is an extension of F. F is called the **ground field** of E/F. E is an F-vector space. If E is finite dimensional over F, we say that E/F is a finite extension.

Definition 2.2. Let E be finite dimensional over F. Then the **degree** $[E : F]$ is $\dim_F(E)$.

Definition 2.3. Let $S \subseteq E$. We say S **generates** E/F if E is the smallest subfield of E containing F and S.

If $S = \{\alpha_1, \dots, \alpha_n\}$, we write $E = F(\alpha_1, \dots, \alpha_n)$.

Lemma 2.1. *Every field F is an extension of $\mathbb{Q}$ if $\operatorname{char}(F) = 0$ and $\mathbb{F}_p$ if $\operatorname{char}(F) = p$.*

Proof. $\mathbb{Q}$ or $\mathbb{F}_p$ here is the subfield generated by 1. □

Definition 2.4. An **intermediate field** E' in E/F is a subfield of E containing F.

Example 2.1. $Q(i)$ and $Q(\sqrt{2})$ are intermediate fields of $\mathbb{C}/\mathbb{Q}$.

Note that $\mathbb{Q}(i) = \mathbb{Q}[i] \subseteq \mathbb{C}$ and $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{C}$. This is not always the case.

Example 2.2. Let $\mathbb{Q}(x) = \{f/g : f, g \in \mathbb{Q}[x], g \neq 0\}$. The field of rational functions is $\mathbb{Q}(\mathbb{Q}[x])$. $\mathbb{Q}(x) \neq \mathbb{Q}[x]$

Lemma 2.2. *Let E/F be an extension and $\alpha \in E$. Then $F(\alpha) = \mathbb{Q}(F[\alpha])$.*

Proof. $F(\alpha)$ is the smallest subfield containing $F \cup \{\alpha\}$. $F[\alpha]$ is the smallest subring containing $F \cup \{\alpha\}$. The inclusion $\iota : F[\alpha] \to F(\alpha)$ is injective and induces an isomorphism $Q(F[\alpha]) \to F(\alpha)$ of fields. □

2.2 Algebraic extensions, minimal polynomials, and splitting fields

Definition 2.5. If E/F is an extension and $\alpha \in E$, then α is **algebraic** (over F) if $F[\alpha] = F(\alpha)$ and **transcendental** otherwise. E/F is **algebraic** if every $\alpha \in E$ is algebraic over F and transcendental otherwise.

Proposition 2.1. *If $\alpha \in E$ is algebraic over F. then there exists a unique monic irreducible polynomial $f \in F[x]$ such that $f(\alpha) = 0$. Moreover, $F[x]/(f) \cong F(\alpha)$ by sending $g(x) \mapsto g(\alpha)$.*

This f is called the **minimal polynomial** of α over F.

Proof. Note that $1/\alpha = g(\alpha)$ for some $g \in F[x]$. Then $\alpha g(\alpha) - 1 = 0$. Set $h = xg(x) - 1$. There exists a monic irreducible $f \mid h$ such that $f(\alpha) = 0$. If $p \in F[x]$ satisfies $p(\alpha) = 0$ and $f \nmid p$, then $(f, p) = (1)$. But the ideal generated by α is not trivial. So $f \mid p$. The last statement follows. $\square$

Corollary 2.1. *If α is algebraic over F, then $F(\alpha)/F$ is finite of degree equal to the degree of the minimal polynomial of α with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ over F.*

Proposition 2.2. *If E/F is finite and $\alpha \in E$, then α is algebraic.*

Proof. The set $\{1, \alpha, \ldots, \alpha^{[E:F]}\}$ is linearly depedent. The relation gives a polynomial with α as a root. $\square$

Corollary 2.2. *If E/F is finite, then $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$.*

Theorem 2.1 (Kronecker)**.** *Given nonconstant $f \in F[x]$, there exists E/F such that E contains a root of F.*

Proof. Take $F[x]/(g)$, where g is monic, irreducible, and $g \mid f$. $\square$

Definition 2.6. A **splitting field** for nonconstant $f \in F[x]$ is a field E in which f factors into a product of linear polynomials.

Corollary 2.3. *For any nonconstant $f \in F[x]$, there exists a splitting field for f over F.*

Example 2.3. A splitting field for $x^3 - 2$ (over $\mathbb{Q}$) in $\mathbb{C}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2})$, where $\omega = e^{2\pi i/3}$.

2.3 Degrees of extensions

Theorem 2.2. *If K/E and E/F are extensions, A is a basis of E/F, and B is a basis of K/E, then $AB \cong A \times B$ is a basis of K/F.*

Proof. If $\gamma \in K$, then $\gamma = \sum c_j \beta_j$, where $c_j \in E$. Then $c_j = \sum d_{i,j}\alpha_i$, where $\alpha_i \in f$. So $\gamma = \sum_i \sum_j d_{i,j}\alpha_i\beta_j$. So AB spans K. If $\sum(\sum a_{i,j}\alpha_i)\beta_j = 0$, then $\sum a_{i,j}\alpha_i = 0$ for all j. Then $a_{i,j} = 0$ for all i, j. $\square$

Corollary 2.4. *If K/E and E/F are finite, then $[K : F] = [K : E][E : F]$.*

Definition 2.7. Let $E, E' \subseteq K$ be subfields. The **compositum** EE' is the smallest subfield of K containing E and E'.

Example 2.4. If E/F, then $E(\alpha) = EF(\alpha)$.

Example 2.5. $F(\alpha, \beta) := F(\alpha)(\beta) = F(\alpha)F(\beta)$.

Proposition 2.3. *If E, E' are finite over F and contained in K, A is a basis of E/F, and B is a basis of E'/F, teen AB spans EE'.*

Proof. Let $A = \{\alpha_1, \dots, \alpha_m\}$ and $B = \{\beta_1, \dots, \beta_n\}$. Then $EE' = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n) = F[\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n]$. Note that $\alpha_1^{i_1} \cdots \alpha_m^{i_m} \in E$ is a linear combination over F of the α_is. Similarly for the β_js in E'. So the $\alpha_i\beta_j$s span EE'. $\square$

Corollary 2.5.
$$[EE' : F] \leq [E : F][E' : F].$$

Corollary 2.6. *If $[E : F]$ and $[E' : F]$ are relatively prime, we get equality.*

Proof. $[E : F]$ and $[E' : F]$ divide $[EE' : F]$. $\square$

Example 2.6. Consider $\mathbb{Q}(\sqrt[3]{2}, \omega^3\sqrt[3]{2})$, where $\omega^2 + \omega + 1 = 0$. Then
$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\omega^3\sqrt[3]{2}) : \mathbb{Q}] = 9, \qquad [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] = 6.$$

Proposition 2.4. *Let E_i be subfields of K containing F for all i in some index set I. The the compositum E of all E_i is $\bigcup F(\alpha_1, \dots, \alpha_n)$, where $n \geq 0$, and each α_j is in some E_i.*

3 Finite Fields and Cyclotomic Fields

3.1 Finite fields

Proposition 3.1. *Let F be a field and $n \geq 1$. Let $\mu_n(F)$ be the n-th roots of unity in F. Then $\mu_n(F)$ is cyclic of order dividing n.*

Proof. Let m be the exponent of $\mu_n(F)$. Then $x^m - 1 = 0$ for all $x \in \mu_n(F)$. So $|\mu_n(F)| \leq m$. Then $|\mu_n(F)| = m$. □

Lemma 3.1. *Let F be a finite field. Then $|F|$ is a power of* $\mathrm{char}(F)$*.*

Proof. Let $p = \mathrm{char}(F)$. Then F is a vector space over $\mathbb{F}_p$. Then $|F| = p^{[F:\mathbb{F}_p]}$. □

Corollary 3.1. *If $|F| = p^n$, then $F^\times$ is cyclic with $F^\times = \mu_{p^n-1}(F)$.*

Corollary 3.2. $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Lemma 3.2. *Let* $\mathrm{char}(F) = p$ *and $\alpha, \beta \in$. Then $(\alpha+\beta)^{p^k} = \alpha^{p^k} + \beta^{p^k}$.*

Proof. This follows from the Binomial theorem. □

Theorem 3.1. *Let $n \geq 1$. Then there exists a unique extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ of degree n up to isomorphism. If $E/\mathbb{F}_p$ is a finite extension of degree a multiple of n, then E contains a unique subfield isomorphic to $\mathbb{F}_{p^n}$. Moreover, $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p^m \iff n \mid m$.*

Proof. Let $\mathbb{F}_{p^n}$ be the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let $F = \{\alpha \in \mathbb{F}_{p^n} L \alpha^{p^n} = \alpha\}$. Note that F is closed under addition by the lemma and is closed under multiplication and taking inverses of nonzero elements. So F is a field. In fact, F is a splitting field of the polynomial, so $F = \mathbb{F}_{p^n}$.

We know that $|\mathbb{F}_{p^n}| \leq p^n$ because the polynomial $x^{p^n} - x$ has at most p^n roots; we want equality. Let $a \in \mathbb{F}_{p^n}^\times$. Consider the polynomial $g(x) = (x^{p^n} - x)/(x-a)$. Then $g(x) = \sum_{i=1}^{p^n-1} a^{i-1} x^{p^n-i}$. Then

$$g(a) = \sum_{i=1}^{p^n-1} a^{p^n-1} = (p^n-1)a^{p^{n-1}} = (0-1)1 = -1 \neq 0.$$

So $x^{p^n} - x$ has p^n distinct roots, giving us $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Let E have degree m, where $n \mid m$. Then $E \cong \mathbb{F}_{p^m}$, so $E^\times = \mu_{p^m-1}(E)$. Since $\mu_{p^n-1}(E) \subseteq \mu_{p^m-1}(E)$, we have $F \subseteq E$ with $F \cong \mathbb{F}_{p^n}$. □

Example 3.1. $[\mathbb{F}_9 : \mathbb{F}_3] = 2$. We can compute that x^2+1, x^2+x-1, and x^2-x-1 are the quadratic irreducible polynomials over $\mathbb{F}_3$. $\mathbb{F}_9$ is the splitting field of each. We get

$$x^9 - x = (x^2+1)(x^2+x-1)(x^2-x-1)x(x+1)(x-1).$$

Proposition 3.2. *Let q be a power of p. Let $m \geq 1$, and let ζ_m be a primitive m-th root of unity in an extension of $\mathbb{F}_q$. Then $[\mathbb{F}_q(\zeta_m) : \mathbb{F}_q]$ equals the order of q in $(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof.

$$\begin{aligned}
\ell = [\mathbb{F}_q(\zeta_m) : \mathbb{F}_q] &\iff \mathbb{F}_q(\zeta_m) = \mathbb{F}_{q^\ell} \\
&\iff m \mid q^\ell - 1 \text{ and } m \nmid q^{j-1} \text{ for all } j < \ell \\
&\iff q \text{ has order } \ell \text{ in } (\mathbb{Z}/m\mathbb{Z})^\times.
\end{aligned}$$

□

Proposition 3.3. *Let $m \geq 1$ and $m = p_1^{r_1} \cdots p_k^{r_k}$, where the p_i are distinct primes. THen $(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})\times$, and*

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & p \text{ odd} \\ \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p = 2, r \geq 2. \end{cases}$$

Proof. The map $(\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ has kernel

$$\frac{1 + p\mathbb{Z}}{1 + p^r\mathbb{Z}} \subseteq (\mathbb{Z}/p^r\mathbb{Z})^\times.$$

If p is odd,

$$(1 + p^k)^p = 1 + p^{k+1} + \cdots + (p^k)^p.$$

Then $kp > k + 1 \iff k(p-1) > 1 \iff k \geq 2$ or $p \geq 3$. So if p is odd, then $(1 + p^k)^p \cong 1 + p^{k+1} \pmod{p}^{k+2}$. This argument gives us that $1 + p$ has order p^{r-1} in $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

For $p = 2$, look at

$$\frac{1 + 4\mathbb{Z}}{1 + 2^r\mathbb{Z}}.$$

Then $(1 + 4)^{2^i} \cong 1 + 2^{i+2} \pmod{2}^{i+3}$. So $1 + 4$ has order 2^{r-2}. This gives us that $\mathbb{Z}/2^r\mathbb{Z} = \langle -1 \rangle + (1 + 4\mathbb{Z})/(1 + 2^r\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$. □

3.2 Cyclotomic fields and polynomials

Let ζ_n be a primitive n-th root of 1 in an extension of $\mathbb{Q}$ (e.g. $\zeta_n = 2^{\pi i/n} \in \mathbb{C}$) such that $\zeta_n^{n/m} = \zeta_m$ for all $m \mid n$.

Definition 3.1. $\mathbb{Q}(\zeta_n)$ is the n-th **cyclotomic field** over $\mathbb{Q}$.

Remark 3.1. $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\mu_n)$, where μ_n is the set of n-th roots of unity in $\mathbb{C}$.

Definition 3.2. The n-th **cyclotomic polynomial** Φ_n is the unique monic polynomial in $\mathbb{Q}[x]$ with roots the primitive n-th roots of 1.

Note that

$$\Phi_n = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (x - \zeta_n^i),$$

$$x^n - 1 = \prod_{\substack{d|n \\ d \geq 1}} \Phi_d.$$

So $\Phi_n \in \mathbb{Q}[x]$ by induction. The degree of Φ_n is $\varphi(n) = |\{1 \leq i \leq n : (i, n) = 1\}|$.

4 Möbius Inversion, Cyclotomic Polynomials, and Field Embeddings

4.1 Möbius inversion and cyclotomic polynomials

Definition 4.1. The **Möbius function** $\mu : \mathbb{Z}_{\geq 1} \to \{-1, 0, 1\}$ is given by

$$\mu(n) = \begin{cases} (-1)^k & n \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 4.1. *For $n \geq 2$,*

$$\sum_{d|n} \mu(d) = 0.$$

Proof. First,

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d),$$

where m is the product of the distinct primes dividing n. Say there are k of them. Then

$$\sum_{d|m} \mu(d) = 1 - k + \binom{k}{2} + \cdots + (-1)^k = (1-1)^k = 0. \qquad \square$$

Theorem 4.1 (Möbius inversion formula)**.** *Let A be an abelian group, and let $f : \mathbb{Z}_{\geq 1} \to A$. Define $g : \mathbb{Z}_{\geq 1} \to A$ by $g(n) = \sum_{d|n} f(d)$. Then*

$$f(n) = \sum_{d|n} \mu(d) g(n/d).$$

Proof. By the lemma,

$$\begin{aligned} \sum_{d|n} \mu(n/d) g(d) &= \sum_{d|n} \sum_{k|d} \mu(n/d) f(k) \\ &= \sum_{k|n} \sum_{\substack{d|n \\ k|d}} \mu(n/d) f(k) \\ &= \sum_{k|n} \left(\sum_{c|n/k} \mu((n/k)/c) \right) f(k) \\ &= f(n). \end{aligned} \qquad \square$$

Corollary 4.1.

$$\Phi_n = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Proof. Let $A = \mathbb{Q}(x)^x$, and let f send $d \mapsto \Phi_d$. Then

$$g(n) = \prod_{d \ midn} \Phi_d = x^n - 1.$$

Now apply the Möbius inversion formula. □

Example 4.1. $\Phi_1 = x - 1$, $\Phi_2 = x + 1$,and $\Phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1$, where p is prime. If $p \mid n$, then $\Phi_{pn}(x) = \Phi_n(x^p)$. This also gives us that

$$\Phi_{p^n} = x^{p^{n-1}(p-1)} + \cdots + x^{p^{n-1}} + 1.$$

If $p \neq q$ are primes,

$$\Phi_{pq}(x) = \frac{\Phi_q(x^p)}{\Phi_q(x)}$$

$$\frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)} = \frac{\Phi_q(x^p)}{\Phi_q(x)}.$$

$$\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

Theorem 4.2. *Φ_n is irreduible in $\mathbb{Q}[x]$.*

Proof. Suppose $\Phi_n = fg$ with f a monic irreducible polynoimal, and let ζ be a root of f. For $p \nmid n$ prime, ζ^p is a root of Φ_n. If ζ^p is a root of g, then $g(x^p)$ has ζ as a root, so $f(x) \mid g(x^p)$. Reduce f and $g \pmod p$. We get $\overline{f}, \overline{g} \in \mathbb{F}_p[x]$. Then $\overline{g}(x^p) = \overline{g}(x)^p$. Then $\overline{f} \mid \overline{g}^p$, but $\overline{f}$ has no multiple roots in $\mathbb{F}_p$, so $\overline{f} \mid \overline{g}$. So Φ_n has multiple roots $\pmod p$¡ which is a contradiction. So ζ^p is a root of f. Therefore, ζ^a is a root of f for all $a \in \mathbb{Z}$ and $\gcd(a, n) = 1$, so $f = \Phi_n$. □

4.2 Field embeddings

Definition 4.2. If $E, E'/F$ and $\varphi : E \to E'$ is an isomorphism, we sat that φ **fixes** F if $\varphi|_F = \mathrm{id}_F$. Elements $\alpha \in E$ and $\beta \in E'$, are **conjugate** over F if there exists an isomorphism $\varphi : F(\alpha) \to F(\beta)$ fixing F with $\varphi(\alpha) = \beta$.

Proposition 4.1. *Let $E, E'/F$. Elements $\alpha \in E$, $\beta \in E'$ are conjugate over F if and only if they have equal minimal polynomials in $F[x]$.*

Proof. Let α, β be conjugate over F. Then $\varphi(g(\alpha)) = g(\beta)$ for all $g \in F[x]$. Then α, β have the same minimal polynomial (α is a root of $g(x)$ iff β is a root of $g(x)$).

If α, β haeve the same minimal polynomial $f \in F[x]$, then $F[x]/(f) \cong F(\alpha)$ via $x \ mapsto \alpha$ and $F[x]/(f) \cong F(\beta)$ via $x \ mapsto \beta$. □

Example 4.2. The roots of $x^2 + 1$a re ± 1. There exists a field automorphism $\mathbb{C} \to \mathbb{C}$ $i \mapsto -i$ fixing $\mathbb{R}$, namely, complex conjugation.

Definition 4.3. A **field embedding** is a ring homomorphism of fields (necessarily injective). If $\varphi : F \to M$ is an embedding and E/F is an extension, then $\Phi : E \to M$ **extends** φ if $\Phi|_F = \varphi$.

Example 4.3. Let $\iota : \mathbb{Q} \to \mathbb{R}$ be the natural inclusion map. There are two field embeddings extending ι; these are $\mathbb{Q}(\sqrt{2} \to \mathbb{R}$ sending $\sqrt{2} \mapsto \sqrt{2}$. There are no extensions to $\mathbb{Q}(i) \to \mathbb{R}$.

Theorem 4.3. *Let E/F be an extension, and let $\alpha \in E$ be algebraic over F. Let $\varphi : F\ toM$ be an embedding, and let $\tilde{\varphi} : F[x] \to M[x]$ be the induced map. Let f be the minimal polynomial of α. Then the extensions $\Phi : F(\alpha) \to M$ of φ are in 1-1 correspondence with the roots of $\tilde{\varphi}(f)$ in M via $\Phi \mapsto \Phi(\alpha)$.*

Proof. If $\tilde{p}(f)$ has a root β in M, let ev_β be evaluation at β. Consider $e_\beta \circ \tilde{\varphi} : F[x] \to M$. Then $\ker(e_\beta \circ \tilde{\varphi}_{\supseteq}(f)$. Since we are working in a PID, this is equality. We get

$$\begin{tikzcd} F[x]/(f) \arrow[r] \arrow[d, "\cong"] & M \\ F(\alpha) \arrow[ur, "\Phi"] & \end{tikzcd}$$

where $\Phi(\alpha) = \beta$.

If $\Phi : F(\alpha) \to M$ extends φ, then write $f = \sum_{i=0}^n c_i x^i$, where $n = \deg(f)$. Then

$$\tilde{\varphi}(f)(\Phi(\alpha)) = \sum_{i=0}^n \varphi(c_i)\Phi(\alpha)^i = \Phi(\sum_{i=0}^n c_i \alpha^i) = \Phi(f(\alpha)) = 0. \qquad \square$$

Corollary 4.2. *Let E/F be finite, and let $\varphi : F \to M$ be a field embedding. The number of extensions of φ to $E \to M$ is $\leq [E : F]$.*

Proof. Induct on the degree. If $E = F(\alpha)$, then the number of roots of $\mathrm{irr}_F(\alpha)$ in M is $\leq [F(\alpha) : F]$. Then the number of extensions is $\leq [F(\alpha) : F]$ by the theorem. Consider extensions of these; the number for each is $\leq [E : f(\alpha)]$ by induction. So the number is $\leq [E : F]$. $\square$

Example 4.4. We can extend $\iota : \mathbb{Q} \to \mathbb{R}$ to $\varphi : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{R}$ in 4 ways. However, there is only one way to embed $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{R}$ because $x^3 - 2 = (x - \sqrt[3]{2}) \cdot (\deg(2))$ in $\mathbb{R}[x]$.

Proposition 4.2. *Let E/F be algebraic, and let $\sigma : E \to E$ be an embedding fixing F. Then σ is an isomorphism.*

Proof. For any $\beta \in E$, let f be its minimal polynomial. The restriction to the finite set of roots $\sigma : \{\text{roots of } f \text{ in } E\} \to \{\text{roots of } f \text{ in } E\}$ is a bijection (as it is injective). So $\beta \in \mathrm{im}(\sigma)$. $\square$

5 Algebraic Closure

5.1 Algebraically closed fields

Definition 5.1. A polynomial **splits** in $L[x]$ if it factors in $L[x]$ as a product of linear polynomials.

Definition 5.2. A field L is **algebraically closed** if every nonconstant polynomial in $L[x]$ has a root in L.

Proposition 5.1. *If $L[x]$ is algebraically closed, then every (nonconstant) poltnomial in $L[x]$ splits over L.*

Corollary 5.1. *If M is an algebraic extension of an algebraically closed field L, then $M = L$.*

Theorem 5.1 (fundamental theorem of algebra)**.** *$\mathbb{C}$ is algebraically closed.*

Here is a proof that uses no algebra.

Proof. Let $f \in \mathbb{C}[x]$ have no roots in $\mathbb{C}$. Then $1/f$ is holomorphic on $\mathbb{C}$. Moreover, $1/f$ is bounded. So $1/f$ is constant by Liouville's theorem. Thus, f is constant. $\square$

Theorem 5.2. *Let E/F be algebraic, and let $\varphi : F \to M$ be a field embedding with M algebraically closed. Then there exists a field embedding $\Phi : E \to M$ extending φ.*

Proof. Let $X = \{(K, \sigma) : E/K/F, \sigma : K \to M \text{ is an embedding extending } \varphi\}$. Then $(K, \sigma) \leq (K', \sigma')$ if $K \subseteq K'$ and $\sigma'|_K = \sigma$ defines a partial order on X. Let $|mcC$ be a chain in X. Then $L = \bigcup_{K \in \mathcal{C}} K$ with $\tau : L \to M$ defined as $\tau|_K = \sigma$ for each $K \in \mathcal{C}$ is an upper bound for $\mathcal{C}$. By Zorn's lemma, we have a maximal element (Ω, Φ).

We want to show that $\Omega = E$. Let $\alpha \in E$, and let $f \in \Omega[x]$ be its minimal polynomial $f(x) = \sum_{i=1}^n a_i x^i$, where $n = \deg(f)$. Define $g := \sum_{i=1}^n \Phi(a_i) x^i \in M[x]$. M is algebraically closed, so g has a root $\beta \in M$. So there exists $\tilde{\Phi} : \Omega(\alpha) \to M$ with $\tilde{\Phi}|_\Omega = \Phi$ and $\alpha \mapsto \beta$. Then $(\Omega(\alpha), \tilde{\Phi}) \geq (\Omega, \Phi)$. So $\alpha \in \Omega$, as (Ω, Φ) is maximal. $\square$

Proposition 5.2. *The set of all algebraic elements over F in an extension E/F is a subfield of E, the largest intermediate field that is algebraic over F.*

Proof. Let M be the set of algebraic elements over F in E. Let $\alpha, \beta \in M$. Then $F(\alpha, \beta)/F$ is finite, so it contains $\alpha - \beta$ and α/β if $\beta \neq 0$, and $F(\alpha, \beta) \subseteq M$. $\square$

Corollary 5.2. *The set $\overline{\mathbb{Q}}$ of algebraic numbers in $\mathbb{C}$ is a subfield of $\mathbb{C}$.*

5.2 Algebraic closure

Definition 5.3. An **algebraic closure** of a field F is an algebraic, algebraically closed extension of F.

Proposition 5.3. *Let $K/E/F$. Then K/F is algebraic if and only if K/E and E/F are algebraic.*

Proof. ($\Longleftarrow$): Take $\alpha \in K$, and let $f \in E[x]$ be its minimal polynomial, $f = \sum_{i=0}^{n} a_i x^i$, where $a_i \in E$. Each of these a_i is algebraic over F. Then $F(a_0, \dots, a_n)(\alpha)$ is finite over F, so every element in it is algebraic over F, so α is algebraic over F. $\square$

Proposition 5.4. *If F is a field and M/F is algebraically closed, then M contains a unique algebraic closure of F, the maximal subfield $\overline{F}$ of M which is algebraic over F.*

Proof. Suppose $f \in \overline{F}[x]$, and look at E/F, generated by the coefficients of f. E/F is finite. If $\alpha \in M$ is a foot of f, then $E(\alpha)/F$ is algebraic by the previous proposition, so α is algebraic over F. Then $\alpha \in \overline{F}$. $\square$

Corollary 5.3. *$\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.*

Example 5.1. $\overline{\mathbb{F}}_p := \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ is an algebraic closure of $\mathbb{F}_p$. This union makes sense because $\mathbb{F}_{p^k}, F_{p^\ell} \subseteq F_{p^m}$, where $m = \operatorname{lcm}(k, \ell)$.

Theorem 5.3. *Every field F has an algebraic closure.*

Proof. Let F be a field, $\Omega = \coprod_f R_f$, where f runs over monic irreducible polynomials in $F[x]$ and R_f is a finite set with one element for each root of f in a splitting field. Then $F \subseteq \Omega$ because a is the unique root of $x - a$. Let $X = \{E/F \text{ algebraic} : E \subseteq \Omega, \alpha \in E\}$. Such an $\alpha \in R_f$, where f is in the minimal polynomial of α. $X \neq \varnothing$, since $F \in X$.

Let $\mathcal{C}$ be a chain in X, and let $K = \bigcup_{E \in \mathcal{C}} E \subseteq \Omega$. Check yourself that $K \in X$. So $\mathcal{C}$ has an upper bound. By Zorn's lemma, we have a maximal element $\overline{F} \in X$. Since $\overline{F} \in X$, it is algebraic. We claim that $\overline{F}$ is algebraically closed. Let $f \in F[x]$ and $g \in \overline{F}[x]$ be monic and irreducible with $g \mid f$. $E = \overline{F}[x]/(g) \subseteq \Omega$ as follows: if $h \in F[x]$ is monic and irreducible with a root in E, then the distinct roots of h in $E \setminus \overline{F}$ inject into elements of $R_h \setminus \overline{F}$. By maximality, $E = \overline{F}$. So $\overline{F}$ is algebraically closed. $\square$

Proposition 5.5. *If M, M' are algebraic closures of F then there exists an isomorphism $\Phi : M \to M'$ fixing F.*

Proof. We have an embedding $F \to M'$. There exists a $\Phi : M \to M'$ extending this inclusion. It suffices to show that $\operatorname{im}(\Phi)$ is algebraically closed. If $\alpha \in M$ is a root of $f \in F[x]$, it maps to a root of $\Phi(\alpha)$ of f in $\Phi(M) \subseteq M'$. So $\Phi(M)$ is algebraically closed, and hence $\Phi(M) = M$. $\square$

6 Transcendental Extensions and Separability

6.1 Transcendental extensions

Definition 6.1. An extension K/F is **purely transcendental** if every $\alpha \in K \setminus F$ is transcendental over F.

Proposition 6.1. *$F((t_i)_{i\in I})$, where I is an indexing set, is purely transcendental over F.*

Proof. Here is the case of $F(t)/F$. Let $\alpha = f/g \in F(t) = F$, where $f, g \in F[t]$, and $g \neq 0$. Then $\alpha g(x) \notin F[x]$, but $\alpha g(x) \in F(t)[x]$. Then $\alpha g(x) \neq f(x) \in F[x]$. But $f(xx) - \alpha g(x)$ has a root t, so t is algebraic over $F(\alpha)$. But t is transcendental over F, so α must be transcendental over F. Thus, $F(t)/F$ is purely transcendental.

For the case of $F(t_1, \ldots, t_n)/F$, proceed by induction. For the general case, every element in $F((t_i)_{i\in I})$ is in $F(t_1, \ldots, t_n)$ for some $i_1, \ldots, i_n \in I$. If it is not in F, it is transcendental by the previous case. $\square$

Proposition 6.2. *Every field extension is a purely transcendental extension of an algebraic extension.*

Proof. Let K/F, and let E be the maximal algebraic extension of F in K. If $\alpha \in K$ is algebraic over E, it is algebraic over F, so $\alpha \in E$. So K/E is purely transcendental. $\square$

Example 6.1. Let F be a field, and let $\overline{F}$ be an algebraic closure. Then $\overline{F}(t)/\overline{F}$ is purely transcendental. We can do it the other way around, as well. $\overline{F}(t)/F(t)$ is algebraic, while $F(t)/F$ is purely transcendental.

Definition 6.2. A subset $S \subseteq K$ for K/F is **algebraically independent** over F if for all nonzero $f \in F[x_1, \ldots, x_n]$ and distinct $s_1, \ldots, s_n \in S$, $f(s_1, \ldots, s_n) \neq 0$.

Here are some lemmas about algebraically independent sets. The proofs are the same as the corresponding properties of linearly independent sets.

Lemma 6.1. *Let $S \subseteq K$ be algebraically independent over F. Then $t \in K$ is transcendental over $F(S)$, where $F(S)$ is the smallest subfield of K generated by S over F, if and only if $S \cup \{t\}$ is algebraically independent over F.*

Lemma 6.2. *$S \subseteq K$ is algebraically independent over F if and only if every $s \in S$ is transcendental over $F(S \setminus \{s\})$.*

Definition 6.3. A subset S of K is a **transcendence basis** for K/F if it is algebraically independent over F and if $K/F(S)$ is algebraic.

Example 6.2. Let $\overline{F}(t)/F$. $\{r\}$ is a transcendence basis, and in fact, $\{t^{1/n}\}$ is a trascendence basis for any n. However $\{t^{1/2}, t^{1/3}\}$ is not because it is not algebraically independent: $(t^{1/2})^2 = (t^{1/3})^3$.

The previous two lemmas imply the following lemma.

Lemma 6.3. *Let $S \subseteq K$. The following are equivalent:*

1. *S is a trascnece basis for K/F.*
2. *S is a maximal F-algebraically independent subset of K.*
3. *S is a minimal subset of K such that K is algebraic over $F(S)$.*

Proof. The first two statements are equivalent by the first lemma. The latter two statements are equivalent by the second. □

Theorem 6.1. *Every F-algebraiclly independent subset of K is contained in a transcendence basis, and every $S \subseteq K$ such that $K/F(s)$ is algebraic contains a trascendence basis.*

The proof is the same argument as the corresponding statement in linear algebra.

Corollary 6.1. *Every field extension has a transcendence basis. In particular, there exists an intermediate extension $K/E/F$ such that K/E is algebraic and E/F is purely transencental.*

Proof. Take $E = F(S)$, where S is a transcendence basis. □

Theorem 6.2. *Any two transcendence bases of K/F have the same cardinality.*

Again, the proof is the same as the corresponding proof in linear algebra.

Definition 6.4. The **transcendence degree** of K/F is the number of elements in a transcendence bases if finite. Otherwise, K/F has infinite transcendence degree.

6.2 Separability

Definition 6.5. Let $f \in F[x]$. The **multiplicity** of a root α of F in an algebraic closure of F is the highest power m such that $(x-\alpha)^m \mid f$ in $\overline{F}[x]$.

Example 6.3. The polynomial $x^p - t = (x - t^{1/p})^p$ in $\mathbb{F}_p(t^{1/p})[x]$. The multiplicity of $t^{1/p}$ is p.

Lemma 6.4. *The multiplicity of a root odes not depend on the choice of $\overline{F}$ and does not depend on the choice of root if f is irreducible.*

Corollary 6.2. *The number of distinct roots in $\overline{F}$ of an irredudcible polynomial $f \in F[x]$ divides* $\deg(f)$.

Proof. Write $f = \prod_{i=1}^{k}(x-\alpha_i)^m$. Then $km = \deg(f)$. □

Definition 6.6. We say that $f \in F[x]$ is **separable** if every root of f has multiplicity 1. An element $\alpha \in \overline{F}$ is **separable** if it is algebraic over F and its minimal polynomial over F is separable. An extension E/F is **separable** if every $\alpha \in E$ is separable over F.

Lemma 6.5. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F. Then α is separable over F if and only if $F(\alpha)/F$.*

Proof. If $F(\alpha)/F$ is separable, then $\alpha \in F(\alpha)$, so α is separable over F. Conversely, suppose α is separable over F, and let $\beta \in F(\alpha)$. The number of embeddings of $F9\beta \int \overline{F}$ fixing F is $\leq [F(\beta) : F]$. Equality holds iff β is separable over F.

The number of embeddings $F(\alpha) \to \overline{F}$ is $[F(\alpha) : F]$. On the other hand, α is separable over $F(\beta)$, so the number of embeddings $F(\alpha) \to \overline{F}$ extending the embedding $F(\beta) \to \overline{F}$ equals $[F(\alpha) : F(\beta)]$. So the number of embeddings $F(\alpha) \to \overline{F}$ over F is the product of the number of embeddings $F(\beta) \to \overline{F}$ with the number of extensions of these embeddings to $F(\alpha) \to \overline{F}$. So the number of embeddings $F(\beta) \to \overline{F}$ fixing F is

$$\frac{[F(\alpha) : F]}{[F(\alpha) : F(\beta)]} = [F(\beta) : F]. \qquad \square$$

7 Inseparability and Perfect Fields

7.1 Towers of separable extensions

Proposition 7.1. *Let E/F be finite, and let $\mathrm{Emb}_F(E)$ be the set of embeddings $\Phi : E \to \overline{F}$ fixing F. Then $|\mathrm{Emb}_F(E)|$ divides $[E : F]$, with equality iff E/F is separable.*

Proof. Let $e = |\mathrm{Emb}_F(E)|$ and $E = F(\alpha_1, \ldots, \alpha_n)$. Let $E_i = F(\alpha_1, \ldots, \alpha_{i=1}$, and let e_i be the number of embeddings in $\mathrm{Emb}_F(E_{i+1})$ extending an embedding in $\mathrm{Emb}_F(E_i)$. We know that $e_i \mid [E_{i+1} : E_i]$ and we get equality iff E_{i+1}/E_i is separable. This is because this is the number of distinct conjugates of α_i over E_i times the multiplicity (number of conjugates times multiplicity is the degree of the polynomial). Now $e = \prod_{i=1}^{n} e_i$, so E/F is separable.

If $e = [E : F]$, take $\beta \in E$. The number of conjugates of $\beta \in \overline{F}$ is $d = |\mathrm{Emb}_F(F(\beta))|$, which divides $[F(\beta) : F]$. The number of extensions of any such embedding to $E \to \overline{F}$ divides $c = [E : F(\beta)]$. Now $cd = e = [E : F]$, so $d = [F(\beta) : F]$, since d divides it and $c \mid [E : F(\beta)]$. Then $F(\beta)/F$ is separable. □

Proposition 7.2. *If $K/E/F$ are salgebraic, and K/E and K/F is separable, then K/F is separable.*

Proof. In the case of finite degree, this follows from the previous proposition. In general, any $\alpha \in K$ has minimal polynomial over E which has coefficients in a finite extension E'/F. So $E'(\alpha)/E'/F$ is finite, $E'(\alpha)/E'$ and E'/F are separable. So, by the finite case, α is separable over F. This is true for all $\alpha \in K$, so K/F is separable. □

7.2 Purely inseparable extensions and degrees of separability and inseparability

Definition 7.1. An extension E/F is **purely inseparable** if every $\alpha \in E \setminus F$ is inseparable. Equivalently, E/F is separable it has no nontrivial intermediate separable extensions over F.

Example 7.1. $\mathbb{F}_p(x)/\mathbb{F}_p(x^p)$ is purely inseparable because it has degree p and because the minimal polynomial of x is $t^p - x^p = (t - x)^p$.

Corollary 7.1. *The set of all separable elements in an extension K/F (call it E) is a field, and K/E is purely inseparable.*

Definition 7.2. Suppose K/F is finite, and E is a maximal separable subextension. Then the **degree of separability** of K/F is $[K : F]_s = [E : F]$. The **degree of inseparability** if $[K : F]_i = [K : S]$.

Lemma 7.1. *Let E/F is algebraic, $f \in E[x]$ be monic, and $m \geq 1$ such that $f^m \in F[x]$. Then either $m = 0$ in F or $f \in F[x]$.*

Proof. Let $f = \sum_{i=0}^{n} a_i x^i$ be monic, and suppose that $f \notin F[x]$. Let $i \leq n-1$ be maximal such that $a_i \notin F$. Let c be the coefficient of $x^{(m-1)n+i}$ in f^m. This is not in F, since c is a sum of terms all in F (involving only a_j with $j > i$ and 1 term coming from $a_i a_n^{m-1} = a_i$). So $c - ma_i \in F$, which means $a_i \in F$ or $m = 0$ in F. But $a_i \notin F$. $\square$

Proposition 7.3. *Let* $\operatorname{char}(F) = p$. *If* E/F *is purely inseparable and* $\alpha \in E$, *then there exists a minimal* $k \geq 0$ *such that* $\alpha^{p^k} \in F$, *and the minimal polynomial of* α *is* $x^{p^k} - \alpha^{p^k}$.

Proof. Let $\alpha \in E \setminus F$ have minimal polynomial $f = \prod_{i=1}^{d}(x - \alpha_i)^m \in \overline{F}[x]$. Of $m > 1$, then $f = g^m$ where $g = \prod_{i=1}^{d}(x - \alpha_i)$. Then $m = p^k t$, where $p \nmid t$,and $k \geq 1$ by the lemma. Then $f = (g^{p^k})^t \in F[x]$. So the lemma forces $t = 1$ since $p \nmid t$. Letting $a_i = \alpha_i^{p^k}$, we get $f = \prod_{i=1}^{d}(x^{p^k} - a_i)$. Then $f = h(x^{p^k})$, where $h = \prod_{i=1}^{d}(x - a_i) \in F[x]$. This is a separable polynomial, so $F(a_i)/F$ is separable for each i. Since E/F is purely inseparable, each $a_i \in F$. Since F is irreducible, we get $d = 1$. So $f = x^{p^k} - \alpha_i^{p^k}$. $\square$

Corollary 7.2. *If* E/F *is finite and* $\operatorname{char}(F) = p$, *then* $[E/F]_i$ *is a power of* p.

Proposition 7.4. $[K : F]_s = |\operatorname{Emb}_F(K)|$.

Corollary 7.3. *Degrees of separability and inseparability are multiplicative in extensions.*

7.3 Perfect fields

Definition 7.3. A field is **perfect** if every algebraic extension of it is separable.

Example 7.2. $\mathbb{F}_p$ is perfect. Finite extensions are $\mathbb{F}_{p^n}$, which is generated by the roots of $x^{p^n} - x$, which has p^n distinct roots. So these extensions are separable.

Theorem 7.1. *Every field of characteristic 0 is perfect.*

Proof. Let $\operatorname{char}(F) = 0$. Then every irreducible monic polynomial is $f = \prod_{i=1}^{d}(x - \alpha_i)^m \in \overline{F}[x]$. Then $f = g^m$, where $g \in \overline{F}[x]$. So $g \in F[x]$ by the lemma. Since f is irreducible, $m = 1$. $\square$

7.4 The primitive element theorem

Definition 7.4. An extension E/F is **simple** if $E = F(\alpha)$ with $\alpha \in E$. Here, α is called a **primitive element** for E/F.

Theorem 7.2 (primitive element theorem)**.** *Every finite separable extension is simple.*

Proof. If $F = \mathbb{F}_q$, then $\mathbb{F}_{q^n}$, where $\mathbb{F}_q(\xi)$, where ξ is the primitive $(q^n - 1)$-th root of 1. Now we may assume that F is an infinite field. It suffices to show that any $F(\alpha, \beta)/F$ (with α, β algebraic) is simple. Look at $\gamma := \alpha + c\beta$ for $c \in F \setminus \{0\}$. Since F is infinite, we can choose $c \neq (\alpha' - \alpha)/(\beta' - \beta)$, where α' is a conjugate of α and same for β. Then $\gamma \neq \alpha' + c\beta'$ for all such α', β'. Let f be the minimal polynomial of α, and let $h(x) = f(\gamma - cx) \in F(\gamma)[x]$. Now $h(\beta) = f(\alpha) = 0$. Then h does not have any other β' as a root. We will finish this next time. $\square$

8 Normal Extensions, Galois Extensions, and Galois Groups

8.1 The primitive element theorem

Let's complete the proof from last time.

Theorem 8.1 (primitive element theorem)**.** *Every finite, separable extension is simple.*

Proof. If $F = \mathbb{F}_q$, then $\mathbb{F}_{q^n}$, where $\mathbb{F}_q(\xi)$, where ξ is the primitive $(q^n - 1)$-th root of 1. Now we may assume that F is an infinite field. It suffices to show that any $F(\alpha, \beta)/F$ (with α, β algebraic) is simple. Look at $\gamma := \alpha + c\beta$ for $c \in F \setminus \{0\}$. Since F is infinite, we can choose $c \neq (\alpha' - \alpha)/(\beta' - \beta)$, where α' is a conjugate of α and same for β. Then $\gamma \neq \alpha' + c\beta'$ for all such α', β'. Let f be the minimal polynomial of α, and let $h(x) = f(\gamma - cx) \in F(\gamma)[x]$. Now $h(\beta) = f(\alpha) = 0$, and $h \in F(\gamma)[x]$. But $h(\beta') = f(\gamma - c\beta) \neq 0$ for all β' conjugate (but not equal) to β. If $g \in F[x]$ is the minimal polynomial of β, then since it and h share just one root, β, in $F(\gamma)$, the minimal polynomial of β is $x - \beta$. Then $\beta \in F(\gamma)$, which gives $\alpha \in F(\gamma)$. So $F(\gamma) = F(\alpha, \beta)$. $\square$

Remark 8.1. Where does separability come into play during the proof? We used that g is separable to show that $g(x) \neq (x - \beta)^k$ for $k > 1$.

8.2 Normal extensions

Definition 8.1. An algebraic extension E/F is **normal** if it is the splitting field of some set of polynomials in $F[x]$.

Example 8.1. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal. The minimal polynomial of $\sqrt[4]{2}$, $x^4 - 2$, has roots not in $\mathbb{Q}(\sqrt[4]{2})$. However, the extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is normal.

Lemma 8.1. *If K/F is normal, then so is K/E for any intermediate E.*

Theorem 8.2. *An algebraic extension E/F is normal if and only if every embedding $\Phi : E \to \overline{F}$ (where $\overline{F} \subseteq E$) fixing F satisfies $\Phi(E) = E$.*

Proof. Let E/F be normal, and say it is the splitting field of $S \subseteq F[x]$. Suppose $\Phi : E \to \overline{F}$ is an embedding fixing F. Let $\alpha \in E$. Then $\Phi(\alpha) = \beta$, where β is conjugate to α over F. So $\beta \in E$, so $\Phi(E) \subseteq E$. Then $\Phi(E) = E$.

Suppose that $\Phi(E) = E$ for all Φ, and let $\alpha \in E$ have minimal polynomial f. Given $\beta \in \overline{F}$ that is a root of f, there exists Φ such that $\Phi(\alpha) = \beta$. Therefore, $\beta \in E$. So in particular, E is the splitting field of all minimal polynomials in $F[x]$ with a root in E. $\square$

Corollary 8.1. *IF E/F is normal and $f \in F[x]$ has a root in E, then f splits in E.*

Proposition 8.1. *If $E, K \subseteq \overline{F}$ are normal over F, then so is the compositum EK.*

Proof. E is the splitting field of S. K is the splitting field of T. Then EK is the splitting field of $S \cup T$. $\square$

Here is an alternative proof.

Proof. If $\varphi \in \mathrm{Emb}_F(EK)$, then since $\varphi(E) = E$ and $\varphi(K) = K$, $\varphi(EK) = EK$. $\square$

8.3 Galois groups and extensions

Definition 8.2. The **Galois group** $\mathrm{Gal}(E/F)$ of a normal extension E/F is the group of field automorphisms $E \to E$ fixing F.

Sometimes, we may write $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E) \subseteq \mathrm{Aut}(E)$.

Remark 8.2. $|\mathrm{Gal}(E/F)| = [E : F]_s$. This equals the degree when E/F is separable.

Definition 8.3. An extensions E/F is **Galois** if it is normal and separable.

Remark 8.3. If E/F is finite, then E/F is Galois iff it is normal and $|\mathrm{Gal}(E/F)| = [E : F]$.

Example 8.2. Last time, we showed that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is separable. $\mathbb{F}_{q^n}$ is the splitting field of $x^{q^n} - x$, which is separable, so $\mathbb{F}_{q^n}$ is Galois. The **Frobenius element** $\varphi_q \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is defined by $\varphi_q(\alpha) = \alpha^q$. This is a field homomorphism; it is an additive homomorphism because we are in characteristic q. What are the other elements of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$?

Proposition 8.2. $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \varphi_q \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. The automorphism $\varphi_q^k(\alpha) = \alpha^{q^k}$ fixes $\mathbb{F}_{q^n}$ iff $n \mid k$. So its order is n. The Galois group has order n, so this must be a cyclic group. $\square$

Example 8.3. $\mathbb{F}_p(t^{1/p})/\mathbb{F}_q(t)$ is purely inseparable. If $\sigma \in \mathrm{Aut}_{\mathbb{F}_q(t)}(\mathbb{F}_q(t^{1/p}))$, then $\sigma(t) = t$. So $\sigma(t^{1/p})^p = \sigma(t) = t$. Then $\sigma(t^{1/p}) = t^{1/p}$. That is, $\mathrm{Aut}_{\mathbb{F}_q(t)}(\mathbb{F}_q(t^{1/p}))$ is trivial.

Example 8.4. Recall that the cyclotomic polynomial Φ_n is irreducible. Then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Let K be a field of characteristic $\nmid n$. Define the n-th **cyclotomic character** $\chi_n : \mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ sending $\sigma \mapsto a \pmod{n}$, where $\sigma(\zeta_n) = \zeta_n^a$. We can also say it like this: $\sigma(\zeta_n) = \zeta_n^{\chi_n(\sigma)}$. This is a homomorphism because

$$\zeta_n^{\chi_n(\sigma\tau)} = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{\chi_n(\tau)}) = \sigma(\zeta_n)^{\chi_n(\tau)} = \zeta_n^{\chi_n(\sigma)\chi_n(\tau)}.$$

This is injective because χ_n is determined on σ by what power σ raises ζ_n to.

Proposition 8.3. *The map* $\chi_n : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ *is an isomorphism.*

Proof. The Galois group has order $\varphi(n)$, the same as the order of $(\mathbb{Z}/n\mathbb{Z})^\times$. We already showed that χ_n is injective. $\square$

8.4 Fixed fields

Definition 8.4. The **fixed field** of a field E by a subgroup G of $\mathrm{Aut}(E)$ is the field $E^G = \{\alpha \in E : \sigma \cdot \alpha = \alpha \, \forall \sigma \in G\}$.

Proposition 8.4. *If if K/F is Galois, then $K^{\mathrm{Gal}(K/F)} = F$.*

Proof. ($\supseteq$): F is fixed by every $\sigma \in \mathrm{Gal}(K/F)$.

($\subseteq$): If $\alpha \in K^{\mathrm{Gal}(K/F)}$, then for all $\sigma \in \mathrm{Gal}(K/F)$, $\sigma \cdot \alpha = \alpha$. But this means that α is the only root of its minimal polynomial in K by normality. Separability gives us that the minimal polynomial is $x - \alpha$. Therefore, $\alpha \in F$. □

Let K/F is finite and Galois, let E be intermediate, and let $\sigma \in \mathrm{Gal}(K/F)$. We can consider the restriction $\sigma|_E : E \to \sigma(E)$. If E is normal over F, then this gives a map $\mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$.

Lemma 8.2. *Let K/F be Galois and E be intermediate. The restriction map res_E : $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \to \mathrm{Emb}_F(E)$ is a bijection. If E/F is Galois, then this is an isomorphism of groups.*

Proof is left as an exercise.[1]

[1] Why, Professor Sharifi? Why?

9 The Fundamental Theorem of Galois Theory

9.1 Restriction of automorphisms and the Galois group over a fixed field

Here, assume all extensions K/F will lie in $\overline{F}$.

Proposition 9.1. *If K/F is Galois and E is intermediate, then there exits a bijection of left $\operatorname{Gal}(K/F)$-sets $\operatorname{res}_F : \operatorname{Gal}(K/F)/\operatorname{Gal}(K/E) \to \operatorname{Emb}_F(E)$ sending $\sigma \operatorname{Gal}(K/E) \mapsto \sigma|_E$. Moreover, E/F is Galois if and only if $\operatorname{Gal}(K/E)$ is normal in $\operatorname{Gal}(K/F)$, in which case res_F is an isomorphism of groups.*

Proof. If $\sigma \in \operatorname{Gal}(K/F)$ and $\tau \in \operatorname{Gal}(K/F)$, then

$$\begin{aligned} \sigma\tau|_E = \sigma|_E &\iff \sigma_\tau(\alpha) = \sigma(\alpha)\ \forall \alpha \in E \\ &\iff \tau(\alpha) = \alpha\ \forall \alpha \in E \\ &\iff \tau \in \operatorname{Gal}(K/E). \end{aligned}$$

To show that this is onto, every $\varphi \in \operatorname{Emb}_F(E)$ lifts to $\sigma : K \to \overline{F}$, but this takes values in K since K/F is normal. So $\sigma \in \operatorname{Gal}(K/F)$. If $|rho \in \operatorname{Gal}(K/F)$, then

$$\operatorname{res}_F(\rho\sigma \operatorname{Gal}(K/E)) = \rho\sigma|_E = \rho \circ \sigma|_E = \rho \circ \operatorname{res}_F(\sigma \operatorname{Gal}(K/E)).$$

If E/F is Galois, then $\operatorname{Gal}(K/F) \to \operatorname{Gal}(E/F)$ sending $\sigma \mapsto \sigma|_E$ has kernel $\operatorname{Gal}(K/E)$, so it is normal.

Conversely, if $\operatorname{Gal}(K/E) \trianglelefteq \operatorname{Gal}(K/F)$, take $\varphi \in \operatorname{Emb}_F(E)$, and $\sigma \in \operatorname{Gal}(K/F)$ lifting φ. Then for all $\tau \in \operatorname{Gal}(K/E)$, $\sigma^{-1}\tau\sigma|_E = 1$. By normality, $\tau\sigma|E = \sigma|_E$. So $\sigma(E)$ is fixed by τ. So $\sigma(E) \subseteq E$, the fixed field of τ. So $\sigma(E) = E$, so E/F is Galois. □

Proposition 9.2. *Let K/F be finite and Galois, and let $H \leq \operatorname{Gal}(K/F)$. Then the Galois group $\operatorname{Gal}(K/K^H) = H$.*

Proof. H fixes K^H, so $H \leq \operatorname{Gal}(K/K^H)$. K/K^H is separable, so by the primitive element theorem, there exists $\theta \in K$ such that $K = K^H(\theta)$. Then $f = \prod_{\sigma \in H}(x - \sigma(\theta)) \in K^H[x]$. The minimal polynomial of θ over K^H divides f, so $[K : K^H] \leq \deg(f) = |H|$. This forces $H = \operatorname{Gal}(K/K^H)$. □

9.2 The Galois correspondence

Theorem 9.1 (Fundamental theorem of Galois theory)**.** *Let K/F be finite, Galois. There are inclusion-reversing inverse bijections $\psi : \{E : K/E/F\} \to \{H : H \leq \operatorname{Gal}(K/F)\}$ and $\theta : \{H : H \leq \operatorname{Gal}(K/F)\} \to \{E : K/E/F\}$ such that $\psi(E) = \operatorname{Gal}(K/E)$, and $\theta(H) = K^H$. For such E/H, $[K : E] = |\operatorname{Gal}(K/E)|$, and $|H| = [K : K^H]$. These restrict to bijections between normal extensions of K and normal subgroups of $\operatorname{Gal}(K/F)$. If E/F is normal, we have the bijection $\operatorname{Gal}(K/F)/\operatorname{Gal}(K/E) \to \operatorname{Emb}_F(E)$, sending $\sigma \operatorname{Gal}(K/E) \mapsto \sigma|_E$.*

Proof. We have proved almost all the statements. We verify

$$\psi(\theta(H)) = \psi(K^H) = \mathrm{Gal}(K/K^H) = H,$$

$$\theta(\psi(E)) = \theta(\mathrm{Gal}(K/E)) = K^{\mathrm{Gal}(K/E)} = E. \qquad \square$$

Example 9.1. The splitting field of $x^4 - 2$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt[4]{2}, i)$. The polynomial $x^4 - 2$ is irreducible over $\mathbb{Q}(i)$. There exists $\tau \in \mathrm{Gal}(K/\mathbb{Q}(i)) \cong \mathbb{Z}/4\mathbb{Z}$ with $\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$; this generates $\mathrm{Gal}(K/\mathbb{Q}(i))$. The $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[4]{2})) \ni \sigma$ such that $\sigma(i) = -i$ and $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$. We can check that $\sigma\tau\sigma^{-1}(\sqrt[4]{2}) = -i\sqrt[4]{2} = \tau^{-1}(\sqrt[4]{2})$. So $\sigma\tau\sigma^{-1} = \tau^{-1}$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_4$.

Here is a diagram of some of the intermediate fields.

$$\begin{tikzcd}
 & \mathbb{Q}(i,\sqrt[4]{2}) \arrow[dl, dash, "4"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(i) \arrow[ddr, dash, "2"'] & \mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash, "2"] & \mathbb{Q}(i\sqrt[4]{2}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Proposition 9.3. *Let K be finite and Galois over F, and let E/F be algebraic. Then the map* $\mathrm{res}_K : \mathrm{Gal}(EK/E) \to \mathrm{Gal}(K/K \cap E)$ *sending* $\sigma \mapsto \sigma|_K$ *is an isomorphism.*

Proof. Let $\sigma \in \mathrm{Gal}(EK/E)$. Then σ fixes E, so $\sigma|_K$ fixes $K \cap E$. If $\sigma|_K = 1$, then σ dixes E and K, so σ fixes EK. So $\sigma = 1$. Then res_K is injective.

Let H be the image. Then $K^H = K^{\mathrm{Gal}(EK/E)} = K \cap E$. So $H = \mathrm{Gal}(K/K^H) = \mathrm{Gal}(K/K \cap E)$. So res_K is onto. $\square$

Proposition 9.4. *Let K/F be finite, Galois of degree n. Then* $\mathrm{Gal}(K/F)$ *embeds into* S_n.

Proof. By the primitive element theorem, $K = G(\theta)$, so $\mathrm{Gal}(K/F)$ permutes the roots of the conjugates of θ, a set with n elements. This action is faithful and transitive. $\square$

10 Profinite Groups and Infinite Galois Theory

10.1 Galois groups of infinite field extensions

Example 10.1. Consider $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. It maps to each $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, so $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. This is injective because an element of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is determined by what it does to $\mathbb{F}_{p^n}$ for all n. It is surjective because we can keep lifting elements in $\mathrm{Gal}(\mathbb{F}_{p^n}.\mathbb{F}_p)$.

This example had nothing to do with $\mathbb{F}_p$. In fact, for any Galois extension K/F,

$$\mathrm{Gal}(K/F) \cong \varprojlim_{\substack{E \subseteq K \\ E/F \text{ finite, Galois}}} \mathrm{Gal}(E/F).$$

Then

$$\varprojlim_n \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}},$$

the Prüfer ring. $\mathbb{Z} < \hat{\mathbb{Z}}$ says that $\langle \varphi_p \rangle < \mathrm{Gal}(\overline{\mathbb{F}}_p, \mathbb{F}_p)$. Then $\overline{\mathbb{F}}_p^{\langle \varphi_p \rangle} = \mathbb{F}_p$. So $\mathrm{Gal}(K, K^H)$ can be bigger than H.

Suppose we have an inverse system $(G_i, \phi_{i,j})$ of groups, where I is a directed set. That is, given $i, j \in I$, there exists some k such that $k \leq i$ or $k \leq j$, and $\phi_{i,j} : G_i \to G_j$. Recall that the inverse limit $\varprojlim_i G_i \subseteq \prod_{i \in I} G_i$ is $\varprojlim_i G_i = \{(g_i)_{i \in I} : \phi_{i,j}(g_i) = g_j \,\forall i, j\}$. Then the Galois group will be $G = \varprojlim_{i \in I} G_i$. If

$$\begin{tikzcd}
 & EE' \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & \\
E \arrow[dr, dash] & & E' \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

then $\mathrm{Gal}(EE'/F)$ surjects onto both $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(E'/F)$.

10.2 Topological and profinite groups

Definition 10.1. A **topological group** G is a group with a topology such that the multiplication map $G \times G \to G$ and inversion map $G \to G$ sending $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous.

Then $\prod_{i \in I}$ has the product topology, which is generated by the base

$$\prod_{j \in J} U_j \times \prod_{i \in I \setminus J} X_i,$$

where $U_j \subseteq X_j$ is open.

Then $G = \varprojlim_i G_i$ has the subspace topology induced from the product topology. G is a topological group with respect to this topology (exercise).

Definition 10.2. A **profinite group** is an inverse limit of finite groups $G = \varprojlim G_i$ endowed with the above topology, the **profinite topology** relative to $(G_i, \phi_{i,j})$

Example 10.2. Let $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. Then $\pi_n : \hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z}$ is continuous, and $n\hat{\mathbb{Z}} = \ker(\pi_n) = \pi_n^{-1}(\{0\})$ is open. Then $n\hat{\mathbb{Z}}$ is a base of open neighborhoods of 0. Then $\{a + n\hat{\mathbb{Z}}\}$ is a basis of open neighborhoods of $a \in \mathbb{Z}$. Since $\mathbb{Z}$ surjects onto $\mathbb{Z}/n\hat{\mathbb{Z}}$, we can find $a_n \in \mathbb{Z}$ such that $a_n \mapsto a + n\hat{\mathbb{Z}}$ for all n. So $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$; that is, its closure is $\hat{\mathbb{Z}}$.

Theorem 10.1. *A topological group G is profinite if and only if it is compact, Hausdorff, and totally disconnected (every connected component is a point).*

Let's assume the following fact from topology.

Proposition 10.1. *A compact, Hausdorff space is totally disconnected if and only if it has a base of clopen neighborhoods.*

We will prove one direction of the theorem.

Proof. Assume G is profinite. Products of compact, Hausdorff spaces are compact, Hausdorff. Closed subsets of Hausdorff spaces are compact, and subsets of Hausdorff spaces are Hausdorff. To show that G is closed, note that

$$G = \bigcap_{\phi_{i,j}} \{(g_i)_{i \in I} : \phi_{i,j}(g_i) = g_j\}.$$

Now let U_j be open for all $j \in J$ with J finite. Then

$$\begin{aligned}
\left(\prod_{j \in J} U_j \times \prod_{i \in I \setminus J} G_i \right)^c &= \left(\bigcap_{j \in J} \left(U_j \times \prod_{i \neq j} G_i \right) \right)^c \\
&= \bigcup_{j \in J} \left(U_j \times \prod_{i \neq j} G_i \right)^c \\
&= \bigcup_{j \in J} U_j^c \times \prod_{i \neq j} G_i.
\end{aligned}$$

So $\prod_i G_i$ is totally disconnected. So $G = \varprojlim G_i$ is totally disconnected. $\square$

Let $\pi_I : G \to G_i$. Then $\ker(\pi_i) = (\prod_{j \neq i} G_j) \times \{1\}$. Then $\prod_{i \in I \setminus J} G_i \times \prod_{j \in J} \{1\}$ is a basis of neighborhoods of 1. Then $\bigcap \varprojlim_i G_i = \bigcap_{j \in J} \ker(\pi_j)$ is an open subgroup of $\varprojlim G_i$ with finite index.

Proposition 10.2. *In profinite groups, subgroups are open if and only if they are closed and have finite index.*

Proof. ($\Longleftarrow$): If $H \leq G$ is closed of finite index, then $\{gH : gH \neq H\} \subseteq G/H$ is a finite set. Each gH is closed, so $\bigcup_{gH \neq H} gH = H^c$. So H is open. $\square$

Definition 10.3. The **Krull topology** on $\operatorname{Gal}(K/F)$ is the profinite topology for

$$\operatorname{Gal}(K/F) = \lim_{\substack{E \subseteq K \\ E/F \text{ finite}}} \operatorname{Gal}(E/F).$$

Definition 10.4. If G is a group, the **profinite completion** is

$$\hat{G} = \varprojlim_{\substack{N \trianglelefteq G \\ \text{finite index}}} N.$$

This gives a functor from the category of groups to the category of topological groups.

10.3 The fundamental theorem of Galois theory for infinite degree extensions

Theorem 10.2 (fundamental theorem of Galois theory)**.** *Let K/F be Galois. There are inverse, inclusion reversing correspondences $\{E : K/E/F\} \to \{H : H \leq \operatorname{Gal}(K/F), H \text{ closed}\}$ sending $E \mapsto \operatorname{Gal}(K/E)$ and $H \mapsto K^H$. Respective correspondences exist for finite or normal extensions to open or normal subgroups. If E/F is normal, then $\operatorname{Gal}(K/F)/\operatorname{Gal}(K/E) \cong \operatorname{Gal}(E/F)$, where this is a topological isomorphism.*

Example 10.3. The **absolute Galois group** of $\mathbb{Q}$ is $G_{\mathbb{Q}} = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Example 10.4. The absolute Galois group of $\mathbb{R}$ is $G_{\mathbb{R}} \cong \mathbb{Z}/2\mathbb{Z}$.

Example 10.5. The absolute Galois group of $\mathbb{F}_p$ is $\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p$,where $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$.

Theorem 10.3 (Kronecker-Weber)**.** *Let μ_n be a primitive n-th root of unity, and let $\mathbb{Q}^{ab} = \bigcup_n \mathbb{Q}(\mu_n)$. Then $G_{\mathbb{Q}^{ab}} = \operatorname{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$*

11 Tensor Products

11.1 Construction, universal property, and examples

Let A be a ring, let M be a right A-module, and let N be a left A-module.

Definition 11.1. The **tensor product** of M and N over A, denoted $M \otimes_A N$, is the quotient of $\mathbb{Z}^{M\times N} = \bigoplus_{(m,n)\in M\times N} \mathbb{Z}(m,n)$ by the $\mathbb{Z}$-submodule generated by

1. $(m+m',n) - (m,n) - (m',n)$
2. $(m,n'+n) - (m,n) - (m,n')$
3. $(ma,n) - (m,an)$

for all $m, m' \in M$, $n, n' \in N$, and $a \in A$. The image of (m,n) in $M \otimes_A N$ is denoted $m \otimes n$ and is called a **simple tensor**.

Example 11.1. How do simple tensors work? Let $k \in \mathbb{Z}$.

$$k(m\otimes n) = (m\otimes n) + \cdots + (m \otimes n) = (m + \cdots + m)\otimes = (km)\otimes n = m \otimes (kn).$$

Similarly,

$$(-1)(m\otimes n) = (-m)\otimes n.$$

$$0 \otimes n = 0 = m \otimes 0.$$

Proposition 11.1 (tensor product universal property)**.** *Let L be an abelian group and $\phi : M \times N \to L$ be such that*

1. *$\phi(m+m',n) = \phi(m,n) + \phi(m',n)$ (left biadditivity)*
2. *$\phi(m,n+n') = \phi(m,n) + \phi(m,n')$ (right biadditivity)*
3. *$\phi(ma,n) = \phi(m,an)$ (A-balanced).*

There exists a unique homomorphism $\Phi : M \otimes_A N \to L$ such that $\Phi(m\otimes n) = \phi(m,n)$ for all $m \in M$ and $n \in N$.

$$\begin{tikzcd} M \times N \arrow[r, "\phi"] \arrow[d] & L \\ M \otimes_A N \arrow[ur, dashed, "\Phi"'] & \end{tikzcd}$$

Proof. $M \otimes_A N = \mathbb{Z}^{M\times N}/I$ for the ideal generated by the relations. $\mathbb{Z}^{M\times N}$ is free over $\mathbb{Z}$, so there exists a unique $\varphi : \mathbb{Z}^{M\otimes N} \to L$ given by $\varphi((m,n)) = \phi(m,n)$. We get

$$\begin{tikzcd} \mathbb{Z}^{M\times N} \arrow[r] \arrow[d] & L \\ M \otimes_A N \arrow[ur, dashed, "\Phi"'] & \end{tikzcd}$$

whrer the map $\mathbb{Z}^{M\otimes N} \to M \otimes_A N$ is surjective. This uniquely determined Φ if it exists; i.e. $\Phi(I) = 0$. We can verify, for example, that

$$\varphi((m+m',n) - (m,n) - (m,n)) = \phi(m+m;,n) - \phi(m,n) - \phi(m',n) = 0. \qquad \square$$

Here is a special case. Let A be an R-algebra, where R is commutative. Let $\psi : R \to Z(A)$, the center of A. M is an R-A bimodule, where $rm = mr$. Recall that an A-B bimodule is a left A-module and a right B module such that $(am)b = a(mb)$ fir all $a \in A$, $m \in M$ and $b \in B$. We can define

$$r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn)$$

to give $M \otimes_A N$ an R-module structure. Another way to do this would be to deinfe $M \otimes_A N$ as $R^{M\times N}$, quotiented by the R-submodule generated by the same relations, plus the relation $r(m,n) - (rm,n)$.

What is the universal property saying?

$$\mathrm{Hom}_{R-\mathrm{mod}}(M \otimes_R N, L) \cong \mathrm{Hom}(M \times N, L),$$

where the right side is homomorphisms that are R-bilinear and A-balanced.

Example 11.2. Let K be a field. Then $K^m \otimes_K K^n$ is an mn-dimensional K vector space, generated by $e_i \otimes e_j$, where $\{e_i\}$ and $\{e_j\}$ form a basis for K^m and K^n, respectively:

$$K^m \otimes K^n = \left(\bigoplus_{i=1}^m K\right) \otimes K^n \cong \bigotimes_{i=1}^m (K \otimes K^n) \cong \bigoplus_{i=1}^m K^n \cong K^{mn}.$$

Example 11.3. $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(m,n)\mathbb{Z}$. We have the biadditive, $\mathbb{Z}$-balanced map $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/(m,n)\mathbb{Z}$ sending $(a,b) \mapsto ab$, so there exists a unique map $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/(m,n)\mathbb{Z}$ sending $a \otimes b \mapsto ab$. This is surjective. Let $a, b \in \mathbb{Z}$. Then $m(a \otimes b) = ma \otimes b = 0$, and $n(a \otimes b) = a \otimes nb = 0$. Also, $a \otimes b = ab(1 \otimes 1)$, which means that this group is cyclic by has order dividing m and dividing n. So the map is injective.

Example 11.4. $A \otimes_A N \cong N$ as let A-modules.

More generally, let A, B, C be rings, let A be an A-B bimodule, and let N be a B-C bimodule. Then $M \otimes_B N$ is an A-C bimodule.

$$a(m \otimes n) = (am) \otimes n, \qquad m \otimes (nc).$$

11.2 Properties of the tensor product

Proposition 11.2. *$M \otimes_A \cong N \otimes_{A^{op}} M$.*

Proof. We have the map $(m, n) \mapsto m \otimes n$ which is bilinear and A-balanced. It induces a unique map $M \otimes_A N \to N \otimes_{A^{\mathrm{op}}} M$. $\square$

Proposition 11.3. *Let L be a right A-module, let M be an A-B bimodule, and let N be a left B-module. Then $(L \otimes_A M) \otimes BN \cong L \otimes_A (M \otimes_B N)$.*

Proof. We can verify this using the universal property, as before. Alternatively, we can define the object $L \otimes_A M \otimes_B N$ as we defined the tensor product and show that $(L \otimes_A M) \otimes BN$ and $L \otimes_A (M \otimes_B N)$ are isomorphic to it. $\square$

Proposition 11.4. *$(\bigoplus_{i \in I} M_i) \otimes_A N \cong \bigoplus_{i \in I}(M_i \otimes AN)$.*

Proposition 11.5. *Let M be a left A-module, and let $I \subseteq A$ be a 2-sided ideal. Then $A/IA \otimes_A M \cong M/IM$ as A-modules.*

Proof. Define a map $\phi : A/IA \times M \to M/IM$ such that $\phi(\overline{a}, m) = am + IM$. This is well-defined because if $b \in I$, then $\phi(b, m) = bm + IM = 0$. This satisfies the properties we need, so there exists a homomorphism $\Phi : A/I \otimes_A M \to M/IM$ of A-modules. This homomorphism is surjective. We can define an inverse $M/IM \to A/IA \otimes_A M$ sending $m + IM \mapsto 1 \otimes m$; this is well-defined because for $b_i \in I$ and $m_i \in M$,

$$\sum b_i m_i \mapsto 1 \otimes \sum b_i m_i = \sum (1 \otimes b_i m_i) = \sum \underbrace{(b_i \otimes m_i)}_{=0} = 0.$$

Check that this is the inverse of Φ. $\square$

We can also take tensor products of R-algebras A and B to get and R-algebra $A \otimes_R B$, where $(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'$.

12 Tensor Products of Algebras and Homomorphism Groups

12.1 Tensor products of algebras

Let A, B, C be R-algebras, where R is a commutative ring. Let M and N be R-balanced A-B and B-C bimodules, respectively.

Definition 12.1. An **R-balanced** bimodule M is a module such that $rm = rm$ for all $r \in R, m \in M$.

This is equivalent to M being a $A \otimes_R B^{\text{op}}$-module. Then $M \otimes_B N$ becomes an R-balanced A-C bimodule:

$$a(m \otimes n) = am \otimes n, \qquad (m \otimes n)c = m \otimes nc.$$

We can also take tensor products of R-algebras, to get an R-algebra $A \otimes_R B$. We can define this by

$$(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'.$$

Proposition 12.1. *Multiplication is well-defined.*

Proof. We want to construct $A \times B \to \text{End}_R(A \otimes_R B)$ sending $(a, b) \mapsto \varphi_{a,b} = (a' \otimes b' \mapsto aa' \otimes bb')$. To show that $\varphi_{a,b}$ is well defined, we want a map $A \times B \to A \otimes_R B$ sending $(a', b') \mapsto aa' \otimes bb'$. By the universal property of the tensor product, we get a unique map $A \otimes_R B \to A \otimes_R B$, which we can set to be $\varphi_{a,b}$.

Now we want to show that our original map is bilinear. Check that

$$(ra_1 + a_2, b) \mapsto \varphi_{ra_1+a_2,b} = r\varphi_{a_1,b} + r\varphi_{a_2}.$$

By the universal property, we get a map $A \otimes_R B \to \text{End}_R(A \otimes_R B)$ sending $a \otimes b \mapsto (a' \otimes b' \mapsto aa' \otimes bb')$. So then we get a map $A \otimes_R \times A \otimes_R B \to A \otimes_R B$ sending $(a \otimes b, a; \otimes b') \mapsto aa' \otimes bb'$. So the operation is well-defined. □

Example 12.1. Let R be a commutative ring. Then $R[x] \otimes_R R[y] \cong R[x, y]$ by specifying $(x^i, y^j) \mapsto x^i y^j$ and extending this map to be bilinear. This map is surjective because we get every monomial in $R[x, y]$. Since $R[x, y]$ is free on the monomials $x^i y^j$, we can define an inverse map defined by $x^i y^j \mapsto x^i \otimes y^j$.

Example 12.2. Let G be a group. The **R-group ring** of G, $R[G]$, is the set of sums $\sum_{g \in G} a_g[g]$, where $a_g \in R$ and $a_g = 0$ for all but finitely many g. We can define multiplication on this by extending the multiplication on monomials defined by $[g] \cdot [h] = [gh]$.

12.2 Homomorphism groups

Example 12.3. Let M, N be R-modules. Then $\mathrm{Hom}_R(M, N)$ is an R-module: Let $\phi, \psi \in \mathrm{Hom}_R(M, N)$. Then we can define $(r\varphi)(m) := \varphi(rm) = r\varphi(m)$ and $(\varphi + \psi)(m) = \varphi(m) + \varphi(m)$. These are still R-module homomorphisms:

$$(r\varphi)(m)(sm) = \varphi(rsm) = \varphi(srm) = s\varphi(rm) = s(r\varphi)(m)$$

for $r, s \in R$.

Remark 12.1. If M, N are A-modules, then $\mathrm{Hom}_A(M, N)$ is an R-module but not an A-module.

Example 12.4. Let M be an R-balanced A-B bimodule, and let N be an R-balanced A-C bimodule. Then $\mathrm{Hom}_A(M, N)$ is a B-C bimodule by defining

$$(b\varphi)(m) := \varphi(mb), \qquad (\varphi c)(m) = \varphi(m)c.$$

Check that everything is balanced.

$\mathrm{Hom}_A(\cdot, \cdot) : A \otimes_R B^{\mathrm{op}}\text{-mod} \to B \times A \otimes_R B^{\mathrm{op}}\text{-mod} \to B \otimes_R C^{\mathrm{op}}\text{-mod}$ is a bifunctor.

$$\mathrm{Hom}_A(M \prod_{i \in I} N_i) \cong \prod_{i \in I} \mathrm{Hom}_A(M, N_i).$$

$$\mathrm{Hom}_A(\bigoplus_{i \in I} M_i, N) \cong \prod_{i \in I} \mathrm{Hom}_A(M_i, N).$$

Definition 12.2. If F is a field, and V is an F vector space, we can define the **dual vector space**, $V^* = \mathrm{Hom}_F(V, F)$.

12.3 Dual vector spaces

If we have a map $f : V \to W$, we get a map $f^* : W^* \to V^*$ defined by $f^*(\varphi)(v) = \varphi \circ f(v)$, so $V \mapsto V^*$ is a contravariant functor from F-vector spaces to F-vector spaces.

If V has basis $v_1, \dots, v_n$, then there is a **dual basis** $\varphi_1, \dots, \varphi_n$ of V^* given by

$$\varphi_i(v_j) = \delta_{i,j} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

So $V \cong V^*$ if V is finite dimensional. This is not the case if V is infinite-dimensional.

The functor $V \mapsto V^{**}$ covariant. We get $\Phi : V \to V^{**}$ given by $\Phi(v)(f) = f(v)$. Check that Φ is F-linear.

Proposition 12.2. *$\Phi : V \to V^{**}$ is injective.*

Proof. If $\Phi(v) = 0$, then $f(v) = 0$ for all $f \in V^*$; if $v \neq 0$, extend v to a basis B. Then there exists $f_v \in V^*$ such that $f_v(v) = 1$ and $f_v(w) = 0$ for all $w \in B$ with $w \neq v$. This is a contradiction. $\square$

However, Φ is not always an isomorphism. If $V = \bigoplus_{i\in I}$, then $V = \mathrm{Hom}(\bigoplus_{i\in I} F, F) = \prod_{i\in I} \mathrm{Hom}(F, F) = \prod_{i\in I} F$, which is bigger than V. So V^{**} will be even bigger.

Proposition 12.3. *If W is finite dimensional over F, then $\mathrm{Hom}_F(V, W) \cong V^* \otimes_F W$ via $f \otimes w \mapsto (v \mapsto f(v)w)$.*

Proof. $W = \bigotimes_{i=1}^n Fw_i$. Then

$$V^* \otimes_F \bigoplus_{i=1}^n F \cong \bigoplus_{i=1}^n V^* \otimes_F F \cong \bigoplus_{i=1}^n V^* \cong \bigoplus_{i=1}^n \mathrm{Hom}(V, F) \cong \mathrm{Hom}(V, \bigoplus_{i=1}^n F).$$

This isomorphism is precisely the map you get from composing these isomorphisms. $\square$

12.4 Adjointness of Hom and $\otimes$

Theorem 12.1. *Let A, B, C be R-algebras, and let M, N, L be R-balanced A-B, B-C, and A-C bimodules, respectively. Then $\mathrm{Hom}_A(M \otimes_B N, L) \cong \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, L))$ as right C-modules. Moreover, these are natural in M, N, L. In fact, we have $t_M : B \otimes_R C^{\mathrm{op}}$-mod $\to$ $A \otimes_R C^{\mathrm{op}}$-mod*

$$\begin{array}{ccc} N & \longrightarrow & M \otimes_R N \\ \big\downarrow{\scriptstyle \lambda} & & \big\downarrow{\scriptstyle \mathrm{id}_M \otimes_R \lambda} \\ N' & \longrightarrow & M \otimes_R N' \end{array}$$

and $h_M : A \otimes_R C^{op}$-mod $\to B \otimes_R C^{op}$-mod such that $\mathrm{Hom}_A(tM(N), L) \cong \mathrm{Hom}_B(N, h_M(L))$ is natural in N and L; i.e. t_M is left adjoint to h_M.

We will prove this next time.

13 Hom-$\otimes$ Adjunction, Tensor Powers, and Graded Algebras

13.1 Adjunction of Hom and $\otimes$

Theorem 13.1. *Let A, B, C be R-algebras, and let M, N, L be R-balanced A-B, B-C, and A-C bimodules, respectively. Then* $\mathrm{Hom}_A(M \otimes_B N, L) \cong \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, L))$ *as right C-modules. Moreover, these are natural in M, N, L. In fact, we have* $t_M : B \otimes_R C^{\mathrm{op}}\text{-mod} \to A \otimes_R C^{\mathrm{op}}\text{-mod}$

$$\begin{array}{ccc} N & \longrightarrow & M \otimes_R N \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \mathrm{id}_M \otimes_R \lambda} \\ N' & \longrightarrow & M \otimes_R N' \end{array}$$

and $h_M : A \otimes_R C^{op}\text{-mod} \to B \otimes_R C^{op}\text{-mod}$ *such that* $\mathrm{Hom}_A(tM(N), L) \cong \mathrm{Hom}_B(N, h_M(L))$ *is natural in N and L; i.e. t_M is left adjoint to h_M.*

Remark 13.1. This is the most general version, but you can safely forget C to get a more readable version of this theorem.

Proof. Let

$$\varphi \mapsto (n \mapsto \underbrace{(m \mapsto \varphi(m \otimes n))}_{\psi_n}).$$

This is a homomorphism of abelian groups. Define $\psi_n : M \to L$ be $\psi_n(m) = m \otimes n$. Then

$$\psi_n(am) = \psi_n((am) \otimes n) = a\psi(m \otimes n) = a\psi_n(m),$$

so $\psi_n \in \mathrm{Hom}_A(M, L)$. Now look at $n \mapsto \psi_n$. Then

$$(b\psi_n)(m) = \psi_n(mb) = mb \otimes n = m \otimes bn = \psi_{bn}(m),$$

so $(n \mapsto \psi_n) \in \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, L))$. Showing that our map is a map of C^{op}-mods is left as an exercise.

Let's find an inverse. Take $\theta \in \mathrm{Hom}_B(N, \mathrm{Hom}(M, L))$, and send

$$\theta \mapsto (m \otimes n \mapsto \theta(n)(m)).$$

Then

$$a(m \otimes n = am \otimes n \mapsto \theta(n)(am) = a\theta(n)(m),$$

so this is a map of A-modules. Also, $(m, n) \mapsto \theta(n)(m)$ gives a map $M \times N \to L$ that is left A-linear, B-balanced, and right C-linear (check this). So $M \otimes_B N \to L$ is a map of $A \otimes_R C^{\mathrm{op}}$-mods. To show that these are inverse maps, let $\varphi \mapsto \theta$, where $\theta(n)(m) = \varphi(m \otimes n)$. Then

$$\theta \mapsto \underbrace{(m \otimes n \mapsto \theta(n)(m) = \varphi(m \otimes n))}_{\varphi}.$$

Check that the other composition works out. $\square$

13.2 Tensor powers and graded algebras

Let M be an R-module, where R is a commutative ring.

Definition 13.1. The k-th **tensor power** of M over R is $M^{\otimes k} = M \otimes_R M \otimes_R \cdots \otimes_R M$.

This satisfies the universal property for multilinear maps:

$$\begin{tikzcd} M \times M \times \cdots \times M \arrow[r] \arrow[d] & L \\ M \otimes_R M \otimes_R \cdots \otimes_R M \arrow[ur, dashed] & \end{tikzcd}$$

Definition 13.2. A **graded ring** $A = \bigoplus_{i=0}^{\infty} A_i$ is ring consisting of a sequence of abelian groups A_i such that

1. The restriction of $+ : A \times A \to A$ to $A_i \times A_i$ is the operation on A_i
2. The restriction of $\cdot : A \times A \to A$ to $A_i \times A_j$ lands in A_{i+j} (so A_0 is a ring).

Here, $\mathrm{gr}^k(A) := A_k$ is called the k-th **graded piece**.

To check that the direct sum of abelian groups together with these maps forms a graded ring, we need these to be the same:

$$(A_i \times A_j) \times A_k \to A_{i+j} \times A_k \to A_{i+k+k},$$
$$A_i \times (A_j \times A_k) \to A_i \times A_{j+k} \to A_{i+j+k}.$$

Definition 13.3. A **graded R-algebra** is a graded ring with the A_i R-algebras, with a map $R \to Z(A_0)$ such that $R \times A_i \to A_i$ and $A_i \times R \to A_i$ are the same, and such that $A_i \times A_j \to A_{i+j}$ is R-bilinear.

Define

$$T(M) = \bigoplus_{k=0}^{\infty} M^{\otimes k},$$

where we have the map $M^{\otimes k} \times M^{\otimes \ell} \to M^{\otimes (k+\ell)}$ given by

$$(m_1 \otimes \cdots \otimes m_k) \cdot (m_1' \otimes \cdots \otimes m_\ell') = m_1 \otimes \cdots m_k \otimes m_1' \otimes \cdots \otimes m_\ell'.$$

Then this is a graded R-algebra.

Example 13.1. Let R be a commutative ring. Then

$$T(R) = \bigoplus_{k=0}^{\infty} R \cong R[x],$$

where the k-th graded piece has basis element $1 \mapsto x^k$.

Example 13.2. Let R be a commutative ring. What is $T(R^{\oplus n}) = T(Rx_1 \oplus \cdots \oplus Rx_n)$? The k-th graded piece is generated by $x_{i_1} \otimes \cdots \otimes x_{i_k}$. However, this is not $R[x_1, \ldots, x_n]$. Notice that $x_i \otimes x_j \neq x_j \otimes x_i$, so $R^{\oplus n} \otimes_R R^{\oplus n} = R^{\oplus n^2}$. So

$$T(R^{\oplus n}) = R\langle x_1, \ldots, x_n \rangle,$$

the noncommutative polynomial ring in n variables over R.

What is the universal property of T? If $\varphi : M \to A$ is a map of A modules, where A is an R-algebra, then there exists a unique $T(\varphi) : T(M) \to A$ such that

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d] & L \\ T(M) \arrow[ur, dashed, "T(\varphi)"'] & \end{tikzcd}$$

because $T(\varphi)(m_1 \otimes \cdots \otimes m_k) = \varphi(m_1) \otimes \cdots \otimes \varphi(m_j)$ determines $T(\varphi)$.

Let $I = \{m \otimes n - n \otimes m : m, n \in M\}$. Then

$$I = \bigoplus_{k=0}^{\infty} \operatorname{gr}^k(I),$$

where $\operatorname{gr}^k(I) := I \cap \operatorname{gr}^k(T(M))$. Then I is a **graded ideal**. If A is a graded R-algebra and I is a graded ideal of A, then

$$A/I \cong \bigoplus_{k=0}^{\infty} \operatorname{gr}^k(A)/\operatorname{gr}^k(I)$$

is a graded ring.

Definition 13.4. The **symmetric algebra** is $S(M) = T(M)/I$.

In the quotient,

$$m_1 \otimes m_2 \otimes m_3 = m_3 \otimes m_1 \otimes m_2 = m_1 \otimes m_3 \otimes m_2 = \cdots.$$

Example 13.3. $S(R^{\oplus n}) = R[x_1, \ldots, x_n]$.

14 Symmetric Powers, Exterior Powers, and Determinants

14.1 Symmetric algebras and powers

Let A be a graded R-algebra.

Definition 14.1. A **homogeneous** ideal I of A is an ideal such that $I = \bigoplus_{k=0}^{\infty} \mathrm{gr}^k(I)$, where $\mathrm{gr}^k(I) = I \cap \mathrm{gr}^k(A)$.

Lemma 14.1. *An ideal is homogeneous if and only if it has a set of generators, each of which lies in some* $\mathrm{gr}^k(A)$*.*

Example 14.1. Let $I = (x^3 - y^2) \subseteq A = R[x, y]$, which is graded by degree. This is not homogeneous, so A/I is not graded.

Let M be an R-module.

Definition 14.2. The **tensor module** is $T(m) = \bigoplus_{k=0}^{\infty} M^{\otimes k}$.

Definition 14.3. The **symmetric algebra** is $S(M) = T(M)/I$, where I is the ideal generated by $m \otimes n - n \otimes m$ for all $m, n \in M$. We call the graded pieces $\mathrm{Symm}^k(M) = \mathrm{gr}^k(S(M))$.

Example 14.2. $S(R^{\oplus n}) = R[x_1, \dots, x_n]$, and $\mathrm{Symm}^k(R^{\oplus n})$ is the set of homogenerous polynomials of degree k in $x_1, \dots, x_n$.

$\mathrm{Symm}^k(M)$ satisfies a universal property.

Proposition 14.1. *For any $\psi : M^k \to L$ which is R-multilinear and symmetric in its variables, there is a unique Ψ such that*

$$\begin{tikzcd} M \times \cdots \times M \arrow[r, "\psi"] \arrow[d] & L \\ \mathrm{Symm}^k(M) \arrow[ur, "\Psi"'] & \end{tikzcd}$$

If $f : M \to N$ is a morphism of R-modules, then $\mathrm{Symm}^k(f) : \mathrm{Symm}^k(M) \to \mathrm{Symm}^k(N)$ sends $m_1 \otimes \cdots \otimes m_k \mapsto \psi(m_1) \otimes \cdots \otimes \psi(m_k)$.

14.2 Exterior algebras and powers

To get antisymmetric instead of symmetric we could try the ideal generated by the $m \otimes n + n \otimes m$. If $n = m$, we get that $2m \otimes m$ is in the ideal, but $m \otimes m$ is not necessarily in the ideal. But we want $\psi(m, m, m, \dots) = 0$. Instead take,

$$J = (\{m \otimes m : m \in M\}).$$

Then

$$J \ni (m+n)\otimes(m+n) - m\otimes m - n\otimes n = m\otimes n + n\otimes m,$$

so we get all the relations we want.

Definition 14.4. The **exterior algebra** on an R-module M is $\bigwedge(M) = T(M)/J = \bigoplus_{k=0}^{\infty}\bigwedge^k(M)$. $\bigwedge^k(M)$ is called the **k-th extenior product** of M.

The k-th exterior product of M is universal for R-bilinear, alternating mpas in k-variables: $\psi(\dots,m,m,\dots)=0$ for all m. We write the elements as

$$m\wedge\cdots\wedge m_k \in \bigwedge^k(M).$$

Here are some properties:

1. $m_1\wedge m_2\wedge m_3 = -m_1\wedge m_3\wedge m_2 = m_3\wedge m_1\wedge m_2 = \cdots$
2. $\cdots\wedge m\wedge m\wedge\cdots = 0$

A generalization of the first property is the following,

Lemma 14.2. *$m_{\sigma(1)}\wedge\cdots\wedge m_{\sigma(k)} = (\operatorname{sign}(\sigma))m_1\wedge\cdots\wedge m_k$.*

$\bigwedge^k(R^{\oplus n})$ is spanned by $e_{i_1}\wedge\cdots\wedge e_{i_k}$, where $2_1,\dots,e_n$ is the standard basis of $R^{\oplus n}$, and $i_1,\dots,i_k\in\{1,\dots,n\}$. In fact, this is spanned by $e_{i_1}\wedge\cdots\wedge e_{i_k}$, where $i_1,\dots,i_k$ are distinct, or equivalently, $i_1<\cdots<i_k$.

Theorem 14.1. *$\bigwedge^k(R^{\oplus n})$ is free on the generators $e_{i_1}\wedge\cdots\wedge e_{i_k}$ with $1\le i_1<\cdots<i_k\le n$. In particular,*

$$\dim\left(\bigwedge^k(R^{\oplus n})\right) = \begin{cases}\binom{n}{k} & k\le n\\ 0 & k>n.\end{cases}$$

Proof. Let $M=R^{\oplus n}$. Fix $i_1<\cdots i_k$. It suffices to show the there exists some $\Phi:\bigwedge^k M\to R$ such that

$$\Psi(e_{i_1}\wedge\cdots\wedge e_{i_k})=1, \qquad \Psi(e_{j_1}\wedge\cdots\wedge e_{j_k})=0$$

if $j_1<\cdots<j_k$ and $(i_1,\dots,i_k)\neq(j_1,\dots,j_k)$. We want a map $\psi: M\times\cdots\times M\to R$. Send

$$\psi(e_{j_1},\dots,e_{j_k}) = \begin{cases}\operatorname{sign}(\sigma) & i_{\sigma(t)}=j_t\ \forall t\\ 0 & \{i_1,\dots,i_k\}\neq\{j_1,\dots,j_k\}\\ 0 & j_1,\dots,j_k \text{ not distinct}\end{cases}$$

If it is alternating on a basis, it is alternating (exercise), so this is well-defined. Then we get a dual basis of the correct size. ∎

14.3 Determinants

Say M is free with basis $e_1, \ldots, e_n$, and $T : M \to M$ is R-linear. This induces $\bigwedge^n(T) : \bigwedge^n(M) \to \bigwedge^n(M)$; this is a map $R \to R$, and it sends $e_1 \wedge \cdots \wedge e_n \mapsto 1$. This is multiplication by some element of R, which we call $\det(T)$. It satisfies $Te_1 \wedge \cdots \wedge Te_n = \det(T) e_1 \wedge \cdots \wedge e_n$.

Definition 14.5. $\det(T)$ is called the **determinant** of T.

Lemma 14.3. $Tv_1 \wedge \cdots \wedge Tv_n = \det(T) v_1 \wedge \cdots \wedge v_n$.

Proof. Expand each v_i as a linear combination of the $e_1 \wedge \cdots \wedge e_n$. Then the statement applies to each $Te_1 \wedge \cdots \wedge Te_n$, and we can do the steps in reverse. □

Proposition 14.2. *Let* $T, U : M \to M$. *Then* $\det(T \circ U) = \det(T)\det(U)$.

Proof.

$$\begin{aligned} \det(TU) e_1 \wedge \cdots \wedge e_n &= TUe_1 \wedge \cdots \wedge TUe_n \\ &= \det(T) Ue_1 \wedge \cdots \wedge Ue_n \\ &= \det(T)\det(U) e_1 \wedge \cdots \wedge e_n. \end{aligned}$$

□

Corollary 14.1. *If* $T : M \to M$ *is an isomorphism,* $\det(T) \in R^\times$.

Proof. $\det(T)\det(T)^{-1} = 1$ by the proposition. □

15 Properties of Determinants and Change of Basis

15.1 Formulas for determinants and effect of elementary matrices

We have an isomorphism $M_n(R) \cong \mathrm{End}_R(R^{\oplus n})$ sending a matrix A to the associated linear transformation T. We say $\det(A) := \det(T)$.

Theorem 15.1. $\det(A) = \sum_{\sigma \in S_n} (\mathrm{sign}(\sigma)) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$.

Proof. Let $v_j \in R^{\oplus n}$ be the j-th column vector of A. Then $T(e_j) = v_j$ for all j. Then

$$v_1 \wedge \cdots \wedge v_n = (\det A) e_1 \wedge \cdots \wedge e_n.$$

On the other hand,

$$v_1 \wedge \cdots \wedge v_n = \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} a_{i_1,1} a_{i_2,2} \cdots a_{i_n,n} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_n$$

In this sum the term will be zero unless all of the i_j are distinct. These also correspond to $\sigma \in S_n$ such that $\sigma(j) = i_j$.

$$\begin{aligned}
&= \sum_{\sigma \in S_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)} \\
&= \sum_{\sigma \in S_n} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \underbrace{\mathrm{sign}(\sigma)}_{=\mathrm{sign}(\sigma^{-1})} e_1 \wedge \cdots \wedge e_n \\
&= \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} e_1 \wedge \cdots \wedge e_n.
\end{aligned}$$

$\bigwedge^n(R^{\oplus n}) \cong R$ with basis $e_1 \wedge \cdots \wedge e_n$, so we get the desired equality. $\square$

Proposition 15.1. *The determinant has the following properties:*

1. $\det(T) = \det(A^\top)$.
2. *If we switch 2 rows or columns of A to get B, then* $\det(B) = -\det(A)$.
3. *If we add an R-multiple of a row or column of A to another to get A, then* $\det(C) = \det(A)$.
4. *If we scale a row or column of A by $\alpha \in R$, to get D, then* $\det(A) = \alpha \det(A)$.

Proof. These follow from the formula for the determinant.

1. We showed this in the proof of the formula.

2. Reindex the sum by composing with a transposition.
3. If we have a repeated v_j, then the term is zero. So

$$v_1 \wedge \cdots \wedge (v_i + cv_j) \wedge \cdots \wedge v_n = v_1 \wedge \cdots \wedge v_n + c(\cancelto{0}{v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_n}).$$

4. The proof is the same as the previous part. □

15.2 Cofactor expansion

Definition 15.1. The (i,j) **minor** of a matrix A is the matrix $A_{i,j}$ with the i-th row and j-th column removed.

The (i,j) minor lies in $M_{n-1}(R)$.

Proposition 15.2. *For all $k \leq j \leq n$,*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det(A_{i,j}).$$

Proof. First, write

$$v_1 \wedge \cdots \wedge v_n = (-1)^{j-1} v_j \wedge (v_1 \wedge \cdots \wedge v_{j-1} \wedge v_{j+1} \wedge \cdots \wedge v_n).$$

Write $v_j = \sum_{i=1}^{n} a_{i,j} e_i$, and write $w_k^{(i)} := v_k - a_{i,k} e_i$ for all i, k.

$$\begin{aligned} &= (-1)^{j-1} \sum_{i=1}^{n} a_{i,j} e_i \wedge (w_1^{(i)} \wedge \cdots \wedge w_{j-1}^{(i)} \wedge w_{j+1}^{(i)} \wedge \cdots \wedge w_n^{(i)}) \\ &= (-1)^{j-1} \sum_{i=1}^{n} a_{i,j} \det(A_{i,j}) e_i \wedge e_1 \wedge \cdots \wedge e_{i-1} \wedge e_{i+1} \wedge \cdots \wedge e_n \\ &= \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det(A_{i,j}) e_1 \wedge \cdots \wedge e_n. \end{aligned}$$

□

Remark 15.1. In this formula, we could have indexed over j, instead.

15.3 Adjoint matrices

Definition 15.2. The **adjoint matrix** to A is the matrix with (i,j)-entry $(-1)^{i+j} \det(A_{j,i})$.

Proposition 15.3. *$A \cdot \mathrm{ad}(A) = \det(A) \cdot I_n$.*

Proof. The (i, j) entry is

$$\sum_{k=1}^{n} a_{i,k}(-1)^{k+j} \det(A_{j,K} = \begin{cases} \det(A) & i = j \\ 0 & i \neq j \end{cases}$$

because if $i \neq j$, this is the determinant of A with the j-th row replaced by the i-th row. So it is 0. $\square$

Corollary 15.1. *$A \in \mathrm{GL}_n(R) \iff \det(A) \in R^\times$. In this case, $A^{-1} = \det(A)^{-1} \operatorname{ad}(A)$.*

Corollary 15.2. *If V is free of rank n, then $T : V \to V$ is invertible iff $\det(T) \in R^\times$.*

15.4 Change of basis

Let V, W be free R-modules of rank n, m respectively. Let $B = (v_1, \ldots, v_n)$ and $C = (w_1, \ldots, w_m)$ be ordered bases of V and W. Let $T : V \to W$ be an R-module homomorphism. Then $A = (a_{i,j})$ represents T with respect to B and C if

$$T(v_j) = \sum_{i=1}^{m} a_{i,j} w_i$$

for all $1 \leq j \leq n$.

B corresponds to $\varphi_B : R^n \to V$, where $\varphi_B(e_i) = v_i$. Given $T : V \to W$, we get $\varphi_C^{-1} \circ T \circ \varphi_B : E^n \to R^m$ is $A \in M_{m,n}(R)$ using the standard basis.

Lemma 15.1. *Let $T' : U \to V$ and $T : V \to W$ be R-module homomorphisms where the modules have bases B, C, C, and D, respectively. Let A' representa T' with respect to B and C, and lt A represent T with respect to C and D. Then AA' represents TT' with respect to B and D.*

Proof. We can see

$$\varphi_D^{-1} \circ T \circ T' \circ \varphi_B = (\varphi_D^{-1} \circ T \circ \varphi_C) \circ (\varphi_C^{-1} \circ T' \circ \varphi_B).$$

The first part is representaed by A, and the latter part is represented by A'. $\square$

Definition 15.3. Let B, B' be bases of VV. The **change of basis matrix** $Q_{B,B'}$ from B to B' is the matrix representing $T_{B,B'} : V \to V$ with $T_{B,B'}(v_i) = v_i'$ with respect to B and B' is the matrix representing $\varphi_B^{-1} T_{B,B'} \varphi_B = \varphi_B^{-1} \circ \varphi_{B'}$.

16 Change of Basis, Characteristic Polynomials, Trace, and Localization of Modules

16.1 Change of basis

Last time, we discussed $Q_{B,B'}$, the change of basis matrix from $B \to B'$.

Remark 16.1. From the definition, we can see $Q_{B,B'}^{-1} = Q_{B',B}$.

Theorem 16.1 (change of basis)**.** *Let $T : V \to W$ be a homomorphism of free R-modules of finite rank. Let B and B' be ordered basis of V, and let C and C' be ordered bases of W. If A represents T with respect to B and C, then $Q_{C',C'}AW_{B,B'}$ represents T with respect to B' and C'.*

Proof. Note that

$$\varphi_{C'}^{-1}T\varphi_{B'} = (\varphi_{C'}^{-1}\varphi_C)(\varphi_C^{-1}T\varphi_{B'})(\varphi_B\varphi_B^{-1}).$$

The left hand side represents T with respect to B' and C'. The right hand side terms are represented by $Q_{C,C'}^{-1}$, A, and $Q_{B,B'}$, respectively. ☐

Definition 16.1. A and A' in $M_n(R)$ are **similar** if there exists some $Q \in \mathrm{GL}_n(R)$ such that $A' = Q^{-1}AQ$.

Definition 16.2. A is **diagonalizable** if it is similar to a diagonal matrix.

16.2 Characteristic polynomials and trace

Now suppose that $R = F$ is a field.

Definition 16.3. The **characteristic polynomial** $c_T \in F[x]$ of an F-linear trnasformation $T : V \to V$ of vector spaces is $\det(x \,\mathrm{id} - T)$.

Here, $x \,\mathrm{id} - T : F[x] \otimes_F V \to F[x] \otimes_F V$, where $x \,\mathrm{id} - T$ is really $x \otimes \mathrm{id} - \mathrm{id} \otimes T$. This is a map of free modules of finite rank. Similarly, we have $c_A(x) \in F[x]$ for $A \in M_n(F)$, where $c_A(x) = \det(xI - A)$, and $xI - A \in M_n(F[x])$.

Remark 16.2. $c_T(x) = c_A(x)$ for A representing T with respect to some basis B. This is independent of the basis B. Let $H = Q^{-1}AQ$. Then

$$\begin{aligned} c_H(x) &= \det(xI - Q^{-1}AQ) = \det(Q^{-1}(xI - a)Q) \\ &= \det(Q)^{-1}\det(xI - A)\det(Q) = \det(xI - A) \\ &= c_A(x). \end{aligned}$$

Remark 16.3. If $T(v) = \lambda v$ for $v \in V, \lambda \in F$, then $c_T(\lambda) = \det(\lambda \,\mathrm{id} - T) = 0$. So $\lambda \,\mathrm{id} - T$ is not invertible.

Definition 16.4. The **trace** of a matrix $A = [a_{i,j}] \in M_n(R)$ is $\operatorname{tr}(A) = \sum_{i=1}^n a_{i,i}$.

$\operatorname{tr} : M_n(R) \to R$ is an additive homomorphism of R-modules.

Lemma 16.1. $c_A(a) = x^n - \operatorname{tr}(A)x^{n-1} + \cdots + (-1)^n \det(A)$.

Proof. To get the constant term, we have

$$c_A(0) = \det(-A) = (-1)^n \det(A).$$

To get the largest nonzero term, note that

$$\det(xI - A) = \sum_{\sigma \in S_n} (\operatorname{sign}(\sigma))(x\delta_{1,\sigma(1)} - a_{1,\sigma(1)}) \cdots (x\delta_{n,\sigma(n)} - a_{n,\sigma(n)}).$$

The coefficient of x^{n-1} comes form the term with $\sigma = \mathrm{id}$:

$$(x - a_{1,1}) \cdots (x - a_{n,n}) = x^n - (a_{1,1} + \cdots + a_{n,n})x^{n-1} + \cdots \qquad \square$$

Definition 16.5. If $Tv = \lambda v$ with $v \neq 0$, then $\lambda \in F$ is called an **eigenvalue** of T, and v is called an **eugenvector** for T. Then $E_\lambda(T) = \{v \in V : Tv = \lambda v\}$ is an F-subspace of V called the λ-**eigenspace** for T.

If $T : V \to V$ is an F-linear transofrmation, then V has an $F[x]$-module structure by $f(x) \cdot v := f(T)(v)$. We want to study the module structure. We might as well study the structure of finitely generated modules over PIDs.

16.3 Localization of modules

Let R be a commutative ring, let M be an R-module, and let S be a multiplicatively closed subset of R.

Lemma 16.2. *The relation $\sim_S$ on $S \times M$ defined by $(s, m) \sim_S (t, n)$ is there exists some $r \in S$ such that $r(sn - tm) = 0$ is an equivalence relation.*

Definition 16.6. The **localization** of M by S, called $S^{-1}M$ is the set of equivalence classes under $\sim_S$. We write m/s for the equivalence class of (s, m).

Lemma 16.3. *$S^{-1}M$ is an $S^{-1}R$-module under the operations*

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st}, \qquad \frac{r}{s} \cdot \frac{m}{t} = \frac{rm}{st}.$$

Example 16.1. Let $p \subseteq R$ be a prime ideal. Let $S_p = R \setminus p$. Then $R_p = S_p^{-1}R$. So $M_p = S_p^{-1}M$ is an R_p-module.

Example 16.2. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}^2$. Then $M_{(3)} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}_{(3)}^2$, is a $\mathbb{Z}_{(3)}$-module, where $\mathbb{Z}_{(3)} = \{a/b : 3 \nmid b\}$.

17 Localization of Modules, Torsion, Rank, and Local Rings

17.1 Localization of modules

Let R be a commutative ring and $S \subseteq R$ be multiplicatively closed. If M is an R-module, we can define the localization $S^{-1}M$, which is an $S^{-1}R$-module.

Example 17.1. Let S be the set of nonzero non-zero divisors in R. Then $S^{-1}R = Q(R)$ is called the **total quotient ring** of R. The module $S^{-1}M$ is a $Q(R)$-module. If R is an integral domain, Q is a field, so $S^{-1}M$ is a vector space.

If M is and R-module and N is an $S^{-1}R$-module,

$$\mathrm{Hom}_{S^{-1}R}(S^{-1}M, N) \cong \mathrm{Hom}_R(M, N).$$

That is, localization is a left-adjoint to the forgetful functor.

Localization satisfies a universal property: For any $\phi : M \to N$, where N is an $S^{-1}R$-module,

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[d] & N \\ S^{-1}M \arrow[ur, dashed, "\Phi"'] & \end{tikzcd}$$

where $\Phi(m/s) = s^{-1}\phi(m)$.

Proposition 17.1. *$S^{-1}M \cong S^{-1}R \otimes_R M$ as $S^{-1}R$-modules.*

Proof. Let $S^{-1}R \times M \to S^{-1}M$ send $(r/s, m) \mapsto (rm)/s$. This is left $S^{-1}R$-linear and right R-linear, so we get a map $S^{-1}R \otimes RM \to S^{-1}M$ of $S^{-1}R$-modules. Conversely, we have the R-module homomorphism $M \to S^{-1}R \otimes_R M$ sending $m \mapsto 1 \otimes m$. The universal property gives a map $S^{-1}M \to S^{-1}R \otimes_R M$ sending $m/s \mapsto s^{-1} \otimes m$. Check that these are inverse maps. $\square$

17.2 Torsion and rank

Let $Q = Q(R)$ be the total quotient ring of R.

Definition 17.1. If M is an R-module, then $m \in M$ is **torsion** if there exists some $r \in S$ such that $rm = 0$.

$M_{\mathrm{tor}} = \{m \in M : m \text{ torsion}\}$ is an R-submodule of M.

Lemma 17.1. *$M_{\mathrm{tor}} = \ker(M \to Q \otimes_R M)$.*

Proof. $m \in M_{\mathrm{tor}}$ iff $m/1 = 0$ in $Q \otimes_R M$, since this is isomorphic to $S^{-1}M$. $\square$

Example 17.2. Let $A = \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Then $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} = A_{\text{tor}}$ is the torsion part.

Definition 17.2. We say M is **torsion-free** if $M_{\text{tor}} = 0$.

Definition 17.3. The **annihilator** of M (in R) is $\text{Ann}(M) := \{r \in R : rm = 0 \, \forall m \in M\}$.

This is an ideal of R.

Lemma 17.2. *If R is an integral domain and M is finitely generated over R, then $\text{Ann}(M) \neq 0$ if and only if $M = M_{\text{tor}}$.*

Proof. ($\Longrightarrow$): If $\text{Ann}(M) \neq 0$, then there exists some $r \neq 0$ in M such taht $rm = 0$ for all $m \in M$. So $m \in M_{\text{tor}}$ for all $m \in M$.

($\Longleftarrow$): Let $m_1, \ldots, m_n \in M$ generated M as an R-module. Let $e_1, \ldots, r_n \in R \setminus \{0\}$ be such that $r_i m_i = 0$ for all i. THen $r_1 \cdots r_n m = 0$ for all $m \in M$. Since R is an integral domain, $r_1 \cdots r_n \neq 0$, so $r_1 \cdots r_n \in \text{Ann}(M)$. □

Definition 17.4. The **rank** of an R-module over an integral domain R is $\text{rank}_R(M) = \dim_Q(Q \otimes_R M)$, if this dimension is finite.

Proposition 17.2. $\text{rank}_R(M)$ *is the maximal number of R-linearly independent elements in M.*

Proof. An element of M_{tor} is by itself linearly dependent. We may replace M by M/M_{tor}, so we may suppose M is R-torsion free. Them $M \to Q \otimes_R M$ is an injection. M has $\leq \dim_Q(Q \otimes_R M) = \text{rank}_R(M) =: n$ linearly independent elements. If $v_1, \ldots, v_n \in Q \otimes_R M$ is a basis over Q, then there exists some $r \in R$ such that $rv_1, \ldots, rv_n \in M$, and the rv_i are R-linearly independent. So we have at least n R-linearly independent elements in M. □

17.3 Local rings

Definition 17.5. A commutative ring R is **local** if it has a unique maximal ideal m.

If R is local, R/m is a field, called the **residue field** of R.

Proposition 17.3. *Let R be commutative, and let $p \subseteq R$ be a prime ideal. Then R_p is a local ring with maximal ideal pR_p. The ideals of R_p are R_p and IR_p with $I \subseteq p$.*

Lemma 17.3. *If R is local and m is maximal, then $R \setminus m = R^\times$.*

Proof. If $a \in R \setminus m$, then $(a) = R$. So $a \in R^\times$. Conversely, if $a \notin R^\times$, then $(a) \neq R$, so $(a) \subseteq m$. So $a \in m$. □

Lemma 17.4. *If R is commutative an $m \subseteq R$ is maximal, then $R/m \cong R_m/mR_m$.*

Proof. Look at $R/m \to R_m/mR_m$ given by $r + m \mapsto r/1 + mR_m$. These are both fields, so this is an injection. If $r \in R$ and $u \in R \setminus m$, then there eixsts some $r \in R \setminus m$ such that $uv = 1 \bmod m$. Then $vr + m \mapsto (vr)/1 + mR_m = r/n + mR_m$. So this is onto. □

Proposition 17.4. *Let R be commutative and M be an R-module. The following are equivalent.*

1. $M = 0$
2. $M_p = 0$ *for all prime ideals* $p \subseteq R$
3. $M_m = 0$ *for all maximal ideals* $m \subseteq R$.

Proof. Each of these is a special case of the last, so we just need to show (3) $\implies$ (1). Let $m \in M \setminus \{0\}$. Let $U = \operatorname{Ann}(R_m) = \{r \in M : rm = 0\}$. I is proper, so $I \subseteq m$ for some maximal ideal m.[2] If $r/u \in R_m$ is such that $(r/u)m = 0 \in M_m$, then there exists $s \in R \setminus m$ such that $srm = 0$. Then $sr \in m$, so $r \in m$ as m is prime. So $\operatorname{Ann}(R_m m) \subsetneq R_m$. Then $m/1 \neq 0$ in R_m. □

Next time, we will prove the following important theorem.

Lemma 17.5 (Nakayama)**.** *If M is a finitely generated module over a local ring (R, m) such that $mM = M$, then $M = 0$.*

Remark 17.1. What does the condition $mM = M$ mean? M/mM is an R/m-vector space. This says that if $M/mM = 0$, then $M = 0$.

[2]This uses Zorn's lemma.

18 Nakayama's Lemma and Structure Theory of Finitely Generated Modules Over PIDs

18.1 Nakayama's lemma and consequences

Lemma 18.1 (Nakayama). *If M is a finitely generated module over a local ring (R, m) such that $M/mM = 0$, then $M = 0$.*

Proof. Let $m_1, \dots, m_n \in M$ generate M. Then $mM = M$, so $m_1 \in mM$; that is there exist $a_i \in m$ such that $m_1 = \sum_{i=1}^n a_i m_i$. So $(1 - a_1)m_1 = \sum_{i=1}^n a_i m_i$. and $1 - a_1 \in R^\times = R \setminus m$. So $m_1 \in \operatorname{span}(\{m_2, \dots, m_n\})$. By recursion, M can be generated by 0 elements, so $M = 0$. $\square$

Corollary 18.1. *Let M be a finitely generated R-module, where (R, m) is local. Let $X \subseteq M$ be such that $\{x + mM : x \in X\}$ generates M/mM as an R/m-vector space. Then X generates M as an R-module.*

Proof. Let $N = Rx \subseteq M$. Then $N + mM = M$. Now $M/N = (N + mM)/N = m(M/N)$. So by Nakayama's lemma, $M/N = 0$, so $M = N$. $\square$

Here's how we use this.

Example 18.1. Do the tuples $(111, 107, 50)$, $(23, -17, 41)$, $(30, -8, 104)$ span $\mathbb{Q}^3$ as a $\mathbb{Q}$-vector space? They will if they span $\mathbb{Z}_{(p)}^3$ for a prime p. By Nakayama's lemma, it suffices to check if they generate $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. For $p = 3$, the tuples are $(0, -1, -1)$, $(-1, 1, -1)$, and $(0, 1, -1)$. These triples span $\mathbb{F}_3^3$, so the otiginal set spans $\mathbb{Q}^3$.

Lemma 18.2. *Let (R, m) be local, and let M be a finitely generated free module over R. Let $X \subseteq M$. If the image of X in M/mM is R/m-linearly independent, then X is R-linearly independent and can be extended to a basis of M.*

Proof. Let $\overline{X}$ be the image of X in M/mM. Extend $\overline{X}$ to a basis $\overline{B}$ of M/mM. By the corollary, any lift B of $\overline{B}$ spans M, and we can choose B to contain X. We claim that B is R-linearly independent. Say $B = \{m_1, \dots, m_n\}$. Consider $\sum_{i=1}^n a_i m_i \in M$, where $a_i \in R$ and are not all 0. Let $k \geq 0$ be minimal such that $a_i \notin m^{k+1}$ for some i. Then we have a map $m^k/m^{k+1} \otimes_R M \cong m^k/m^{k+1} \otimes M/mM \to m^k M/m^{k+1}M$. These are both vector spaces over R/m. This map is an isomorphism if $M = R$. In general, $M \cong \bigoplus_{i=1}^n R$, and tensor products distribute over direct sums, so $m^k M/m^{k+1}M \cong \bigoplus_{i=1}^n m^k/m^{k+1}$. Then $\sum_{i=1}^n a_i \otimes m_i \mapsto \sum_{i=1}^n a_i m_i$, so if the latter is 0, so is the former. But $\sum_{i=1}^n a_i \otimes m_i \neq 0$ since the m_i are a basis of M/mM. $\square$

18.2 Structure theory of finitely generated modules over PIDs

Let R be a PID, and let $Q = Q(R)$.

Lemma 18.3. *Any finitely generated R-submodule of Q is cyclic (generated by a single element).*

Proof. If $M \subseteq Q$ is a finitely generated R-submodule ,then $M = \sum_{i=1}^{n} R\alpha_i$, where $\alpha_i \in Q$. Then there exists a nonzero $d \in R$ such that $d\alpha_i \in R$ for all i. Then $dM \subseteq M$, so $dM = (a)$, where $a \in R$. Since $d : M \to dM$ is an isomorphism, $M = R(a/d)$. $\square$

Proposition 18.1. *Let V be an n-dimensional Q-vector space, and let $M \subseteq V$ be a finitely generated R-submodule. Then there exists a basis $B = \{v_1, \ldots, v_n\}$ of V such that M is a fer R-module with basis $\{v_1, \ldots, v_k\}$ ($k \leq n$).*

Proof. WIthout loss of generality, $M \neq 0$. Take $m_1 \in M \setminus \{0\}$. Then $Qm_1 \subseteq V$ is a 1-dimensional Q-vector space. Then $M \cap Qm_1 = Rv_1$ for some $v_1 \in M$ by the lemma. Let $\overline{M} = M/Rv_1$, and let $\overline{V} = V.Qv_1$. Then $\overline{M} \to \overline{V}$ is an injection. By induction on n, there exist $v_2, \ldots, v_n \in V$ such that $\overline{M}$ is free on $v_2 + Rv_1, \ldots, v_k + Rv_1$ with $k \leq n$, and $v_i + Rv_1$ form a basis of $\overline{V}$ for $2 \leq i \leq n$. Then $M = \bigoplus_{i=1}^{k} Rv_i$, and $V = \bigoplus_{i=1}^{n} Qv_i$. $\square$

Corollary 18.2. *Every finitely generated torsion-free module over a PID is free.*

Proof. Let M be a finitely generated torsion-free R-module. Then we have an map $M \to M \otimes_R Q$, which is an injection, since the kernel is $M_{\text{tor}} = 0$. It follows by the proposition that M is free. $\square$

Corollary 18.3. *Any submodule of a free R-module of rank n is free of rank $\leq n$.*

Proposition 18.2. *Let R be a ring, and let $\pi : M \to F$ be a surjection of R-modules with F free. Then there exists a spitting $\iota : F \to M$ such that ι is injection and $\pi \circ \iota = \mathrm{id}_F$. Moreover, $M = \ker(\pi) \oplus \iota(F)$; i.e. F is a direct summand of M.*

Proof. Let B be a basis of F. For each $b \in B$, let $m_b \in M$ be such that $\pi(m_n) = b$. Define $\iota : F \to M$ by $\iota(b) = m_b$ using the universal property of F. We get $\pi \circ \iota = \mathrm{id}_F$ (since linear maps that agree on a basis are equal). Then $\pi(m - \iota \circ \pi(m)) = \pi(m) - (\pi \circ \iota)(\pi(m)) = \pi(m) - \pi(m) = 0$. So $m - \iota \circ \pi(m) \in \ker(\pi)$. So $M = \ker(\pi) + \mathrm{im}(\iota)$. If $m \in \ker(\pi)$ and $m = \iota(n)$, then $0 = \pi(m) = (\pi \circ \iota)(n) = n$, so $m = 0$. So these have trivial intersection, giving us $M = \ker(\pi) \oplus \mathrm{im}(\iota)$. $\square$

19 Structure Theorem for Finitely Generated Modules over PIDs

19.1 Stripping off the torsion free part from a module

Last time, we proved the following:

Proposition 19.1. *Let R be a ring, and let $\pi : M \to F$ be a surjection of R-modules with F free. Then there exists a spitting $\iota : F \to M$ such that ι is injection and $\pi \circ \iota = \mathrm{id}_F$. Moreover, $M = \ker(\pi) \oplus \iota(F)$; i.e. F is a direct summand of M.*

Proposition 19.2. *If R is a PID and M is a finitely generated R-module, then $M \cong R^n \oplus M_{\mathrm{tor}}$ for $r = \mathrm{rank}_R(M)$.*

Proof. Let $Q = Q(R)$. Then $M \to M \otimes_R Q$ has kernel M_{tor}, so the image of $M/M_{\mathrm{tor}} \to M \otimes_R Q$ is torsion-free and hence free. So we have a surjection $M \to R^r$, where $r = \mathrm{rank}_R(M)$. Then $M/M_{\mathrm{tor}} \otimes_R Q \cong M \otimes_R Q$ with kernel M_{tor}. So $M = M_{\mathrm{tor}} \oplus R^r$. $\square$

19.2 Decomposition of the torsion part of a module

Let M be a finitely generated R-torsion module. Then $\mathrm{Ann}(M) = (x)$ for some $c \in R$ because R is a PID. The Chinese remainder theorem gives

$$R/(c) = \prod_{i=1}^{r} R/(\pi_i^{k_i}),$$

where $c{=}\pi_1^{k_1} \cdots \pi_r^{k_r}$ is a factorization of c into distinct irreducibles. We then get

$$M \cong M/cM \cong M \otimes_R R/(c) \cong \bigoplus_{i=1}^{r} M \otimes_R R/(\pi_i^{k_i}) \cong \bigoplus_{i=1}^{r} M/\pi_i^{k_i} M.$$

We have shown that

$$M \cong \bigoplus_{i=1}^{k_i} M_{(\pi_i)} \cong \bigoplus_{i=1}^{k} M/\pi_i^{k_i} M.$$

$R_{(\pi_i)}$ is a local ring with maximal ideal (π_i), so all of its ideals have the form (π_i^j) for $j \geq 0$ and (0). So

$$R/\pi_i^{k_i} R \cong R_{(\pi_i)}/\pi_i^{k_i} R(\pi_i)$$

has ideals (π_i^j) for $j \geq 0$ and (0).

Now let $\pi \in R$ be irreducible with $k \geq 1$, and write $\overline{R} = R/(\pi^k)$. Let M be a finitely generated $\overline{R}$-module. We split into cases. If $\overline{R} = R/(\pi)$ is a field: Then $M \cong \overline{R}^d$ for some $d \geq 0$. For the next case, we need the following.

Proposition 19.3. *If M be a finitely generated R-module with $\pi^k M = 0$, then $M \cong \bigoplus_{i=0}^{n} R/(\pi^{j_i})$ with $j_1 \geq j_2 \geq \cdots \geq j_n \geq 1$.*

We want to induct to get this, so we need the following lemma:

Lemma 19.1. *If m is a finitely generated $\overline{R}$-module and F is a maximal free $\overline{R}$-submodule, then $M = F \oplus C$ with $\pi^{k-1}C = 0$.*

Here is a case we have to watch out for:

Example 19.1. $\mathbb{Z}$ is a free $\mathbb{Z}$-module, and $2\mathbb{Z}$ is a free $\mathbb{Z}$-submodule, but the latter is not a direct summand of the former.

Lemma 19.2. *Any free $\overline{R}$-submodule of a finitely generated $\overline{R}$-module is a direct summand.*

To prove this lemma, we first have the following fact.

Proposition 19.4. *Any free $\overline{R}$-submodule of a free, finitely generated $\overline{R}$-module is a direct summand.*

Proof. Let A be a free $\overline{R}$-submodule of a finitely generated free $\overline{R}$-module B. We have the map $\iota : A \to B/\pi B$. If $a \in A$ with $\iota(a) = 0$¡ then $a \in A \cap \pi B$, so $\pi^{k-1}a = 0$. Then $a \in \pi A$. So $A/\pi A \to B/\pi B$ is an inclusion.

Then $B/\pi B = A/\pi A \oplus \overline{N}$. Last time, we showed that we can lift a basis of $B/\pi B$ containing a basis of $A/\pi A$ to a basis of B containing a basis of A. Now $B = A \oplus N$ for some N. $\square$

Assuming lemma 1 is true, we can use the fact to prove the second lemma as follows.

Proof. If $A \subseteq M$ is a free $\overline{R}$-submodule, choose F to be a maximal free submodule containing A. Then $M = F \oplus C$, and $F = A \oplus D$ by assumption, so $M = A \oplus (C \oplus D)$. $\square$

Now we can prove lemma 1.

Proof. Let $k \geq 2$. Let f be a maximal free $\overline{R}$-submodule. Let $N = M[\pi^{k-1}] = \{n \in M : \pi^{k-1}n = 0\}$. Then $\pi F \subseteq N$, and πF is a free R/π^{k-1}-submodule of N. By induction, there exists an R/π^{k-1}-submodule C such that $N = \pi F \oplus C$; here, we are using lemma 2 in the inductive step.

We claim that $M = F \oplus C$. Note that $F/\pi F \to M/N$ is an isomorphism. For injectivity, $F \cap N = \pi F$. Surjectivity follows from the maximality of F: we can lift a basis of M/N containing a basis of $F/\pi F$ to a basis of a larger or equal free $\overline{R}$-module (inside M) by the result from last time. Then $M = N + F = C + F$. Then $F \cap C = \pi F \cap C = 0$, so $M = F \oplus C$. $\square$

19.3 The structure theorem

Theorem 19.1 (structure theorem for finitely generated modules over PIDs)**.** *Let R be a PID, and let M be a finitely generated R-module.*

1. *There exist unique $r, k \geq 0$ and nonzero proper ideals $I_1 \subseteq I_2 \subseteq \cdots I_k$. such that $M \cong R^r \oplus R/I_1 \oplus \cdots \oplus R/I_k$.*
2. *There exist unique $r, \ell \geq 0$ and distinct nonzero prime ideals $\mathfrak{p}_i$ (up to ordering) and integers $\nu_{i,1} \geq \nu_{i,2} \geq \cdots \geq \nu_{i,m_i} \geq 1$ for some $m_i \geq 1$ such that*

$$M \cong R^r \oplus \bigoplus_{i=1}^{\ell} \bigoplus_{j=1}^{m_i} R/\mathfrak{p}_i^{\nu_{i,j}}.$$

The ideals $I_1, \dots, I_k$ are called **invariant factors**, and the $\mathfrak{p}_i^{\nu_{i,j}}$ are called **elementary divisors**.

Remark 19.1. When $R = \mathbb{Z}$, this is exactly the statement of the structure theorem for finitely generated abelian groups.

Proof. We have already proved the second part. For the first part, let $b_j = \pi_1^{\nu_{1,j}} \pi_2^{\nu_{2,j}} \cdots \pi_\ell^{\nu_{\ell,j}}$ for $j = 1, \dots, k$, where k is maximal such that $b_j \neq 1$. Here, we take $\nu_{i,j} = 0$ for $j > m_i$. Set $I_j = (b_j)$ and apply the Chinese remainder theorem:

$$R/(b_j) \cong \bigoplus_{i=1}^{\ell} R/(\pi_i^{\nu_{i,j}}).$$

Uniqueness is left as an exercise.[3] $\square$

[3]:(

20 Jordan Canonical Form

20.1 Existence and description of the Jordan canonical form

Let F be a field. Recall that an F-vector space V with a linear transformation $T : V \to V$ is the same as an $F[x]$-module V; The isomorphisms are

$$(V, T) \mapsto f(x) \cdot v = f(T)(v)$$

$$(V, x : V \to V) \leftarrow\!\shortmid V$$

This induces a correspondence between finite dimensional vector spaces with $T : V \to V$ and finitely generated torsion $F[x]$-modules V. A finitely generated torsion $F[x]$-module is

$$V \cong \bigoplus_{i=1}^{r} F[x]/(f_i)$$

where $f_i \in F[x]$ is monic with $\deg(f_i) = n_i$ and $f_1 \mid f_2 \mid \cdots \mid f_r$. Take the basis of V:

$$\{1, x, \ldots, x^{n_1-1}, 1, x, \ldots, x^{n_2-1}, \ldots, 1, x, \ldots, x^{n_r-1}\}$$

A matrix representing $x : V \to V$ with respect to this basis is

$$A = \begin{bmatrix} A_{f_1} & & & \\ & A_{f_2} & & \\ & & \ddots & \\ & & & A_{f_r} \end{bmatrix}.$$

$V_f = F[x]/(f)$, where f is monic, irreducible and of degree n has basis $1, x, \ldots, x^{n-1}$. The matrix A_f representing $x : V_f \to V_f$ is determined by:

$$x \cdot x^{i-1} = x^i, \qquad 1 \leq i \leq n-1$$

$$x \cdot x^{n-1} = x^n = -\sum_{i=1}^{n-1} c_i x^i,$$

where $f = \sum_{i=1}^{n} c_i x^i$, $c_n = 1$. So

$$A_f = \begin{bmatrix} 0 & & & & -c_0 \\ 1 & 0 & & & -c_1 \\ & 1 & \ddots & & \vdots \\ & & & 0 & \vdots \\ & & & 1 & -c_{n-1} \end{bmatrix},$$

the **companion matrix** to f. The characteristic polnynomial is

$$c_T(x) = c_A(x) = c_{A_{f_1}}(x) \cdots c_{A_{f_r}}(x),$$

where

$$\begin{aligned}
c_{A_f}(x) &= \begin{vmatrix} x & & & & c_0 \\ -1 & x & & & c_1 \\ & -1 & \ddots & & \vdots \\ & & & x & \vdots \\ & & & -1 & x + c_{n-1} \end{vmatrix} \\
&= x \begin{vmatrix} x & & & & c_1 \\ -1 & x & & & c_2 \\ & -1 & \ddots & & \vdots \\ & & & x & \vdots \\ & & & -1 & x + c_{n-1} \end{vmatrix} + (-1)^{n-1} c_0 \begin{vmatrix} -1 & x & & \\ & -1 & x & \\ & & \ddots & x \\ & & & -1 \end{vmatrix} \\
&= x \left(\frac{f - c_0}{x} \right) + c_0 \\
&= f.
\end{aligned}$$

So $c_T(x) = f_1 \dots f_r$. Then $\mathrm{Ann}(V) = (f_r) = (m_T(x))$, where $m_T(x)$ is the **minimal polynomial**.

Assume $c_T(x)$ splits completely (e.g. F is algebraically closed. By the structure theorem, we can write

$$V \cong \bigoplus_{j=1}^{t} F[x]/(x - \lambda_j)^{n_j},$$

where $\lambda_j \in F$. Then

$$V = \bigoplus_{i=1}^{m} V_{\lambda_i}, \qquad \text{where } \bigoplus_{j=1}^{t_\lambda} F[x]/(x - \lambda_i)^{n_{\lambda,j}}$$

by grouping the terms with the same λ together. Let

$$V_{n,\lambda} = F[x]/(x - \lambda^n).$$

Take the basis $(x - \lambda)^{n-1}, (x - \lambda)^{n-2}, \dots, 1$. Then

$$x \cdot (x - \lambda^{n-i} = \lambda(x - \lambda)^{n-i} + (x - \lambda)^{n-i+1}, \qquad 2 \le i \le n$$

$$x \cdot (x - \lambda)^{n-1} = \lambda(x - \lambda)^{n-1}$$

Then

$$J_{n,\lambda}\begin{bmatrix}\lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda\end{bmatrix} \in M_n(F)$$

is called a **Jordan block**, and the matrix

$$A = \begin{bmatrix}J_{n_1,\lambda_1} & & \\ & \ddots & \\ & & J_{n_t,\lambda_t}\end{bmatrix}$$

represents $x : V \to V$ with respect to the basis

$$(x - \lambda_1^{n_1 - 1}, \ldots, 1, (x-\lambda_2)^{n_2-1}, \ldots, 1, \ldots, (x-\lambda_t)^{n_t-1}, \ldots, 1.$$

The characterisitc polynomial is

$$c_{A_{n,\lambda}}(x) = \begin{vmatrix} x-\lambda & -1 & & \\ & x-\lambda & & \\ & & \ddots & -1 \\ & & & x-\lambda\end{vmatrix} = (x-\lambda)^n.$$

20.2 Eigenvalues and eigenspaces

Proposition 20.1. *λ is an eigenvalue of T iff $\lambda = \lambda_i$ for some i (where λ_i are those appearing in the Jordan canonical form).*

Proof. Look at $J_{\lambda,n}$. Then $J_{\lambda,n}e_1 = \lambda e - 1$, and $(J_{\lambda,n} - \lambda I)e_i = e_{i-1}$. λ is an eigenvalue of R iff λ is on the diagonal of A. □

Definition 20.1. The **generalized eigenspace** of T for λ is

$$\{v \in V : (T - \lambda I)^m v = 0 \text{ for some } m \geq 0\}$$

Proposition 20.2. *$c_t(x)$ splits completely iff V s a direct sum of its generalized eigenspaces.*

Example 20.1. Let

$$A = \begin{bmatrix}2 & 2 & 3 \\ 1 & 3 & 3 \\ -1 & -2 & -2\end{bmatrix}.$$

The characteristic polynomial is $c_A(x) = (x-1)^3$. We have 3 possibilities for the Jordan canonical form:

$$\begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{bmatrix}.$$

Note that

$$A - I = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ -1 & -2 & -3 \end{bmatrix}$$

has nullspace spanned by

$$\begin{bmatrix} 2 \\ -1 \\ 0 \end{bmatrix}, \qquad \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix}.$$

So we must be in the 2nd case. Look at

$$(A - I)e_1 = e_1 + e_2 - e_3.$$

Then we have the basis

$$B = (e_1, e_1 + e_2 + e_3, 2e_1 - e_2),$$

and A in this basis is

$$J = \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix} = Q^{-1}AQ,$$

where Q is the change of basis matrix from the standard basis to B. We can calculate

$$Q = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & -1 \\ 0 & -1 & 0 \end{bmatrix}.$$

21 Elementary Symmetric Functions and Discriminants

21.1 Elementary symmetric functions

Definition 21.1. If F is a field and $x_1, \ldots, x_n$ are indeterminates, for $1 \leq k \leq n$, the k-th **elemetary symmetric polynomial** in $x_1, \ldots, x_n$ is $s_{n,k} \in F[x_1, \ldots, x_n]$ given by

$$s_{n_k} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k} = \sum_{\substack{P \subseteq [n] \\ |P| = k}} \prod_{i \in P} x_i.$$

Example 21.1. Here are some examples of elementary symmetric polynomials.

$$s_{n,1} = x_1 + \cdots + x_n$$

$$x_{n,n} = x_1 \cdots x_n$$

$$x_{n,2} = x_1 x + 2 + x_1 x_3 + \cdots + x_1 \cdots x_n + x_2 x_3 + \cdots + x_2 x_2 + \cdots + x_{n-1} x_n$$

The module generated by these polynomials is isomorphic to $T^k(F^{\oplus n})^{S_k} \cong \mathrm{Sym}^k(F^{\oplus n})$ if $k! \in F^\times$.

Proposition 21.1. *$F(x_1, \ldots, x_n)/F(s_{n,1}, \ldots, s_{n,n})$ is finite, Galois with Galois group S_n.*

Proof. Call this extension K/E. Then

$$f(y) = \prod_{i=1}^{n} (y - x_i) = \sum_{i=1}^{n} (-1)^{n-i} s_{n,i} y^i$$

has roots $x_1, \ldots, x_n$. So K is the splitting field of f over E. If $\rho \in S_n$, there exists a unique $\phi(\rho) \in \mathrm{Aut}_R(K)$ such that $\phi(\rho)(h(x_1, \ldots, x_n)) = h(x_{\rho(1)}, \ldots, x_{\rho(n)})$. Then $\phi(\rho)(s_{n,k}) = s_{n,k})$ so $|phi(\rho) \in \mathrm{Gal}(K/E)$. So $\phi : S_n \to \mathrm{Gal}(K/E)$ is injective. This is also onto as $[K : E] \leq \deg(f)! = n!$. □

Corollary 21.1. *Every finite group is the Galois group of some field extension.*

Proof. If $H \leq S_n$, take $\mathrm{Gal}(K/K^H)$. □

Whether this happens for extensions of $\mathbb{Q}$ is still an open problem. This is false over $\mathbb{Q}_p$, the p-adic numbers, because all finite extensions of $\mathbb{Q}_p$ are solvable.

21.2 Discriminants

Definition 21.2. The **discriminant** of a monic, degree n polynomial $f \in F[x]$ with $f = \prod_{i=1}^{n}(x - \alpha_i) \in \overline{F}[x]$ is

$$D(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Proposition 21.2. *Let $f \in F[x]$. The following are equivalent:*

1. *f is inseparable.*
2. *$D(f) = 0$.*
3. *$f = \sum_{i=0}^{n} a_i x^i$ and $f' = \sum_{i=1}^{n} i a_i x^i$ share a common factor in $F[x]$.*

Proposition 21.3. *$D(f) \in F$.*

Proof. We may assume f is separable. Let K be the splitting field and $\sigma \in \mathrm{Gal}(K/F)$. Then

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j) \in F[x_1, \dots, x_n].$$

For $\sigma \in \Delta$, $\sigma(\Delta) = \mathrm{sgn}(\sigma)\Delta$. Then $\sigma(\Delta^2) = \Delta^2$. We have an injective map $\mathrm{Gal}(K/F) \to S_n$ sending $\tau \mapsto \rho(\tau)$. This tells us that $\tau(D(f)) = D(f)$. $\square$

We have actually shown the following.

Corollary 21.2. *Let f be monic, separable, and irreudcible. $D(f) \in (F^\times)^2$ if and only if $\mathrm{Gal}(K/F) \to A_n$ is an embedding via permutation of the roots.*

Example 21.2. Let $f = x^2 + ax + b$. Let α, β be the roots in $\overline{F}$. We also have $F(\alpha) = F(\beta)$. Then $-a = \alpha + \beta$, and $b = \alpha\beta$.

$$D = D(f) = (\alpha - \beta)^2 = a^2 - 4b.$$

If $\mathrm{char}(F) = 2$, then $a^2 - 4b = a^2$. So $F(\alpha)/F$ is trivial if $a \neq 0$ and inseparable if $a = 0$. If $\mathrm{char}(F) \neq 2$, then $F(a)/F$ is separable. Then $a^2 - rb \in F^2 \iff \alpha \in F$. The quadratic formua gives us that $F(\alpha) = F(\sqrt{D})$.

Example 21.3. Suppose $\mathrm{char}(F) \neq 3$, and let $f = x^3 + ax^2 + bx + c \in F[x]$. If we let $y = x + 1/3$, then

$$f(x) = f(y - a/3) = y^3 + \underbrace{(-a^2/3 + b)}_{p}\, y + \underbrace{(3a^2/27 - ab/3 + c)}_{q}.$$

So we have gotten rid of the degree 2 term. Let $g = x^3 + px + q \in F[x]$. Let K be the splitting field of f over F, and let $\alpha, \beta, \gamma \in K$ be the roots of g. Then

$$s_{3,1}(\alpha, \beta, \gamma) = \alpha + \beta + \gamma = 0$$

$$s_{3,2}(\alpha\beta, \gamma) = p$$

$$s_{3,3}(\alpha\beta, \gamma) = -\alpha\beta\gamma = q$$

Then

$$0 = (\alpha + \beta + \gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 + 2p$$

$$p = (\alpha\beta + \alpha\gamma + \beta\gamma)^2 = \alpha^2\beta^2 + \alpha^2 2\gamma^2 + \beta^2\gamma^2.$$

We can the compute

$$g' = 3x^2 + p = s_{3,2}(x - \alpha, x - \beta, x - \gamma)$$

$$g'(x) = 3\alpha^2 + \beta = (\alpha - \beta)(\alpha - \gamma)$$

So in the end, we get

$$-D(g) = (3x^2 + p)(3\beta^2 + p)(3\gamma^2 + \beta) = 27q^2 + 4p^3.$$

Then observe that

$$D(f) = D(g) = -27q^2 - 4p^3.$$

If f is irreducible, then $\mathrm{Gal}(K/F) \to S_3$ is an embedding and the Galois group has order divisible by 3. So this is isomorphic to $A_3 \cong \mathbb{Q}/3$, or it is isomorphic to S_3 itself. We get $\mathrm{Gal}(K/F) \cong \mathbb{Z}/3\mathbb{Z}$ if $D(f) \in (F^\times)^2$, and $\mathrm{Gal}(K/F) \cong S_3$ otherwise.

22 Norm, Trace, Characters, and Hilbert's Theorem 90

22.1 Norm and trace

Definition 22.1. Let E/F be a finite extension. For $\alpha \in E$, let $m_\alpha : E \to E$ be $x \mapsto x_\alpha$. The **trace** $\mathrm{tr}_{E/F} : E \to F$ and **norm** $N_{E/F} : E \to F$ send $\alpha \mapsto \mathrm{tr}(m_\alpha)$ and $\alpha \mapsto \det(m_\alpha)$, where we view $m_\alpha \in \mathrm{End}_F(E)$ as a matrix.

Remark 22.1. $m_{\alpha+\lambda\beta} = m_\alpha + \lambda m_\beta$, so the trace is a linear map. The norm is multiplicative because $m_{\alpha\beta} = m_\alpha \circ m_\beta$.

Proposition 22.1. *Let E/F be finite with $x \in E$. Then*

$$N_{E/F}(x) = \prod_{\sigma \in \mathrm{Emb}_F(F(x))} \sigma(x)^N = \prod_{\sigma \in \mathrm{Emb}_F(E)} \sigma(x)^{[E:F]_i},$$

$$\mathrm{tr}_{E/F}(x) = N \sum_{\sigma \in \mathrm{Emb}_F(F(x))} \sigma(x) = \left(\sum_{\sigma \in \mathrm{Emb}_F(E)} \sigma(x) \right) [E:F]_i,$$

where $N = [F(x):F]_i[E:F(x)] = [F(x):F]_i[E:F(x)]_i[E:F(x)]_s$

Proof. In each case, the second equality follows from

$$\begin{aligned} N &= [F(x):F]_i[E:F(x)] \\ &= [F(x):F]_i[E:F(x)]_i[E:F(x)]_s \\ &= [E:F]_i[E:F(x)]_s. \end{aligned}$$

Case 1: $E = F(x)$: Let $n = [F(x):F]$, let $f_x(t) = \sum_{i=0}^n a - it^i$ be the minimal polynomial of x over F. We can write $f_x(t) = \prod_{\sigma \in \mathrm{Emb}_F(F(x))} (t - \sigma(x))^{[F(x):F]_i}$. Let β be the basis $\{1, x, \ldots, x^{n-1}$ of $F(x)$. We want to show that $f_x(t)$ is the characteristic polynomial of m_x. The matrix of m_x is

$$[m_x]_\beta = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & & & & -a_1 \\ & 1 & & & \vdots \\ & & \ddots & & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

Then the characteristic polynomial of m_x is $\sum_{i=0}^n a_i t^i$. So

$$\mathrm{tr}(_{E/F}(x) = \mathrm{tr}(m_x) = -a_{n-1} = [F(x):F]_i \sum \sigma_{\sigma \in \mathrm{Emb}_F(F(x))}(x)$$

$$N_{E/F}(x) = \det(m_x) = (-1)^n a_0 = \prod_{\sigma \in in\, \mathrm{Emb}_F(F(x))} \sigma(x)^{[F(x),F]_i}$$

For the general case, let $\{y-1, \ldots, y_k\}$ be an $F(x)$-basis for E. Then $E = \bigoplus_{i=1}^k F(x) y_i$. is a decomposition into m_x-invariant subspaces ($k = [E : F(x)]$). So $\beta = \{x^i y_j\}$ is a basis for E/F, and

$$[m_x]_\beta = \begin{bmatrix} m_x & & & \\ & m_x & & \\ & & \ddots & \\ & & & m_x \end{bmatrix}$$

is block diagonal with blocks of the type of the previous case. So

$$\mathrm{tr}(m_x) = [E : F(x)][F(x) : F]_i \sum \sigma_{\sigma \in \mathrm{Emb}_F(F(x))}(x)$$

$$\det(m_x) = \prod_{\sigma \in \mathrm{Emb}_F(F(x))} \sigma(x)^{[E:F(x)][F(x):F]_i}. \qquad \square$$

Corollary 22.1. *Let $E/K/F$ be finite. Then*

$$N_{K/F} = N_{E/F} \circ N_{K/E},$$

$$\mathrm{tr}_{K/F} = \mathrm{tr}_{E/F} \circ \mathrm{tr}_{K/E}.$$

Proof. Let $x \in K$. Then

$$N_{E/F}(N_{K/E}) = \prod_{\sigma \in \mathrm{Emb}_F(E)} \sigma \left(\prod_{\tau \in \mathrm{Emb}_E(K)} \tau(x) \right)$$

Any $\varphi : K \to \overline{F}$ can be written as $\hat{\sigma} \circ \tau$ for some unique $|sigma \in \mathrm{Emb}_F(E)$ and $\tau \in \mathrm{Emb}_E(K)$.

$$\begin{tikzcd}
K \arrow[r, "\varphi"] \arrow[d, dash] & \overline{F} \\
E \arrow[ur, "\sigma"] \arrow[d, dash] & \\
F \arrow[uur] &
\end{tikzcd}$$

Then $\tau = \varphi \circ \hat{\sigma}^{-1}$ fixes E. So

$$N_{E/F}(N_{K/E}) = \prod_\sigma \prod_\tau \hat{\sigma}\tau(x) = \prod_{\varphi \in \mathrm{Emb}_F(K)} \varphi(x). \qquad \square$$

22.2 Characters and Hilbert's theorem 90

Theorem 22.1 (Hilbert's theorem 90)**.** *Let E/F be finite, Galois with cyclic Galois group $G = \langle \sigma \rangle$. Then*

$$\ker(N_{E/F}) = \{\sigma(x)/x : x \in E^\times\},$$
$$\ker(\mathrm{tr}_{E/F}) = \{\sigma(x) - x : x \in E\}.$$

The $\supseteq$ containments require no conditions, so we need to prove the other containments. To prove this, we need a bit of character theory.

Definition 22.2. Let G be a group, and let E be a field. A **character** on G with values in E is a group homomorphism $\chi : G \to E^\times$.

The set of all characters $\mathrm{char}_F(G) \subseteq \mathrm{Fun}(G.E)$ is subset of an E-vector space.

Lemma 22.1. $\mathrm{char}_E(G)$ *is linearly independent.*

Proof. Let $\{\chi_1, \dots, \chi_m\}$ be a minimal linearly dependent set. Let $\sum_{i=1}^\infty a_i\chi_i = 0$ with all $a_i \neq 0$. Choose $h \in G$ such that $\chi_1(h) \neq \chi_m(h)$. Let $b_i = a_i(\chi_i(h) - \chi_m(h)) \in E$; then $b_1 \neq 0$ and $b_m = 0$ (by definition). Now for $g \in G$,

$$\begin{aligned}
\sum_{i=1}^{m-1} b_i\chi_i(g) &= \sum_{i=1}^{m-1} a - i\chi_i(h)\chi_i(g) - a_i\chi_m(j)\chi_i(g) \\
&= \sum_{i=1}^{m-1} a_i\chi_i(hg) - \chi_m(h)\sum_{i=1}^{m-1} a_i\chi_i(g) \\
&= -a_m\chi_m(hg) - \chi_m(h)(-a_m\chi_m(g)) \\
&= -a_m\chi_m(hg) + a - m\chi_m(hg) \\
&= 0.
\end{aligned}$$

This contradicts the minimality of $\{\chi_1, \dots, \chi_m\}$. $\square$

We can now prove Hilbert's theorem 90.

Proof. We want to show that $\ker(N_{E/F}) = \{\sigma(x)/x : x \in E^\times\}$. Take $x \in \ker(N_{E/F})$. Then

$$\chi_x = \sum_{i=0}^{n-1}\left(\prod_{j=0}^{i-1} \sigma^j(x)\right)\sigma^i$$

is a character. Then

$$\chi_x(y) = y + x\sigma(y) + x\sigma(x)\sigma^2(y) + \cdots + x\sigma(x)\sigma^2(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(y).$$

The idea is we want to find a fixed point of applying σ and multiplying by x. This is because if $y \neq 0$,

$$x = \frac{\sigma(y)}{y} \iff x = \frac{y}{\sigma(y)} \iff \sigma(y)x = y.$$

For all $y \in E$, we have that $x\sigma(\chi_x(y)) = \chi_x(y)$. If $\chi_x(y) \neq 0$, we are done because $x = \chi_x(y)/\sigma(\chi_x(y))$. So χ_x is a nonzero linear combination of distinct characters and is hence nonzero by the lemma. Thus, there exists $y \in E^\times$ such that $\chi_x(y) \neq 0$. $\square$

We will do the trace next time.

23 Discriminants of Linear Maps

23.1 Hilbert's theorem 90

Let's complete our proof of Hilbert's theorem 90.

Theorem 23.1 (Hilbert's theorem 90)**.** *Let E/F be finite, Galois with cyclic Galois group $G = \langle \sigma \rangle$. Then*

$$\ker(N_{E/F}) = \{\sigma(x)/x : x \in E^\times\},$$
$$\ker(\mathrm{tr}_{E/F}) = \{\sigma(x) - x : x \in E\}.$$

Last time, we proved the result for the trace.

Proof. $\dim \ker(\mathrm{tr}) \geq n-1$, where $n = [E : F]$. Since $\ker(\mathrm{tr}_{E/F}) \supseteq \{\sigma(x) - x : x \in E\}$, it suffices to show that $\mathrm{tr}_{E/F} \neq 0$. Write the trace as $\mathrm{tr}_{E/F} = \sum_{\sigma \in G} \sigma$. This is a nonzero linear combination of characters, so $\mathrm{tr}_{E/F} \neq 0$. $\square$

23.2 Discriminants of linear maps

Recall that if $f \in F[t]$ factors in $\overline{F}$ as $f = \prod_{i=1}^n (t - \alpha_i)$, then the discriminant is $\mathrm{disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$. If $F(\alpha) = E/F$ is Galois and f is the minimal polynomial of α, then we can embed $G \to A_n$ iff $\mathrm{disc}(f)$ is a square in F.

Let V be an F-vector space with $\dim(V) = n$. The space $\{\psi : V \otimes V \to F\}$ of bilinear forms on V has dimension n^2. Let $\beta = \{v_1, \dots, v_n\}$ be an ordered basis for V. Then

$$\mathrm{Hom}(V \otimes_F V, F) \cong M_n(F),$$

via the maps

$$\psi \mapsto M_\psi = [\psi(v_i \otimes v_j)]_{i,j},$$
$$\psi_M(v_i \otimes v_j \mapsto v_i^\top M v_j) \leftarrow\!\shortmid M.$$

Definition 23.1. The **discriminant** of ψ (with respect to β) is $\mathrm{Disc}_\beta(\psi) = \det(M_\psi)$.

Proposition 23.1. *Let $T : V \to V$ be linear with basis β of V. Let $T \otimes T : V \otimes V \to V \otimes V$. Then*

$$\mathrm{Disc}_\beta(\psi \circ T \otimes T) = \det(T)^2 \,\mathrm{Disc}_\beta(\psi).$$

Proof. $\psi(Tv_i, Tv_j) = ([T]_\beta, e_i)^\top M_\psi [T]_\beta e_j$, so

$$M_{\psi \circ T \otimes T} = [T]_\beta^\top M_\psi [T]_\beta.$$

$\square$

Let E/F be a field extension, and let $\beta = \{v_1, \ldots, v_n\}$ be a bassi for E/F. Let

$$E \otimes E \xrightarrow{m} E \xrightarrow{\mathrm{tr}_{E/F}} F$$

send $v \otimes W \mapsto \mathrm{tr}(vw)$. Call this composition map tr.

Proposition 23.2. *Let* $\mathrm{Emb}_F(E) = \{\sigma_1, \ldots, \sigma_n\}$. *Define* $Q = [\sigma_i(v_j)]_{i,j}$. *Then* $M_{\mathrm{tr},\beta} = Q^\top Q$. *In particular,*

$$\mathrm{Disc}_\beta(\mathrm{tr}) = \det(Q)^2.$$

Proof.

$$\begin{aligned}
\mathrm{tr}(v_i, v_j) &= \sum_{k=1}^n \sigma_k(v_i v_j) \\
&= \sum_{k=1}^n \sigma_k(v_i)\sigma_k(v_j) \\
&= (Q^\top Q)_{i,j}.
\end{aligned}$$

□

Let $f(t) = \prod_{i=1}^n (t - \alpha_i) \in F[t]$ be irreducible and separable. Consider $F(\alpha_1)/F$. We have the nice basis $\beta = \{1, \alpha_1, \ldots, \alpha_1^{n-1}\}$. THen $\mathrm{Emb}_F(F(\alpha)) = \{\sigma_i : \alpha_1 \mapsto \alpha_i\}$. Then

$$Q(\alpha_1, \ldots, \alpha_n) = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

is the **Vandermonde matrix**.

Proposition 23.3. $\det(Q(\alpha_1, \ldots, \alpha_n)) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$.

Proof.

$$\begin{aligned}
\begin{vmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{vmatrix} &= \begin{vmatrix} 1 & 0 & \cdots & 0 \\ 1 & \alpha_2 - \alpha_1 & \cdots & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n - \alpha_1 & \cdots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix} \\
&= 1 \begin{vmatrix} \alpha_2 - \alpha_1 & \cdots & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & \vdots \\ \alpha_n - \alpha_1 & \cdots & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{vmatrix}
\end{aligned}$$

$$= (\alpha_2 - \alpha_1) \begin{vmatrix} 1 & \alpha_2 & \cdots & \alpha_1^{n-2} \\ 1 & \alpha_3 & \cdots & \alpha_2^{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-2} \end{vmatrix}.$$

This is the Vandermonde determinant for $n-1$ variables. By induction, we are done. □

So if $F(\alpha)/F$ is eparable and f is the minimum polynomial of α, then

$$\mathrm{Disc}(f) = \det(Q(\alpha_1, \ldots, \alpha_n))^2 = \mathrm{Disc}_{\{1,\alpha,\ldots,\alpha^{n-1}\}}(\mathrm{tr})$$

Proposition 23.4. *Let $F(\alpha)/F$ be separable of degree n, and let f be the minimum polynomial of α. Then*

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2} N_{E/F}(f'(\alpha))/$$

Proof. Let $f(r) = \prod_{i=1}^n (t-\alpha_i)$. Then $f'(t) - \sum_{i=1}^n \prod_{j\neq i}(t-\alpha_j)$, and $f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$. Then

$$\begin{aligned} N_{E/F}(f'(\alpha_i)) &= \prod_{j=1}^n \sigma_j(\prod_{j\neq i}(\alpha_i - \alpha_j)) \\ &= \prod_{(i,j), i\neq j} (\alpha_i - \alpha_j) \\ &= (-1)^{n(n-1)/2} \prod_{1\leq i<j\leq n} (\alpha_j - \alpha_i) \\ &= (-1)^{n(n-1)/2}\, \mathrm{Disc}(f). \end{aligned}$$

□

Corollary 23.1. *Let E/F be separable. The discriminant of the trace form is nonzero.*

Proof. Write $E = F(\alpha)$. Write $\beta = \{1, \alpha, \alpha^n\}$. Let f be the minimum polynomial of α. Then

$$\mathrm{Disc}_\beta(\mathrm{tr}) = \mathrm{Disc}(f) = \pm N_{E/F}(f'(\alpha)) \neq 0.$$

□

24 Kummer Theory and Solvability by Radicals

24.1 Kummer theory

Definition 24.1. A **Kummer extension** of a field F is an extension generated by roots of elements of $F^\times$

Let F be a field, and let $\mu_n = \mu_n(\overline{F})$ be the n-th roots of unity in an algebraic closure of $\overline{F}$ of F.

Proposition 24.1. *Let $n \geq 1$, and let $a \in F$. Set $E = F(a)$,where $\alpha^n = a$. Let $d \geq 1$ be minimal such that $\alpha^d \in F$.*

1. *E/F is Galois iff $\mathrm{char}(F) \nmid d$ and $\mu_d \subseteq E$.*
2. *If E/F is Galois, and $\mu_d \subseteq F$, then $\chi_a : \mathrm{Gal}(E/F) \to \mu_n$ such that $\chi_a(\sigma) = \sigma(\alpha)/\alpha$ is an isomorphism onto μ_d.*

Definition 24.2. χ_a is the n-th **Kummer character** of a.

Proof. To prove (1), let f be the minimal polynomial of α. Then $f \mid (x^d - \alpha^d)$, but $f \nmid (x^m - \alpha^m)$ for all m property dividing d (by the minimality of d. If $|\mu_d| = d$, then all roots of $x^d - \alpha^d$ are distinct. So f is separable. If $|\mu_d| = m \neq d$, then $x^d - \alpha^d = (x^m - \alpha^m)^{d/m}$. But $f \mid x^d - \alpha^d$ and $f \nmid x^m - \alpha^m$, so f is not separable. So $\mathrm{char}(F) \nmid d$ iff E/F is separable.

Now assume that $\mathrm{char}(F) \nmid d$. Let $\sigma : E \to \overline{F}$ be an embedding fixing F satisfying $\sigma\alpha = \zeta\alpha$ for some $\zeta \in \mu_d$. If $\mu_d \subseteq E$, then $\zeta_\alpha \in E$, so $\sigma(E) \subseteq E$. So E/F is normal and hence Galois. If $\mu_d \not\subseteq E$, then there exists σ such that ζ has order d, since $f \nmid x^m - \alpha^m$ for all m strictly dividing d. Then $\zeta\alpha \notin E$, so $\sigma\alpha \notin E$. So E/F is not normal.

To prove (2), suppose that E/F is Galois and $\mu_d \subseteq F$. Then

$$\chi_a(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma\tau(\alpha)}{\sigma(\alpha)}\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma\alpha}{\alpha}\sigma\left(\underbrace{\frac{\tau(\alpha)}{\alpha}}_{\in\mu_d\subseteq F}\right) = \chi_a(\sigma)\cdot\sigma(\chi_a(\tau)).$$

Then χ_a is 1 to 1 since it is onto and $[E : F] \leq d$, since $f \mid (x^d - \alpha^d)$. □

Remark 24.1. In general, even if $\mu \not\subseteq F$, we have a map $\chi_a : \mathrm{Gal}(E/F) \to \mu_f$ send ing $\sigma \mapsto \sigma(\alpha)/\alpha$ that is a **1-cocycle**: $\chi_a(\sigma\tau) - \chi_a(\sigma) \cdot \sigma(\chi_a(\tau))$.

Proposition 24.2. *Let $\mathrm{char}(F) \nmid n$, and $\mu_n \subseteq F$. If E/F is a cyclic extension of degree N, then $E = F(\alpha)$ with $\alpha^n \in F^\times$.*

Proof. Let $\mu_n = \langle \zeta \rangle$. Then $N_{E/F}(\zeta) = \zeta^n = 1$. Then Hilbert's theorem 90 gives us that there exists $\alpha \in E$ and $\sigma \in \mathrm{Gal}(E/F)$ of order n such that $\sigma(\alpha)/\alpha = \zeta$.

$$N_{E/F}(\alpha) = \prod_{i=0}^{n-1} \sigma^i(\alpha) = \prod_{i=0}^{n-1} \zeta^i \alpha = \zeta^{n(n-1)/2}\alpha^n = (-1)^{n-1}\alpha^n.$$

Set $a = -N_{E/F}(-\alpha) \in F^\times$. Then

$$\alpha^n = (-1)^{n-1} N_{E/F}(\alpha) = -N_{E/F}(-\alpha) = a \in F^\times. \qquad \square$$

24.2 Perfect pairing

Definition 24.3. An R-bilinear pairing $(\cdot,\cdot) : A \times B \to C$ is **perfect** if the induced maps $A \to \mathrm{Hom}_R(B, C)$ and $B \to \mathrm{Hom}_R(A, C)$ are both isomorphisms. It is **nondegenerate** if these are both injective.

Example 24.1. Let V be an infinite-dimensional vector space over F. Then look at the pairing $V \times V^* \to F$. Then we get an embedding $V \to \mathrm{Hom}(V^*, F) = V^**$, which is not in general an isomorphism. So this pairing is nondegenerate, but it is not perfect.

Theorem 24.1. *Let* $\mathrm{char}(F) \nmid n$ *and* $\mu_n \subseteq F$. *Let* E/F *be (finite) abelian of exponent dividing* n*, and set* $\Delta = F^\times \cap (E^\times)^n$. *Then there is a perfect pairing* $\mathrm{Gal}(E/F) \times \Delta/(F^\times)^n \to \mu_n$ *sending* $(\sigma, \alpha) \mapsto \sigma(a^{1/n})/a^{1/n} = \chi_a(\sigma)$, *and* $E = F(\sqrt[n]{\Delta}) = F(\sqrt[n]{a} : a \in \Delta)$. *In particular we have bijections between (finite) abelian extension of* F *of exponent dividing* n *and subgroups of* $F^\times$ *containing* $(F^\times)^n$ *(with finite index):*

$$E \mapsto F^\times \cap (E^\times)^n,$$

$$F(\sqrt[n]{\Delta}) \leftarrow\!\shortmid \Delta.$$

Proof. We have a map $\Delta/(F^\times)^n \to \mathrm{Hom}(\mathrm{Gal}(E/F), \mu_n)$ sending $a \mapsto \chi_a$. Then $\chi_a = 1$ iff $a \in (F^\times)^n$. So this map is 1 to 1. Given $\chi : \mathrm{Gal}(E/F) \to \mu_n$, the kernel H of χ corresponds to $K = E^H$ with K/F cyclic of degree dividing n. By the previous proposition, there exists some $a = \alpha^n \in \Delta$ such that $K = F(\alpha)$. Then $a \mapsto \chi_a$. Then χ is some power of χ_a. So this map is onto, as well.

We have a map $\mathrm{Gal}(E/F) \to \mathrm{Hom}(\Delta/(F^\times)^n, \mu_n)$ sending $\sigma \mapsto (a \mapsto \chi_a(\sigma))$. Then $\sigma \mapsto 1$ iff $\sigma|_\Delta = \mathrm{id}|_\Delta$, which is equivalent to $\sigma|_K = 1$ for all cyclic K/F in E. This is equivalent to $\sigma = 1$. This is an injective map between groups of the same order, so it is onto. $\square$

24.3 Solvability by radicals

Definition 24.4. A finite field extension is **solvable by radicals** if there exists $s \geq 0$ and fields E_i with $0 \leq i \leq s$ such that

1. $E_0 = F$,
2. $E_{i+1} = E_i(\sqrt[n_i]{a_i})$ $a_i \in E_i^\times$, $n_i \geq 1$
3. $E_s \supseteq E$.

If $E_s = E$, then we call E a **radical extension**.[4]

Theorem 24.2. *If $f \in F[x]$ is nonconstant with splitting gield K of degree prime to* $\mathrm{char}(F)$*, then* $\mathrm{Gal}(K/F)$ *is solvable if and only if K/F is solvable by radicals.*

[4] We do this because E is just so cool.

25 Solvability by Radicals and Integral Extensions

25.1 Solvability by radicals

Theorem 25.1. *Let $f \in F[x]$ be nonconstant with splitting field K of degree not divisible by* $\operatorname{char}(F)$. *Then K is solvable by radicals if and only if* $\operatorname{Gal}(K/F)$ *is solvable.*

Proof. Let $n = [K : F]$, let $L = K(\zeta_n)$, and let $E = F(\zeta_n)$, where $\langle \zeta_n \rangle = \mu_n$. We claim that K/F is solvable by radicals iff L/E is solvable by radicals. For ($\Longrightarrow$), we adjoin the same roots of unity. For ($\Longleftarrow$), if L/E is solvable by radicals, then L/F is solvable by radicals. Then K/F is solvable by radicals because $K \subseteq L \subseteq K_s(\zeta_n)$ (where K_s is as in the definition of solvability by radicals).

Now $\operatorname{Gal}(L/E) \cong \operatorname{Gal}(K/K \cap E) \leq \operatorname{Gal}(K/F)$, so if $\operatorname{Gal}(K/F)$ is solvable, then $\operatorname{Gal}(L/E)$ is solvable. Conversely, since $\operatorname{Gal}(L/E)$ is solvable, and since $\operatorname{Gal}(K \cap E/F) \subseteq \operatorname{Gal}(E/F)$ is abelian, $\operatorname{Gal}(L/F)$ solvable $\Longrightarrow$ $\operatorname{Gal}(K/F)$ is solvable.

So we may assume that $\zeta_n \in F$. Suppose K/F is solvable by radicals. There exists $L \supseteq L$ such that L/F is a radical extension. Exercise: we may choose L such that L/F is Galois. (The idea for this is to show that the normal closure of L/F is still radical.) Tbe $\operatorname{Gal}(L/F)$ is salvable since we have fields $F = L_0 \subseteq L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L$, such that each L_i/L_{i-1} is abelian, and L_i/F is Galois.

Suppose $\operatorname{Gal}(K/F)$ is solvable. Then there exist intermediate fields K_i/F which are normal and $K_s = K$ such that each $\operatorname{Gal}(K_{i+1}/K_i)$ is finite and abelian (given by adjoining n-th roots of elements in the previous field). So K/F is solvable by radicals. ☐

Corollary 25.1. *If* $\operatorname{char}(F) \nmid 6$ *and K is the splitting field of an irreducible polynomial of degree ≤ 4, then K/F is solvable by radicals.*

Why 4? This is because A_5 is the smallest nonsolvable group.

Example 25.1. $f = 2x^5 - 10x + 5$ has Galois group S_5. It is irreducible by Eisenstein's criterion. It has 3 real roots.

25.2 Integral extensions

Let B be a commutative ring, and let A be a subring of B. B/A is an extension of commutative rings.

Definition 25.1. We say $\beta \in B$ is **integral** over A if β is the root of a monic polynomial in $A[x]$.

Example 25.2. Any element $a \in A$ is integral over a, as it is the root of $x - a$.

Example 25.3. Let L/K be an extension of fields. If β is algebraic over K, then β is integral over K , as it is the root of its minimal polynomial.

Example 25.4. $\sqrt{2}$ is integral over $\mathbb{Z}$ as the root of $x^2 - 2$.

Example 25.5. $(1-\sqrt{5})/2$ is integral over $\mathbb{Z}$ as the root of $x^2 - x - 1$.

Example 25.6. $1/2$ is not integral over $\mathbb{Z}$. Let $f = \sum_{i=1}^{n} a_i x^i$ with $a_n = 1$, $a_i \in \mathbb{Z}$. Then $f(1/2) \in (1/2)^n + (1/2^{n-1})\mathbb{Z}$, so $f(1/2) \neq 0$.

Definition 25.2. $\beta \in \overline{\mathbb{Q}} \subseteq \mathbb{C}$ is an **algebraic integer** if it is integral over $\mathbb{Z}$.

Definition 25.3. A **number field** is a finite extension of $\mathbb{Q}$.

Proposition 25.1. *Let $\beta \in B$. The following are equivalent.*

1. *β is integral over A.*
2. *There exists $n \geq 1$ such that $\{1, \beta, \ldots, \beta^{n-1}\}$ generates $A[\beta]$ as an A-module.*
3. *$A[\beta]$ is finitely generated as an A-module.*
4. *There exists an $A[\beta]$-submodule M of B that is finitely generated over A and faithful (i.e. $\operatorname{Ann}_{A[\beta]}(M) = 0$).*

Proof. (1) $\implies$ (2): There exists a monic $f \in A[x]$ of degree n with $f(\beta) = 0$. Then $f(x) = x^n + \sum_{i=1}^{n-1} a - i - 1x^i$, so $\beta^n = -\sum_{i=1}^{n-1} a_{i-1}\beta^i \in A(1, \beta, \ldots, \beta^{n-1})$. By recursion, $\beta^m \in A(1, \beta, \ldots, \beta^{n-1})$ for all $M \geq n$. So $A[\beta]$ is generated by $\{1, \beta, \ldots, \beta^{n-1}\}$ as an A-module.

(2) $\implies$ (3): This is a special case.

(3) $\implies$ (4): Let $M = A[\beta]$. Then $\operatorname{Ann}_{A[\beta]}(A[\beta]) = 0$ since $A[\beta]$ is free over $A[\beta]$.

(4) $\implies$ (1): $M = \sum_{i=1}^{n} A\gamma_i \subseteq B$ for some $\gamma_i \in B$. Without loss of generality, suppose $\beta \neq 0$. Then $\beta\gamma_i = \sum_{j=1}^{n} a_{i,j}\gamma_j$, where $a_{i,j} \in A$. So we can form a linear transformation $T : A^n \to A^n$ by $[T]_{i,j} = a_{i,j}$. Then $f = c_T(x)$. Since $f(\beta) : M \to M$ is 0 and M is faithful, $f(\beta) = 0$. □

Example 25.7. $1/2 \in \mathbb{Q}$ is not integral over $\mathbb{Z}$ since $\mathbb{Z}[1/2]$ is not $\mathbb{Z}$-finitely generated.

Definition 25.4. B/A is an **integral extension** if eery $\beta \in B$ is integral over A.

Example 25.8. $\mathbb{Z}[\sqrt{2}]/\mathbb{Z}$ is an integral extension. It suffices to show that $\alpha = a + b\sqrt{2}$ is always the root of a polynomial. Take the polynomial $x^2 + 2az + (a^2 - 2b^2)$.

Example 25.9. Let B be a finitely generated A-module, and let M be a finitely generated B-module. Then M is a finitely generated A-module.

Next time, we will prove the following.

Proposition 25.2. *Let $B = A[\beta_1, \ldots, \beta_n]$. The following are equivalent.*

1. *B is integral over A.*
2. *Each β_i is integral over A.*
3. *B is finitely generated as an A-module.*

26 Integral Extensions and Integral Closure

26.1 Towers of integral extensions

Proposition 26.1. *Let $B = A[\beta_1, \dots, \beta_n]$. The following are equivalent.*

1. *B is integral over A.*
2. *Each β_i is integral over A.*
3. *B is finitely generated as an A-module.*

Proof. (1) $\implies$ (2): This is by definition.

(2) $\implies$ (3): Recall the lemma that if B is a finitely generated A-module and M is a finitely generated B-module, then M is a finitely generated A-module. So it is enough to show (by recursion) that $A[\beta_1, \dots, \beta_{j+1}]$ is finitely generated over $A[\beta_1, \dots, \beta_j]$ for all $0 \leq j \leq k-1$. So we reduce to the case $B = A[\beta]$, where β is integral over A. By a proposition from last time, B is finitely generated over A.

(3) $\implies$ (1): B is a faithful B-module, and it is finitely generated over A. Take $\beta \in B$. Then B is an $A[\beta]$-submodule of B that is faithful and finitely generated over A, so β is integral over A (by the same proposition from last time). $\square$

Proposition 26.2. *If B/A and C/B are integral, then so is C/A.*

Proof. Let $\gamma \in C$. There exists a monic $f \in B[x]$ with γ as a root. Let B' be the A-subalgebra of B generated by the coefficients of f. By the previous proposition, B' is finitely generated as an A-module. Then $B'[\gamma]/B'$ is integral, so $B[\gamma]$ is finitely generated as a B' module. Then $B'[\gamma]$ is finitely generated as an A-module. Thus, γ is integral over A. So C is integral over A. $\square$

26.2 Integral closure

Definition 26.1. The **integral closure** of A in B is the subset of elements in B integral over A.

Proposition 26.3. *The integral closure of A in B is an A-subalgebra of B.*

Proof. Look at $A[\alpha, \beta]$, where $\alpha, \beta \in B$ are integral over A. This is integral over A. So $\alpha - \beta$ and $\alpha\beta$ are integral over A. $\square$

Example 26.1. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$.

Example 26.2. The integral closure of $\mathbb{Z}$ in $\mathbb{Z}[x]$ is $\mathbb{Z}$.

Example 26.3. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.

Definition 26.2. The **ring of integers** O_K of a number field K is the integral closure of $\mathbb{Z}$ in K.

Remark 26.1. Integral closure as we have defined it is not absolute. It is relative to the larger ring B.

Definition 26.3. A domain A is **integrally closed** if it is its own integral closure in its quotient field.

Example 26.4. $\mathbb{Z}$ is integrally closed.

Example 26.5. Any field is integrally closed.

So this is not the same notion as algebraically closed.

Proposition 26.4. *Let A be an integrally closed domain (resp. UFD). Let $K = Q(A)$, and let L/K be a field extension. If $\beta \in L$ is integral over A with minimal polynomial $f \in K[x]$, then $f \in A[x]$.*

Proof. Let A be integrally closed. Let $g \in A[x]$ be monic, having β as a root. Then $f \mid g$ in $K[x]$. Every root of g in $\overline{K}$ (algebraic closure) is integral over A. In $\overline{K}[x]$, $f(x) = \prod_{i=1}^{n}(x - \beta_i)$, where the β_i are integral over A. So all coefficients of f are integral over A and are in K. So $f \in A[x]$, as A is integrally closed.

Let A be a UFD. There exists a $d \in K$ such that $df \mid g$ (since A is a UFD). f is monic, so $d \in A$. g is monic, so $d \in A^{\times}$. So $f \in A[x]$. □

Corollary 26.1. *UFDs are integrally closed.*

Proof. Let A be a UFD, and let $a \in K = Q(A)$ be integral over A. $x - a \in K[x]$ is the minimal polynomial. By the proposition, $x - a \in A[x]$. So $a \in A$. □

Example 26.6. $\mathbb{Z}[\sqrt{17}]$ is not integrally closed. $\alpha = (1 + \sqrt{17})/2$ satisfies $x^2 - x - 4$. So $\mathbb{Z}[\sqrt{17}]$ is not a UFD.

Proposition 26.5. *The integral closure of an integral domain A in an integrally closed extension B/A is integrally closed.*

Proof. Let $\overline{A}$ be the integral closure of A in B. Let $Q = Q(\overline{A})$ be the quotient field of $\overline{A}$. Let $\alpha \in Q$ be integral over $\overline{A}$. $\overline{A}[\alpha]/\overline{A}$ is integral (by a previous proposition). Also, $\overline{A}/A$ is integral, so $\overline{A}[\alpha]/A$ is integral. So α is integral over A, and $\alpha \in B$, so $\alpha \in \overline{A}$. □

Example 26.7. Let $\overline{\mathbb{Z}}$, the algebraic integers, be the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Then $\overline{\mathbb{Z}}$ is integrally closed.

Example 26.8. Let $K \subseteq \overline{\mathbb{Q}}$ be a number field. Then the ring of integers, $O_K = \overline{Z} \cap K$, is integrally closed.

Proposition 26.6. *Let A be an integrally closed domain with quotient field K. Let L be an algebraic extension of K. Then the integral closure of B of A in L has quotient field L.*

$$\begin{tikzcd}
L \arrow[dd, dash] \arrow[dr, dash] & \\
& B \arrow[dd, dash] \\
K \arrow[dr, dash] & \\
& A
\end{tikzcd}$$

In fact, if $\beta \in L$, then $\beta = b/d$ with $b \in B$, $d \in A$.

Proof. Let $\beta \in L$ be a root of $f = \sum_{i=0}^{n} a_i x_i \in K[x]$, where $a_n = 1$. Let $d \in A \setminus \{0\}$ be such that $df \in A[x]$. Consider $g = d^N f(d^{-1}x) = \sum_{i=0}^{n} d^{n-i} a_i x^i \in A[x]$ is monic, and $g(d\beta) = 0$. So $d\beta \in B$. Since $b := d\beta \in B$, $\beta = b/d$. $\square$

Theorem 26.1. *Let $d > 1$ be squarefree.*

$$O_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4. \end{cases}$$

Proof. Let $\alpha = a + b\sqrt{d} \in O_{\mathbb{Q}(\sqrt{d})}$, where $a, b \in \mathbb{Q}$. If $b = 0$, then $a \in \mathbb{Z}$. If $b \neq 0$, then α has a minimal polynomial $f = x^2 - 2ax + (a^2 - b^2 d)$. α is integral, so $f \in \mathbb{Z}[x]$. So $2a \in \mathbb{Z}$. We have 2 cases:

1. If $a \in \mathbb{Z}$, then $b^2 d \in \mathbb{Z}$. This implies $b \in \mathbb{Z}$, since d is squarefree.

2. If $a \notin \mathbb{Z}$, then $2a = a', 2b = b' \in \mathbb{Z}$, where a', b' are odd. Then $a^2 - b^2 - d = \frac{(a')^2 - (b')^2 d}{4} \in \mathbb{Z}$. So $(a')^2 \equiv (b')^2 d \pmod 4$. The only squares in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1. So $f \equiv 1 \pmod 4$. In this case, check that $\frac{1+\sqrt{d}}{2}$ is integral. $\square$

27 Ideals of Extensions of Rings

27.1 The going up theorem

Suppose B/A is an extension of commutative rings. How do ideals of A and ideals of B compare? If we have an ideal $\mathfrak{a}$ of A, then $\mathfrak{a}B$ is an ideal of B. We can go back by sending $\mathfrak{b} \mapsto \mathfrak{f} \cap A$.

Definition 27.1. We say an ideal $\mathfrak{b} \subseteq B$ **lies over** $\mathfrak{a} \subseteq A$ if $\mathfrak{b} \cap A = \mathfrak{a}$.

If $\mathfrak{p}$ is prime, then $\mathfrak{p}B$ need not be prime.

Example 27.1. Extend $\mathbb{Z}$ to $\mathbb{Z}[\sqrt{2}]$. Then $(2) \mapsto 2\mathbb{Z}[\sqrt{2}] = (sqrt2)^2$. However, if $\mathfrak{q} \subseteq \mathbb{Z}[\sqrt{2}]$ is prime, then $\mathfrak{q} \cap \mathbb{Z}$ is prime in $\mathbb{Z}$.

Proposition 27.1. *Let B/A be an extension of commutative rings.*

1. *If $\mathfrak{b} \subseteq B$ lies over $\mathfrak{a} \subseteq A$, then $A/\mathfrak{a}$ injects into $B/\mathfrak{b}$.*

2. *If $S \subseteq A$ is a multiplicatively closed subset and B/A is integral, then so is $S^{-1}B/S^{-1}A$.*

3. *If B/A is integral and A is a field, then so is B.*

Proposition 27.2. *Suppose B/A is integral. If $\mathfrak{p} \subseteq A$ is prime, then there exists a prime $\mathfrak{q} \subseteq B$ lying over $\mathfrak{p}$.*

Proof. Consider $S_\mathfrak{p} = A \setminus \mathfrak{p}$. Let $B_\mathfrak{p} := S_\mathfrak{p}^{-1}B$; this is integral over $A_\mathfrak{p}$. Let $\mathfrak{M} \subseteq B_\mathfrak{p}$ be maximal. Then $\mathfrak{m} = \mathfrak{M} \cap A_\mathfrak{p}$ is maximal: $A/\mathfrak{m} \to B/\mathfrak{M}$ is an injection, so by the 1st property, $A/\mathfrak{m}$ is a field. So $\mathfrak{p} = A_\mathfrak{p}$. Let $\iota : B \to B_\mathfrak{p}$. Then $q = \iota^{-1}(\mathfrak{M})$, so $\mathfrak{q}$ is prime. Then $\mathfrak{q} \cap A = \iota^{-1}(\mathfrak{M}) \cap A = \iota^{-1}(A_\mathfrak{p})\iota^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$. □

Theorem 27.1 (going up theorem)**.** *Let B/A be integral. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ be primes of A, and let $\mathfrak{q}_1 \subseteq B$ be lying over $\mathfrak{p}_1$. Then there exists a prime $\mathfrak{q}_2 \subseteq B$ with $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$ such that $\mathfrak{q}_2$ lies over $\mathfrak{p}_2$.*

Proof. Let $\overline{A} = A/\mathfrak{p}_1$, and let $\overline{B} = B/\mathfrak{q}_1$. Let $\pi : B \to \overline{B}$ be the quotient map. Let $\overline{\mathfrak{p}_2} := \pi(\mathfrak{p}_2)$. $\overline{B}/\overline{A}$ is integral, so there exists aprime $\overline{\mathfrak{q}_2}$ of $\overline{B}$ lying over $\overline{\mathfrak{p}_2}$. Then $q_2 = \pi^{-1}(\overline{\mathfrak{q}_2}) \supseteq \mathfrak{q}_1$. Then $\mathfrak{q}_2 \cap A = \pi^{-1}(\overline{q}_2 \cap \overline{A}) = \pi^{-1}(\overline{\mathfrak{p}_2}) = \mathfrak{p}_2$ since $\mathfrak{p}_2 \supseteq \mathfrak{p}_1$. □

27.2 The going down theorem

Proposition 27.3. *Let B/A be an extension, and let B' be the integral closure of A in B. Then for any multiplicatively closed $S \subseteq A$, $S^{-1}B'$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

That is, integral closure is preserved by localization.

Proof. If $b/s \in S^{-1}B$ is integral over $S^{-1}A$, there exists a monic $f \in S^{-1}A[x]$ $f(b/s) = 0$. Write $f = x^n + \sum_{i=0}^{n-1} \frac{a_i}{s_i} x^i$ with $a_i \in A$, $s_i \in S$. Set $t = s_0 \cdots s_{n-1}$. Then $(st)^n f(x/ts) \in A[x]$ has root $x = bt \in B'$. So $s^{-1}b = s^{-1}t^{-1}x$ in $S^{-1}B'$. □

In commutative algebra, we often study what properties are local. For example, we showed earlier that a module is zero iff its localizations at all maximal or all prime ideals are zero.

Proposition 27.4. *Let A be an integral domain. The following are equivalent.*

1. *A is integrally closed.*
2. *$A_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p} \subseteq A$.*
3. *$A_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m}$ of A.*

Proof. Let $\overline{A}$ be the integral closure of A in $Q(A)$. Then $A = \overline{A}$ iff $\overline{A}/A = 0$. This is an A-modules, so this happens iff $(\overline{A}/A)_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$. Observe that $(\overline{A}/A)_{\mathfrak{p}} = \overline{A}_{\mathfrak{p}}/A_{\mathfrak{p}}$, where $\overline{A}_p = S_{\mathfrak{p}}^{-1}A$ is the integral closure of $A_{\mathfrak{p}}$. □

Theorem 27.2 (going down theorem)**.** *Let B/A be an integral extension of integral domains such that A is integrally closed. Let $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$ be primes of A, and let $\mathfrak{q}_1 \subseteq B$ be lying over $\mathfrak{p}_1$. Then there exists a prime $\mathfrak{q}_2 \subseteq B$ with $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$ such that $\mathfrak{q}_2$ lies over $\mathfrak{p}_2$.*

27.3 Integral extensions in extensions of the quotient field

Let A be an integral domain, and let $K = Q(A)$. Let L be a finite, separable extension of K, and let B be the integral closure of A in L. Then

Lemma 27.1.

$$\mathrm{Tr}_{L/K}(B) \subseteq A, \qquad N_{L/K}(B) \subseteq A.$$

Proof. The minimal polynomial f of $\beta \in B$ lies in $A[x]$. Then $f = x^n - \mathrm{Tr}_{L/K}(\beta)x^{n-1} + \cdots + (-1)^{n-1}N_{L/K}(\beta)$. □

Proposition 27.5. *There exists an ordered basis $\{\alpha_1, \ldots, \alpha_n\}$ of L/K contained in B^n. Set $d = D(\alpha_1, \ldots, \alpha_n)$ and $M = \sum_{i=1}^n A\alpha_i$. Then $M \subseteq B \subseteq d^{-1}M$.*

Proof. Start with a basis $\{\beta_1, \ldots, \beta_n\}$ of L/K. Recall that each $\beta_i = b_i/a_i$ with $b_i \in B$ and $a_i \in A$. So multiplying through by $a_1, \ldots, a_n$, we have a basis of L/K in B^n.

Given $\{\alpha_1, \ldots, \alpha_n\}$, any $\beta \in L$ has the form $\beta = \sum_{i=1}^n c_i\alpha_i$, where $c_i \in K$. Suppose $\mathrm{Tr}_{L/K}(\alpha\beta)]inA$ for all $\alpha \in B$ (e.g. this holds if $\beta \in B$ by the lemma). Consider $A \ni$

$\mathrm{Tr}_{L/K}(\alpha_i\beta) = \sum_{j=1}^n c_j \mathrm{Tr}_{L/K}(\alpha_i\alpha_j)$. Note that $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)$ is the $(i,)$ entry of $Q = (\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))$. Then $Q^* = \mathrm{adj}(Q)$, and $QQ^* = dI_n$. So we get

$$QQ^* \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} dc_1 \\ \vdots \\ dc_n \end{bmatrix} \in A^n.$$

So we get $d\beta = d\sum_{i=1}^n a_i\alpha_i = \in \sum_{i=1}^n A\alpha_i = M$. Then $dB \subseteq M$, so $B \subseteq d^{-1}M$. $\square$

Remark 27.1. If B is Noetherian, then M is a finitely generated torsion-free B-submodule of L. If B were a PID, then we would get that M is free.

Now assume K/Q is a finite extension. We could define $\mathrm{disc}(K) = \mathrm{disc}(\text{basis of } O_K/\mathbb{Z})$. This is actually independent of basis.