Overview of Algebra

Zachary Gardner

zacharygardner137@gmail.com

1 Groups

1.1 Key Results

Let $A \subseteq G$. The **centralizer** subgroup of A in G is

$$C_G(A) := \{g \in G : gag^{-1} = a \text{ for every } a \in A\} = \text{stab}_G(A)$$

with the stabilizer taken with respect to the action of G on itself by conjugation, while the **normalizer** subgroup of A in G is

$$N_G(A) := \{g \in G : g \text{ normalizes } A\} = \{g \in G : gAg^{-1} = A\}.$$

Proposition 1.1.1. *A **normal** subgroup of a group G is $N \leq G$ satisfying any of the following equivalent conditions:*

(i) $gN = Ng$ *for every* $g \in G$.

(ii) $gNg^{-1} \subseteq N$ *for every* $g \in G$.

(iii) $N_G(N) = G$.

In any of the above cases we write $N \trianglelefteq G$.

A subgroup of G fixed by every automorphism of G is called **characteristic**.

Let $\text{Inn}(G) \leq \text{Aut}(G)$ denote the subgroup of **inner** automorphisms given by conjugation. This is a normal subgroup with quotient the **outer** automorphism group defined by $\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G)$. Note that $\text{Inn}(G) \cong G/\mathcal{Z}(G)$ and so G is abelian if and only if $\text{Inn}(G)$ is trivial if and only if $G/\mathcal{Z}(G)$ is cyclic.

Theorem 1.1.2 (Orbit-Stabilizer Theorem)**.** *Let G be a group acting on a set X. Given $x \in X$, there is a well-defined bijection between the G-orbit of x and the set of cosets of* $\text{stab}_G(x)$ *in G given by $g \cdot x \mapsto g\,\text{stab}_G(x)$. In particular, if G and X are both finite then the size of the G-orbit of x is $|G : \text{stab}_G(x)|$.*

Theorem 1.1.3 (Class Equation)**.** *Let G be a finite group and $g_1, \ldots, g_r$ a complete list of representatives for the distinct nontrivial conjugacy classes of G. Then,*

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Proposition 1.1.4. *Let $H, K \leq G$. Then, $HK := \{hk : h \in H, k \in K\}$ satisfies*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

In particular, if $H \cap K$ is trivial (e.g., when H, K have coprime orders) then $|HK| = |H||K|$.

Proposition 1.1.5. *Let $H, K \leq G$. Then, $HK \leq G$ if and only if $HK = KH$.*

Corollary 1.1.6. *Let $K \leq G$. If $H \leq G$ such that $H \leq N_G(K)$ then $HK \leq G$. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for every $H \leq G$.*

Note that $HK \trianglelefteq G \implies H, K \trianglelefteq G$.

Proposition 1.1.7. *Let $H, K \leq G$ such that $H, K \trianglelefteq G$ and $H \cap K = 1$. Then, $HK \cong H \times K$.*

The condition $H \cap K = 1$ ensures that every element of HK can be written **uniquely** as hk for $h \in H, k \in K$.

Theorem 1.1.8 (Group Isomorphism Theorems)**.** *Let G be a group.*

(1) *Let $\varphi : G \to H$ be a group homomorphism. Then, $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \operatorname{im} \varphi$. Moreover, every normal subgroup of G occurs as the kernel of a group homomorphism.*

(2) *Let $A, B \leq G$ with $A \leq N_G(B)$. Then, $AB \leq G, B \trianglelefteq AB, A \cap B \trianglelefteq A, AB/B \cong A/(A \cap B)$.*

(3) *Let $H, K \trianglelefteq G$ with $H \trianglelefteq K$. Then, $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.*

(4) *Let $N \trianglelefteq G$. Then, subgroups of G/N correspond to subgroups of G containing N. This bijection preserves intersections and normality.*

Theorem 1.1.9 (Cauchy)**.** *Let G be a finite group and p a prime dividing the order of G. Then, G has an element of order p.*

Cauchy's Theorem admits a vast generalization.

Theorem 1.1.10 (Sylow)**.** *Let G be a finite group with $|G| = p^r m$ for $\gcd(p, m) = 1$. Define $\operatorname{Syl}_p(G)$ to be the set of p-Sylow subgroups of G – i.e., p-subgroups of G with maximal order p^r – and let $n_p := |\operatorname{Syl}_p(G)|$.*

(i) *$n_p \neq 0$ and, moreover, every p-subgroup $H \leq G$ is contained in some $P \in \operatorname{Syl}_p(G)$.*

(ii) *Let $P, Q \in \operatorname{Syl}_p(G)$. Then, P and Q are conjugate.*

(iii) *$n_p \mid m$ and $n_p \equiv 1 \pmod{p}$. In fact, $n_p = |G : N_G(P)|$ for any $P \in \operatorname{Syl}_p(G)$ with normalizer $N_G(P)$.*

Note that $P \in \operatorname{Syl}_p(G), N \trianglelefteq G \implies P \cap N \in \operatorname{Syl}_p(N)$.

Proposition 1.1.11. *Let G be a finite group and p the smallest prime dividing $|G|$. Suppose $H \leq G$ has index p. Then, $H \trianglelefteq G$.*

Proof. The goal is to realize H as the kernel of a homomorphism out of G. G acts on the coset space G/H by left multiplication and so defines a group homomorphism $\varphi : G \to \mathrm{Sym}(G/H) \cong S_p$. This gives $G/\ker\varphi \cong \mathrm{im}\,\varphi \leq S_p$ and so $|G : \ker\varphi|$ divides $p!$. At the same time, we have $\ker\varphi \leq H$ and so $|\ker\varphi|$ divides $|H|$ hence p divides $|G : \ker\varphi|$. Thus, since $|G : \ker\varphi|$ divides $|G|$, $|G : \ker\varphi|$ divides $\gcd(p!, |G|)$ and so $|G : \ker\varphi|/p$ divides $\gcd((p-1)!, |G|/p) = 1$ since p is the smallest prime factor of $|G|$ and all of the prime factors of $(p-1)!$ are smaller than p. It follows that $|G : \ker\varphi| = p$ and so $\ker\varphi = H$. □

An abstract group is **simple** if it has no nontrivial normal subgroups. For bookkeeping reasons the trivial group is not considered to be simple.

A **composition series** for G is an exhaustive chain of normal subgroups whose successive quotients, called **composition factors**, are simple – i.e., it is a chain

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{k-1} \leq N_k = G$$

such that $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is simple.

Example 1.1.12. *Two different composition series for D_4 are given by*

$$1 \trianglelefteq \langle s \rangle \trianglelefteq \left\langle s, r^2 \right\rangle \trianglelefteq D_4$$

and

$$1 \trianglelefteq \left\langle r^2 \right\rangle \trianglelefteq \langle r \rangle \trianglelefteq D_4,$$

each having three copies of $\mathbb{Z}/2$ as composition factors. Note that each successive pair in each chain must be normal since the associated index is 2.

Theorem 1.1.13 (Jordan-Hölder)**.** *Let G be a nontrivial finite group. Then, G has a composition series and, moreover, the length of the series and the isomorphism types of the composition factors are unique, up to rearrangement.*

Let K, H be groups and $\varphi : K \to \mathrm{Aut}(H)$ a homomorphism. Define $H \rtimes_\varphi K$ to be the group whose underlying set is $H \times K$ and whose group law is

$$(h_1, k_1)(h_2, k_2) := (h_1\varphi(k_1)(h_2), k_1k_2).$$

a quick calculation shows that $H \rtimes_\varphi K$ is abelian if and only if φ is trivial and H, K are both abelian, in which case we recover the direct product $H \times K$.

Theorem 1.1.14. *Let (*) denote the short exact sequence of groups*

$$1 \longrightarrow H \longrightarrow G \longrightarrow K \longrightarrow 1$$

(i) *(*) is left split if and only if G can be compatibly identified with $H \times K$ – i.e., there is a group isomorphism $\theta : G \to H \times K$ such that the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & K & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \theta} & & \| & & \\ 1 & \longrightarrow & H & \longrightarrow & H \times K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes. The correspondence is given by taking $\theta = (\alpha', \beta)$ for $\alpha' : G \to H$ a left splitting.

(ii) *(*) is right split if and only if G can be compatibly identified with $H \rtimes_\varphi K$ for some group homomorphism $\varphi : K \to \mathrm{Aut}(H)$ – i.e., there is a group isomorphism $\theta : G \to H \rtimes_\varphi K$ such that the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & K & \longrightarrow & 1 \\ & & \| & & \vdots\theta & & \| & & \\ 1 & \longrightarrow & H & \longrightarrow & H \rtimes_\varphi K & \longrightarrow & K & \longrightarrow & 1 \end{array}$$

commutes. The correspondence is obtained as follows. Given a right splitting $\beta' : K \to G$, define $\varphi : K \to \mathrm{Aut}(H)$ by taking $\varphi(k)(h)$ to be the unique element of H such that

$$\beta'(k)\alpha(h)\beta'(k)^{-1} = \alpha(\varphi(k)(h)).$$

We then have $\theta^{-1} : H \rtimes_\varphi K \to G$ given by $(h, k) \mapsto \alpha(h)\beta'(k)$. Given compatible θ, we take $\beta'(k) = \theta^{-1}(1, k)$.

In the case that everything is abelian, we see that (*) is left split if and only if it is right split if and only if it is split (i.e., compatibly identified with $H \times K$).

1.2 Some More Group Classification

Given $H \leq G$, we have $C_G(H) \trianglelefteq N_G(H)$ with $N_G(H)/C_G(H) \hookrightarrow \mathrm{Aut}(H)$.

Given $H, K \leq G$ with $K \trianglelefteq G$, H acts by conjugation on K via automorphisms. This is the starting point for the idea of semidirect products.

Proposition 1.2.1. *Let P be a p-group.*

(a) *P has a nontrivial center.*

(b) *Suppose $|P| = p^2$. Then, P is abelian.*

For (a), use the Class Equation. For (b), use the fact that $G/\mathcal{Z}(G)$ is cyclic implies that G is cyclic.

Here are some important automorphism groups to keep in mind.

- $\mathrm{Aut}(\mathbb{Z}/n) \cong (\mathbb{Z}/n)^\times$.
- $(\mathbb{Z}/p^n)^\times \cong \mathbb{Z}/p^{n-1}(p-1)$ for p odd prime.
- $(\mathbb{Z}/2^n)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{n-2}$ for $n \geq 3$.
- Let V be an abelian group of order p^n. Then, we can regard V as a vector space of dimension n over $\mathbb{F}_p$ and hence $\mathrm{Aut}(V) \cong \mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{F}_p)$.
- If $n \neq 6$ then $\mathrm{Aut}(S_n) \cong \mathrm{Inn}(S_n) \cong S_n$.
- If $n = 6$ then $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$.
- $\mathrm{Aut}(D_8) \cong D_8$.
- $\mathrm{Aut}(Q_8) \cong S_4$.

A quick combinatorial argument shows that $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.

Proposition 1.2.2. *Let P be a nonabelian group of order p^3. Then, P is isomorphic to either the Heisenberg group of order p^3 (discussed in more detail below) or the group of matrices of the form*

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix}$$

with $m, b \in \mathbb{Z}/p^2$.

Proposition 1.2.3. *Let G be a group of order pq for distinct primes $p < q$.*

(a) *Any element of G with order q generates a normal subgroup of G.*

(b) *Suppose p does not divide $q-1$. Then, G is cyclic.*

(c) *Suppose p does divide $q-1$ and G is nonabelian. Then, G is the unique nonabelian group of order pq.*

Note that the number of elements of order pq in G must be $pq - n_p(p-1) - n_q(q-1) - 1$.

1.3 Key Examples

The **symmetric group (on n symbols)**, denoted S_n, is the group of permutations of an n-element set. Every $\sigma \in S_n$ can be written as a product of transpositions, with the number of transpositions being an invariant mod 2 called the **sign** of σ (often denoted $|\sigma|$, $\operatorname{sgn}(\sigma)$, or $\epsilon(\sigma)$). If $|\sigma|$ is 0 mod 2 then σ is **even** – otherwise it is **odd**. $\epsilon(\sigma)$ is sometimes taken to have values ± 1 instead of $0, 1$ and can be computed explicitly as $\Delta_n/\sigma(\Delta_n)$ for

$$\Delta_n := \prod_{1 \le i < j \le n} (x_i - x_j).$$

The **alternating group (on n symbols)**, denoted A_n, is the subgroup of S_n of even permutations. Viewing $\epsilon : S_n \to \{\pm 1\}$ as a group homomorphism, we thus have $A_n = \ker \epsilon$. Historically, permutation groups were the only groups that people studied. Abstract groups arose later and were originally viewed as a separate concept. This separation is a farce, however, since there is always an injection $G \hookrightarrow S_{|G|}, g \mapsto \ell_g$ for G an abstract finite group (this result is known as Cayley's Theorem). Every permutation can be decomposed uniquely (up to reordering) as a product of non-overlapping cycles written in cycle notation. This decomposition is known as the **cycle type** of a permutation. It is easy to see that a cycle is even if and only if it has odd length, giving a simple way to compute the sign of a permutation based on its cycle type.

Note that, for $n \ge 3$, A_n is generated by 3-cycles. Additionally, S_n is generated by any combination of an n-cycle and transposition or $(n-1)$-cycle and transposition.

Proposition 1.3.1. *Two elements of S_n are conjugate if and only if they have the same cycle type. Hence, the number of conjugacy classes of S_n is the number of partitions of n.*

The **dihedral group (of an n-gon)** is the group of symmetries of a regular n-gon. It is often denoted either D_n or D_{2n}, the former reflecting the dependence of the group on n and the latter reflecting the size of the group. We will stick with the former notational convention. D_n is a group of order $2n$ generated by a rotation r of order n and a reflection s of order 2, yielding a presentation

$$\left\langle r, s \mid r^n = s^2 = (rs)^2 = 1 \right\rangle.$$

Said in words, reflecting, rotating, and then reflecting is the same as rotating in the opposite direction.

The **quaternion group** Q_8 is a group of order 8 with presentation

$$\left\langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1, (-1)^2 = 1 \right\rangle.$$

The element k can be eliminated from the presentation by noting that $ij = k$. Q_8 is important for its role in the classification of groups of order 8, with a complete list of distinct representatives given by

$$Q_8, D_4, \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2, \mathbb{Z}/2 \times \mathbb{Z}/4, \mathbb{Z}/8$$

The lattice of subgroups of D_4 can be constructed by noting that r, r^3 are the elements of order 4 and $r^2 s, s, r^2, r^3 s, rs$ are the elements of order 2. These give rise to three order-4 subgroups each isomorphic to the Klein 4-group and five subgroups of order 2.

Let G be a finite group such that every nontrivial element has order p prime. If G is abelian then G is called an **elementary abelian group** and is isomorphic to $(\mathbb{Z}/p)^n$. If $p = 2$ then G is necessarily abelian. If $p \neq 2$ then G need not be abelian. This can be seen by examining the (mod p)-**Heisenberg group** of order p^3 consisting of matrices in $\mathrm{SL}_3(\mathbb{F}_p)$ of the form

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Indeed, we have

$$A^n = \begin{pmatrix} 1 & na & n(b + (n-1)ac/2) \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

and so $A^p = I$ (note that this depends crucially on p being odd).

2 Linear Algebra

2.1 General Classification of Modules over PIDs

Theorem 2.1.1 (Invariant Factor Decomposition)**.** *Let R be a PID and M a finitely generated R-module.*

(1) *There exist rank $r \in \mathbb{Z}^{\geq 0}$ and **invariant factors** $a_1, \ldots, a_m \in R$ nonzero such that $a_1 \mid a_2 \mid \cdots \mid a_m$ and $M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$.*

(2) *M is torsion-free if and only if it is free.*

(3) *$\mathrm{Tor}(M)$ is precisely the non-free part of the above decomposition and the annihilator of $\mathrm{Tor}(M)$ is (a_m).*

Theorem 2.1.2 (Elementary Divisor Decomposition)**.** *Let R be a PID and M a finitely generated R-module. Then, there exist rank $r \in \mathbb{Z}^{\geq 0}$ and **elementary divisors** $p_1^{e_1}, \ldots, p_s^{e_s}$ for $p_1, \ldots, p_s \in R$ prime and $e_1, \ldots, e_s \in \mathbb{Z}^{\geq 0}$ such that $M \cong R^r \oplus R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_s^{e_s})$.*

Theorem 2.1.3 (Primary Decomposition)**.** *Let R be a PID and M a nonzero torsion R-module with annihilator generated by nonzero $a \in R$. Choose a prime factorization $a = up_1^{e_1} \cdots p_s^{e_s}$ and let*

$$N_i := \{x \in M : p_i^{e_i} x = 0\}$$

*be the p_i-**primary part** of M. Then, N_i is the submodule of M annihilated by some power of p_i and $M \cong N_1 \oplus \cdots \oplus N_s$.*

Theorem 2.1.4 (Decomposition Uniqueness)**.** *Let R be a PID and M a finitely generated R-module. Then, the data of a free rank and a list of either invariant factors or elementary divisors determines M up to isomorphism (in the sense that there is an isomorphism between finitely generated modules with the same data).*

2.2 Rational Canonical Form

Let V be an F-vector space of finite dimension n and $T \in \mathrm{End}_F(V)$. Then, T encodes an $F[x]$-module structure on V that is necessarily torsion. The **minimal polynomial** of T is the unique monic polynomial $m_T(x) \in F[x]$ such that $(m_T(x)) = \mathrm{Ann}_{F[x]}(V)$. Examining the invariant factor decomposition of (V, T) shows that $m_T(x)$ is the largest invariant factor and is thus divisible by all of the other invariant factors. Say the invariant factor decomposition of V looks like

$$V \cong F[x]/(a_1(x)) \oplus \cdots \oplus F[x]/(a_m(x)).$$

T acts on $F[x]/(a_i(x))$ as a matrix with 1s on the subdiagonal and $-b_0, \ldots, -b_{k-1}$ down the last column, where $a_i(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0$. This matrix is called the **companion matrix** of $a_i(x)$ and denoted $\mathcal{C}_{a_i(x)}$.

Theorem 2.2.1 (Existence and Uniqueness of Rational Canonical Forms)**.** *Let V be an F-vector space of finite dimension n and $T \in \mathrm{End}_F(V)$. Then, a **rational canonical form** of T exists – i.e., T is represented by a matrix which is the direct sum of companion matrices associated to the invariant factors of V. Moreover, this form is unique.*

Theorem 2.2.2. *Let V be an F-vector space of finite dimension n and $S, T \in \mathrm{End}_F(V)$. TFAE:*

(i) *S, T are similar – i.e., conjugate in $\mathrm{End}_F(V)$.*

(ii) *S, T encode isomorphic $F[x]$-module structures on V.*

(iii) *S, T have the same canonical form.*

All of these notions make sense for a matrix A. The reason why the word rational is used is because everything takes place in F. In fact, we need only work with the smallest field containing the entries of A to compute minimal polynomials, characteristic polynomials, invariant factors, and similarity relations.

Note that, given $a(x) \in F[x]$ monic, the characteristic polynomial of $\mathcal{C}_{a(x)}$ is itself $a(x)$. On a different note, the characteristic polynomial of a block diagonal matrix is the product of the characteristic polynomials of the blocks (and hence the same applies to determinants by looking at constant terms).

Theorem 2.2.3. *Let $A \in \mathrm{Mat}_n(F)$. Then, $c_A(x)$ is the product of all of the invariant factors of A. Hence, $m_A(x) \mid c_A(x)$ and $c_A(x) \mid m_A(x)^k$ for some exponent k.*

The above theorem includes a simple version of the Cayley-Hamilton Theorem that we will explore in more detail later on.

Rational canonical form is useful for computing similarity classes of matrices over general fields and, in particular, matrices of finite order. Jordan canonical form is useful for doing the same but over algebraically closed fields.

3 Field and Galois Theory

3.1 General Facts

Theorem 3.1.1 (Ring Isomorphism Theorems)**.** *Let R be a ring.*

(1) *Let $f : R \to S$ be a ring homomorphism. Then, $\ker f$ is an ideal of R and $R/\ker f \cong \operatorname{im} f$. Moreover, every ideal of R occurs as the kernel of a ring homomorphism.*

(2) *Let $A \subseteq R$ be a subring and $I \subseteq R$ an ideal. Then, $A + I$ is a subring of R, $A \cap I$ is an ideal of A, and $(A + I)/I \cong A/(A \cap I)$.*

(3) *Let $I, J \subseteq R$ be ideals such that $I \subseteq J$. Then, $J/I \subseteq R/I$ is an ideal and $(R/I)/(J/I) \cong R/J$.*

(4) *Let $I \subseteq R$ be an ideal. Then, subrings (resp. ideals) of R/I correspond to subrings (resp. ideals) of R containing I. This bijection preserves intersections and gives rise to a correspondence between both the sets of prime ideals and maximal ideals.*

Lemma 3.1.2 (Gauss)**.** *Let A be a UFD with fraction field K. Then, $f \in A[x]$ is irreducible in $A[x]$ if and only if it is irreducible in $K[x]$ and primitive in $A[x]$.*

In this setup, the content of a product of elements in $A[x]$ is the product of the contents. The content of a nonzero element of $A[x]$ is obtained by taking the GCD of the coefficients. Being primitive is the same as having content a unit.

Corollary 3.1.3. *Let A be a UFD. Then, $A[x]$ is a UFD.*

The idea is to use Gauss's Lemma to track what happens to factorizations in $A[x]$ and $K[x]$.

Proposition 3.1.4 (Eisenstein Criterion)**.** *Let A be an integral domain, $\mathfrak{p} \in \operatorname{Spec} A$, and $f = a_n x^n + \cdots + a_0 \in A[x]$ such that $a_n \notin \mathfrak{p}$, $a_0 \notin \mathfrak{p}^2$, and $a_i \in \mathfrak{p}$ for $i < n$. Then, f cannot be written as a product of two non-constant polynomials. If f is also primitive then f is irreducible.*

Theorem 3.1.5 (Counting Irreducibles mod p)**.** *Let p be a prime. Then, the number of irreducible polynomials in $\mathbb{F}_p[x]$ of degree n is*

$$\frac{1}{n} \sum_{d \mid n} \mu(d) p^{n/d}.$$

In particular, there is at least one such polynomial.

Theorem 3.1.6 (Rational Root Theorem)**.** *Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and $r \in \mathbb{Q}$ such that $f(r) = 0$. Then, $r = d_0/d_n$ for $d_0 \mid a_0$ and $d_n \mid a_n$. In particular, $r \in \mathbb{Z}$ if f is monic.*

3.2 Galois Theory

Definition 3.2.1. *Let L/K be an extension of fields. Then, L/K is:*

- ***algebraic*** *if every $\alpha \in L$ is* ***algebraic over*** *K – i.e., α is a root of some nonzero polynomial with coefficients in K;*
- ***separable*** *if every $\alpha \in L$ is* ***separable over*** *K – i.e., the minimal polynomial of α over K has no repeated roots;*
- ***normal*** *if every irreducible polynomial with coefficients in K either has no roots in L or splits completely in L;*
- ***Galois*** *if it is algebraic, separable, and normal;*
- ***abelian*** *if it is Galois and $\mathrm{Gal}(L/K)$ is abelian;*
- ***cyclic*** *if it is Galois and $\mathrm{Gal}(L/K)$ is cyclic.*

*For L/K Galois, we let $\mathrm{Gal}(L/K)$ denote the group $\mathrm{Aut}(L/K)$ of K-linear automorphisms of L fixing K pointwise. We say L/K is G-**Galois** if L/K is Galois with $\mathrm{Gal}(L/K) \cong G$.*

Theorem 3.2.2 (Linear Independence of Characters)**.** *Let G be a group, L a field, and $\chi_1, \ldots, \chi_n : G \to L^\times$ distinct characters. Then, $\chi_1, \ldots, \chi_n$ are linearly independent. Hence, distinct embeddings and, in particular, automorphisms of a field are linearly independent.*

Corollary 3.2.3. *Let K be a field, $G \leq \mathrm{Aut}(K)$, and $F := K^G$. Then, $[K : F] = |G|$.*

Corollary 3.2.4. *Let K/F be a field extension of finite degree. Then, $|\mathrm{Aut}(K/F)| \leq [K : F]$.*

Corollary 3.2.5. *Let G_1, G_2 be finite subgroups of $\mathrm{Aut}(K)$. Then, their fixed fields are also distinct.*

Galois extensions admit alternative characterizations in the finite case.

Theorem 3.2.6. *Let L/K be a field extension of finite degree. TFAE:*

(i) $|\mathrm{Aut}(L/K)| = [L : K]$.

(ii) *L/K is normal and separable.*

(iii) *L is the splitting field of a separable polynomial in $K[x]$.*

Note that if L/K is Galois and E is an intermediate field then L/E is Galois as can be seen by looking at minimal polynomials. With the above theorem in mind, given $f(x) \in K[x]$ irreducible, we let $\mathrm{Gal}_K(f) = \mathrm{Gal}(f)$ denote the Galois group of the splitting field of f over K.

Theorem 3.2.7 (Fundamental Theorem of (Finite) Galois Theory)**.** *Let L/K be a G-Galois extension of fields. Then, the maps $H \mapsto L^H$ and $E \mapsto \mathrm{Gal}(L/E)$ induce an inclusion-reversing bijection between the set of subgroups of G and fields intermediate between K and L. Moreover,*

(a) *$H \leq G \implies L/L^H$ is Galois with $\mathrm{Gal}(L/L^H) \cong H$;*

(b) *normal subgroups of G correspond to Galois extensions of K (and, more generally, conjugates correspond to conjugates).*

Proposition 3.2.8. *Let K be a field and L_1, L_2 Galois over K. Then, the compositum L_1L_2 is Galois over K satisfying*

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

with image $\{(\sigma, \tau) : \sigma|_{L_1 \cap L_2} = \tau|_{L_1 \cap L_2}\}$. Hence, if L_1, L_2 are abelian over K then L_1L_2 is as well.

The map $\mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ is given by sending σ to $(\sigma|_{L_1}, \sigma|_{L_2})$. This map makes sense for general (possibly non-Galois) extensions and is always injective by definition of the compositum. In the general situation, the subgroup of $\mathrm{Aut}(L_1/K) \times \mathrm{Aut}(L_2/K)$ described in the proposition might be larger than the image of this map.

We say K is **perfect** if every finite extension of K is separable. If K is finite or $\mathrm{char}\, K = 0$ then K is perfect. For $\mathrm{char}\, K = p > 0$, K is perfect if and only if every element of K is a pth power. Recall that if ℓ/k is an extension of finite fields then ℓ/k is cyclic with $\mathrm{Gal}(\ell/k)$ generated by the **Frobenius map** $\sigma : \alpha \mapsto \alpha^{|k|}$.

Theorem 3.2.9 (Primitive Element Theorem)**.** *Let L/K be a finite separable extension. Then, there exists $\alpha \in L$ such that $L = K(\alpha)$.*

Theorem 3.2.10 (Normal Basis Theorem)**.** *Let L/K be a finite G-Galois extension. Then, there exists $\alpha \in L$ such that $\{\sigma\alpha : \sigma \in G\}$ is a K-basis for L. Equivalently, $L \cong K[G]$ as G-modules.*[1]

Proposition 3.2.11. *Let ℓ, p be distinct primes. Then, the reduction $\overline{\Phi}_\ell(x)$ mod p of $\Phi_\ell(x)$ factors into $(\ell - 1)/d$ distinct irreducibles in $\mathbb{F}_p[x]$ each of degree d, where d is the order of p mod ℓ. Moreover, the Galois group of the splitting field of $\overline{\Phi}_\ell(x)$ over $\mathbb{F}_p$ is isomorphic to $(\mathbb{Z}/d)^{(\ell-1)/d}$.*

3.3 Galois Computations and Abel's Theorem

Let $x_1, \ldots, x_n$ be indeterminants and $s_0, \ldots, s_n$ the elementary symmetric polynomials in these variables. The **general polynomial** of degree n is

$$P_n(x) := (x - x_1) \cdots (x - x_n) = \sum_{k=0}^{n} (-1)^{n-k} s_{n-k} x^k.$$

Theorem 3.3.1 (Fundamental Theorem of Symmetric Functions)**.** *Using the above setup,*

$$F(x_1, \ldots, x_n)^{S_n} = F(s_1, \ldots, s_n).$$

[1] Given a ring R and group G, we use the notation $R[G]$ to denote the group ring of R-linear formal sums of elements of G. An R-module with a compatible G action is then the same thing as an $R[G]$-module.

In fact, $R[x_1, \ldots, x_n]^{S_n} = R[s_1, \ldots, s_n]$ for every commutative unital ring R.

Theorem 3.3.2. *$P_n(x) \in F(s_1, \ldots, s_n)[x]$ is separable with Galois group S_n.*

Theorem 3.3.3. *Let K/F be a field extension of degree n with n not dividing the characteristic of F and F containing the nth roots of unity. Then, K/F is cyclic if and only if K is obtained from F by adjoining an nth root of some element.*

The conditions ensure that nth roots of unity are a meaningful concept and that K/F is Galois. This theorem marks the beginning of Kummer theory.

Solving by radicals means using addition, subtraction, multiplication, division, and extracting nth roots. More precisely, an element α algebraic over F can be **expressed by radicals** if α lies in a field K obtained by successive simple radical extensions. A polynomial $f \in F[x]$ can be **solved by radicals** if all of its roots can be expressed by radicals.

In the situation that α is expressible by radicals, we can always arrange that K is Galois and the successive extensions are cyclic by adjoining appropriate roots of unity and taking Galois closures.

Theorem 3.3.4 (Solvability by Radicals)**.** *Let F be a field of appropriate characteristic (e.g., 0) and $f \in F[x]$. Then, f can be solved by radicals if and only if $\mathrm{Gal}_F(f)$ is solvable.*

Corollary 3.3.5 (Abel's Theorem)**.** *Let F be a field of appropriate characteristic and $P_n(x) \in F[x]$ the general polynomial of degree n. If $n \geq 5$ then $P_n(x)$ is not solvable by radicals.*

The proof comes the fact that the Galois group of $P_n(x)$ is S_n, which is not solvable for $n \geq 5$.

4 Representation Theory of Finite Groups

4.1 Representations

Let G be a group. A **(linear) k-representation** of G is the data of a pair (V, φ) with V a k-vector space and $\varphi : G \to \mathrm{Aut}_k(V)$ a group homomorphism. Two representations (V, φ) and (W, ψ) are **equivalent** if there exists a $k[G]$-linear isomorphism between V and W. This is the same data as a k-linear isomorphism $T : V \to W$ such that

$$\begin{array}{ccc} V & \xrightarrow{\varphi(g)} & V \\ \downarrow{\scriptstyle T} & & \downarrow{\scriptstyle T} \\ W & \xrightarrow{\psi(g)} & W \end{array}$$

commutes for every $g \in G$.

The **regular representation** is the representation afforded by $k[G]$ induced by the action of G on itself by left multiplication. The **trivial representation** is the representation afforded by k induced by a trivial action of G. The regular representation has dimension $|G|$ and has sub-representations afforded by the **augmentation ideal**

$$I := \left\{ \sum_{g \in G} a_g g : \sum_{g \in G} a_g = 0 \right\}$$

and **trace ideal**

$$N := \left\{ \sum_{g \in G} a_g g : a_g = a_h \text{ for every } g, h \in G \right\}.$$

The group S_n admits the **permutation representation** afforded by k^n as well as the **sign representation** $S_n \to \mu_2 \subseteq k^\times$ given by $\sigma \mapsto \mathrm{sgn}(\sigma)$.

Let M be an R-module. M is **reducible** if it has a nontrivial submodule, and **irreducible** otherwise (a synonymous term is **simple**). M is **decomposable** if it has nontrivial submodules M_1, M_2 such that $M \cong M_1 \oplus M_2$, and **indecomposable** otherwise. M is **completely reducible** if it is a direct sum of irreducible submodules. It follows that irreducible modules are both indecomposable and completely reducible. The term "irreducible representation" is often abbreviated as "irrep."

Theorem 4.1.1 (Maschke)**.** *Let G be a finite group and k a field such that $\mathrm{char}(k)$ does not divide $|G|$. Then, every reducible $k[G]$-module is decomposable – i.e., every subrepresentation of every k-representation of G has a direct sum complement.*

Proof. Let V be a $k[G]$-module and $U \subseteq V$ a submodule. The k-linear inclusion map $U \hookrightarrow V$ has an associated k-linear projection map $\pi_0 : V \twoheadrightarrow U$. This induces a $k[G]$-linear projection map $\pi : V \twoheadrightarrow U$ via

$$\pi := \frac{1}{|G|} \sum_{g \in G} g \pi_0 g^{-1}.$$

The desired complement to U is $\ker \pi$. □

Theorem 4.1.2 (Schur's Lemma)**.** *Let M be a simple R-module. Then, $\mathrm{End}_R(M)$ is a division ring.*

This follows from the fact that every nonzero homomorphism between simple R-modules must be an isomorphism.

Theorem 4.1.3. *Let G be a finite group. Then, G has a finite number r of equivalence classes of complex irreps. In fact, letting $n_1, \ldots, n_r$ be the complex dimensions of representatives of each class, we have:*

(1) *r is the number of conjugacy classes in G;*

(2) *$|G| = n_1^2 + \cdots + n_r^2$; and*

(3) *there is a decomposition $\mathbb{C}[G] \cong \mathrm{Mat}_{n_1}(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_{n_r}(\mathbb{C})$.*

Moreover, each n_i divides $|G|$ (this a consequence of basic character theory).

Corollary 4.1.4. *Let G be a finite group.*

(1) *Suppose that G is abelian. Then, every complex irrep of G is 1-dimensional and G has precisely $|G|$ equivalence classes of complex irreps. Moreover, every finite dimensional complex representation of G is diagonalizable.*

(2) *G has precisely $|G/[G,G]|$ equivalence classes of 1-dimensional complex irreps, where $[G,G]$ is the commutator subgroup of G.*

4.2 Characters

Let G be a finite group and (V, φ) a representation of G. The associated **character** is the map $\chi : G \to k$ given by $g \mapsto \mathrm{tr}_{V/k}\, \varphi(g)$. The **principal character** of G is the character of the trivial representation. Characters are examples of **class functions** – i.e., k-valued functions on G invariant under conjugation. It is clear that equivalent representations induce the same character.

Given representations (V, φ) and (W, ψ) of G, what can we do to produce a new representation? The obvious candidate vector spaces are $V \otimes_k W$ and $V \oplus W$. These inherit G-actions via

$$g \cdot (v \otimes w) := (g \cdot v) \otimes (g \cdot w)$$

and

$$g \cdot (v, w) := (g \cdot v, g \cdot w).$$

We call the resulting representations $\varphi \otimes \psi$ and $\varphi \oplus \psi$. The associated character relations are

$$\chi_{\varphi \otimes \psi} = \chi_\varphi \chi_\psi$$

and

$$\chi_{\varphi \oplus \psi} = \chi_\varphi + \chi_\psi.$$

The first relation comes from looking at Kronecker products.

A permutation representation of G induces a linear representation whose associated character computes the number of fixed points of an element of G acting on $\{1, \ldots, n\}$. This character is called a **permutation character**.

For the rest of this section we focus on the case $k = \mathbb{C}$. Let $\mathcal{C}(G)$ denote the set of class functions on G, which is a finite dimensional complex vector space with basis given by indicator functions. By the above structure theory for complex representations, we see that every character of G breaks up as a nonnegative integral sum of irreducible characters. It is a fact that these irreps are linearly independent and so two representations of G are equivalent if and only if they have the same character.

Moreover, the irreducible characters of G form a basis for $\mathcal{C}(G)$. This becomes an ON basis under the Hermitian inner product $\langle \bullet, \bullet \rangle : \mathcal{C}(G) \times \mathcal{C}(G) \to \mathbb{C}$ defined by

$$\langle \theta, \eta \rangle := \frac{1}{|G|} \sum_{g \in G} \theta(g) \overline{\eta(g)}.$$

The details come from looking at orthogonal primitive central idempotents. As with any inner product we have a projection formula and an induced norm. We can write the above inner product in a different way that is sometimes useful. Let $K_1, \ldots, K_r$ be the conjugacy classes of G with distinct representatives $g_1, \ldots, g_r$ and sizes $d_1, \ldots, d_r$. Then,

$$\langle \theta, \eta \rangle = \frac{1}{|G|} \sum_{i=1}^{r} d_i \theta(g_i) \overline{\eta(g_i)}.$$

$\langle \bullet, \bullet \rangle$ provides a nice way to check for irreducibility: a character is irreducible if and only if it has norm 1.

Theorem 4.2.1 (Second Orthogonality Relation)**.** *Let $\chi_1, \ldots, \chi_r$ be the irreducible characters of G. Then,*

$$\sum_{i=1}^{r} \chi_i(x)\overline{\chi_i(y)} = \begin{cases} |C_G(x)|, & x, y \text{ conjugate}, \\ 0, & \text{otherwise}, \end{cases}$$

for every pair of $x, y \in G$.

Theorem 4.2.2 (Burnside-Frobenius Lemma)**.** *Let $G \leq S_n$. Given $g \in G$, let $\mathrm{Fix}(g)$ denote the number of fixed points of g acting on $\{1, \ldots, n\}$. Let N denote the number of orbits of G. Then,*

$$N|G| = \sum_{g \in G} \mathrm{Fix}(g).$$

Theorem 4.2.3. *Let χ be an irrep of G. Then, the degree $\chi(1)$ of χ divides $|G|$.*

Thus, character theory provides a proof of the claim made earlier that the integers n_i appearing in the regular representation of G are divisors of $|G|$. This is because each n_i is of the form $\chi_i(1)$.

5 Commutative and Homological Algebra

5.1 General Useful Facts About Rings

Given ideals $I, J \subseteq R$, define their **colon ideal** to be $(I : J) := \{x \in R : xJ \subseteq I\}$. This should be thought of as a formalization of the "quotient" I/J (an undefined object in general).

Let $f : R \to S$ be a ring homomorphism and $I \subseteq R$ and $J \subseteq S$ ideals. The **contraction** of J (by f) is the ideal $f^{-1}(J)$ of R. The **extension** of I (by f) is the ideal of S generated by $f(I)$ (note that $f(I)$ need not itself be an ideal). Extension and contraction are related in a number of fun little ways.

Theorem 5.1.1 (Chinese Remainder Theorem)**.** *Let R be a ring and $I_1, \ldots, I_n$ pairwise comaximal ideals (i.e., $I_j + I_k = R$ for $j \neq k$). Then,*

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$$

and the natural map

$$R \to R/I_1 \times \cdots \times R/I_n$$

is surjective with kernel $I_1 \cdots I_n$.

Slogan: Ideals maximal with respect to a certain property tend to be prime or even maximal.

Let $R_1, \ldots, R_n$ be rings and $R := R_1 \times \cdots \times R_n$. Given $\mathfrak{p} \subseteq R$ a prime ideal, there exist prime ideals $\mathfrak{p}_i \subseteq R_i$ such that $\mathfrak{p} = \mathfrak{p}_1 \times \cdots \times \mathfrak{p}_n$.

A map $R \to S$ of rings is said to be **finite** if it endows S with a finitely generated R-module structure.

Let $I \subseteq R$ be an ideal such that $\sqrt{I}$ is maximal. Then, R/I is a local ring. This rests on the description of $\sqrt{I}$ as the intersection of all prime ideals containing I.

Let $(R, \mathfrak{m}, k)$ be a local ring. Then, $R = R^\times \coprod \mathfrak{m}$. This is because every non-unit element of R is contained in a maximal ideal (hence $\mathfrak{m}$) by Zorn's Lemma. This property characterizes local rings.

Localizations of integral domains (resp., UFDs) are integral domains (resp., UFDs), at least when localizing away from 0.

5.2 Useful General Facts About Modules

An R-module P is projective if it satisfies any of the following equivalent criteria.

(i) $\mathrm{Hom}_R(P, \bullet)$ is exact.

(ii) Given an epimorphism $M \to N$, we have a commutative diagram

$$\begin{array}{ccccc} & & & & P \\ & \swarrow & & & \downarrow \\ M & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

(iii) Any short exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

splits.

(iv) P is a direct summand of a free R-module (which may be taken to have finite rank if P is finitely generated).

Projectivity can also sometimes be fruitfully understood in terms of duality. Namely, the canonical map

$$P^\vee \otimes_R P \to \mathrm{End}_R(P)^\vee$$

is an isomorphism if and only if P is finitely generated projective.

An R-module I is injective if it satisfies any of the following equivalent criteria.

(i) $\mathrm{Hom}_R(\bullet, I)$ is exact.

(ii) Given a monomorphism $M \to N$, we have a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \longrightarrow & N \\ & & \uparrow & \nearrow & \\ & & I & & \end{array}$$

(iii) Any short exact sequence

$$0 \longrightarrow I \longrightarrow M \longrightarrow N \longrightarrow 0$$

splits.

Every module has an injective hull (also called an injective envelope), which is both the smallest injective module containing it and the largest essential extension. This allows us to show that module categories have enough injectives and so the theory of right-derived functors can get off the ground.

Every injective module M is divisible, which means that multiplication by r defines an epimorphism of M for every $r \in R$ (so we can "divide" by r). The converse is true if R is a PID and is called Baer's Criterion.

Tensor-Hom adjunction says there is a canonical isomorphism:

$$\mathrm{Hom}_R(N \otimes_R M, P) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, P)).$$

5.3 Nakayama's Lemma

Theorem 5.3.1 (Cayley-Hamilton)**.** *Let $I \subseteq R$ be an ideal and M an R-module that can be generated by n elements (so there is an epimorphism from R^n). Let $\varphi \in \mathrm{End}_R(M)$ such that $\varphi(M) \subseteq IM$. Then, there exists a monic polynomial*

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

with $a_j \in I^j$ such that $p(\varphi) = 0$ in $\mathrm{End}_R(M)$.

This is a generalization of the more familiar linear algebraic Cayley-Hamilton Theorem.

Corollary 5.3.2. *Let M be a finitely generated R-module and $\alpha \in \mathrm{End}_R(M)$. Then, α is an isomorphism.*

Proof. Regard M as an $R[t]$-module with t acting by α. Apply the Cayley-Hamilton Theorem with I taken to be the ideal generated by t in $R[t]$ and φ the identity map on M. □

Note that we can prove this without using the Cayley-Hamilton Theorem in the case that M is Noetherian since

$$\ker(\alpha) \subseteq \ker(\alpha \circ \alpha) \subseteq \cdots$$

is an ascending chain of submodules which necessarily does not terminate if α is not injective.

Theorem 5.3.3 (Nakayama's Lemma)**.** *Let M be a finitely generated R-module and $I \subseteq R$ an ideal contained in the Jacobson radical (given by the intersection of all of the maximal ideals of R). Then, $M/IM = 0 \implies M = 0$.*

Corollary 5.3.4. *Let M be a finitely generated R-module and $I \subseteq R$ an ideal contained in the Jacobson radical. Then, a spanning set for M/IM lifts to a spanning set for M. In particular, if $(R, \mathfrak{m}, k)$ is local then a k-basis for $M/IM \cong k \otimes_R M$ lifts to an R-linear spanning set for M.*

Corollary 5.3.5. *Let M be a finitely generated R-module and $I \subseteq R$ an ideal contained in the Jacobson radical. Let $N \subseteq M$ be a finitely generated submodule such that $M = IM + N$. Then, $M = N$.*

The key is that $I(M/N) = (IM + N)/N = M/N$ and so $(M/N)/I(M/N) = 0$.

Corollary 5.3.6. *Let R be a local ring and M, N finitely generated R-modules such that $M \otimes_R N = 0$. Then, $\mathrm{Ann}_R(M) + \mathrm{Ann}_R(N) = R$.*

We have the following string of implications that holds for every module.

$$\text{Free} \implies \text{Projective} \implies \text{Flat} \implies \text{Torsion-Free}$$

When can we can go in the other direction? Finitely presented flat modules are the same as finitely generated projective modules. Finitely generated projective modules are locally free. Other reverse implications come from looking at structure theorems for modules over PIDs, DVRs, Dedekind domains, etc.

Localization of modules can be obtained from localization of rings by taking tensor products. Any localization can be described as a filtered colimit of localizations at the multiplicative sets generated by individual elements. Localization is an exact functor, so localized modules are flat as modules over the original ring. Beware of what this is **not** saying. Localization can kill nonzero modules. Just think about tensoring a torsion $\mathbb{Z}$-module with $\mathbb{Q}$. The stronger condition that prevents this from happening is **faithful flatness**, in which a sequence of modules is exact if and only if its image sequence under tensor product is also exact. We note that M is faithfully flat if and only if $M/\mathfrak{m}M \neq 0$ for every maximal ideal $\mathfrak{m}$ of R.

5.4 Ext and Tor

As derived functors, Ext and Tor satisfy all of the usual functoriality (including acyclic base change) properties and give rise to long exact sequences induced by short exact sequences of modules.

Lemma 5.4.1. *Let X be an A-module.*

(i) *X is projective if and only if $\operatorname{Ext}^\bullet_A(X, \bullet) = 0$ if and only if $\operatorname{Ext}^1_A(X, \bullet) = 0$.*

(ii) *X is injective if and only if $\operatorname{Ext}^\bullet_A(\bullet, X) = 0$ if and only if $\operatorname{Ext}^1_A(\bullet, X) = 0$.*

Theorem 5.4.2 (Balancing)**.** *Let M, N be A-modules.*

(i) *$\operatorname{Ext}^\bullet_A(M, N)$ can be computed by projectively resolving M or injectively resolving N.*

(ii) *$\operatorname{Tor}^A_\bullet(M, N)$ can be computed by projectively resolving either M or N.*

Corollary 5.4.3. Tor *commutes with filtered colimits of modules in either of its arguments.*

Proof. This holds because homology and tensor products commute with filtered colimits. □

To get a similar result for Ext (What is the precise statement?), note that, given any category $\mathscr{C}$, $\operatorname{Mor}_\mathscr{C} : \mathscr{C}^{\mathrm{op}} \times \mathscr{C} \to \mathsf{Set}$ commutes with limits in either of its arguments. This means that Ext^n, viewed as a bifunctor on $\mathsf{Mod}_R \times \mathsf{Mod}_R$, commutes with colimits in its first argument and limits in its second argument.

We have the useful computations

$$\operatorname{Tor}^R_n(R/(x), M) \cong \begin{cases} M/xM, & n = 0, \\ M[x], & n = 1, \\ 0, & n > 1, \end{cases}$$

and

$$\operatorname{Ext}^n_R(R/(x), M) \cong \begin{cases} M[x], & n = 0, \\ M/xM, & n = 1, \\ 0, & n > 1, \end{cases}$$

where $M[x]$ denotes the x-torsion of M.

Theorem 5.4.4 (Flat Base Change for Tor and Ext)**.** *Let S be a flat R-algebra (so there is a ring map $R \to S$ realizing S a flat R-module). Let M, N be R-modules.*

(1) *Suppose that M is finitely presented. Then, the canonical map*

$$S \otimes_R \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N)$$

is an isomorphism. This induces an isomorphism on Ext*.*

(2) *There is a canonical isomorphism*

$$\operatorname{Tor}^R_n(M, N) \cong \operatorname{Tor}^S_n(S \otimes_R M, N)$$

of R-modules for every n. This implies that there is also an S-module isomorphism similar to the one for Ext *above.*

5.5 Flatness

Flatness is a criterion which can be checked locally at either prime or maximal ideals. An R-module M is flat if and only if $I \otimes_R M \to R \otimes_R M \cong M$ is injective for every finitely generated ideal $I \subseteq R$, which is the same as the multiplication map $I \otimes_R M \to IM$ being an isomorphism. This ultimately boils down to the fact that colimits commute with colimits. It is easy to see that this is the same as $\operatorname{Tor}_1(R/I, M) = 0$ for every finitely generated ideal I.

Theorem 5.5.1 (Artin-Rees Lemma)**.** *Let R be a Noetherian ring, $I \subseteq R$ an ideal, and M a finitely generated R-module with I-stable filtration $M = M_0 \supseteq M_1 \supseteq \cdots$. Given $M' \subseteq M$ (which is finitely generated since R and hence M is Noetherian), the I-filtration of M' induced by intersection is I-stable.*

In the above, $M = M_0 \supseteq M_1 \supseteq \cdots$ is a (descending) I-filtration in the sense that $IM_n \subseteq M_{n+1}$ for every $n \geq 0$ (where each M_n is a submodule). Such an I-filtration is stable if $IM_n = M_{n+1}$ for every $n \gg 0$ (i.e., for n sufficiently large).

Theorem 5.5.2 (Krull Intersection Theorem)**.** *Let R be a Noetherian ring, M a finitely generated R-module, and $I \subseteq R$ an ideal. Then, there exists $r \in I$ such that $(1 - r) \bigcap_{n \geq 1} I^n M = 0$. In particular, $\bigcap_{n \geq 1} I^n M = 0$ if R is local and $\bigcap_{n \geq 1} I^n = 0$ if R is an integral domain.*

This follows from the Artin-Rees Lemma and an almost immediate corollary of the Cayley-Hamilton Theorem.

Theorem 5.5.3 (Local Criterion for Flatness)**.** *Let $(R, \mathfrak{m})$ be a local Noetherian ring and $(S, \mathfrak{n})$ a local Noetherian R-algebra such that $\mathfrak{m}S \subseteq \mathfrak{n}$ – i.e., there is a local ring map $(R, \mathfrak{m}) \to (S, \mathfrak{n})$. Let M be a finitely generated S-module, which inherits an R-module structure from the algebra map above. Then, M is flat as an R-module if and only if $\operatorname{Tor}_1(R/\mathfrak{m}, M) = 0$.*

Proof. The forward implication is clear, so suppose $\operatorname{Tor}_1(R/\mathfrak{m}, M) = 0$. We will show $\operatorname{Tor}_1(N, M)$ for N an R-module of finite length by induction on length(N). If length$(N) = 1$ then $N \cong R/\mathfrak{m}$ (look at annihilators) and so $\operatorname{Tor}_1(N, M) = 0$ by hypothesis. Assume now that length$(N) > 1$. Let N' be a nontrivial proper submodule of N. Then, the exact sequence

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N/N' \longrightarrow 0$$

induces an exact sequence

$$\operatorname{Tor}_1(N', M) \longrightarrow \operatorname{Tor}_1(N, M) \longrightarrow \operatorname{Tor}_1(N/N', M)$$

By the inductive hypothesis, $\operatorname{Tor}_1(N') = 0 = \operatorname{Tor}_1(N/N', M)$ and so $\operatorname{Tor}_1(N, M) = 0$ by exactness. M is flat if and only if $\operatorname{Tor}_1(R/I, M) = 0$ for all ideals $I \subseteq R$ (in fact, we need only consider the finitely generated ideals by abstract nonsense since colimits commute with colimits). Thus, M is flat if and only if, given any ideal $I \subseteq R$, $\ker(I \otimes M \to M) = 0$. So, fix an ideal $I \subseteq R$. Our goal will be to show $\ker(I \otimes_R M \to M) = 0$ by "threading the needle." The R-module $I \otimes_R M$ inherits a natural S-module structure from M, and is finitely generated as an S-module since M is as well. Since $\mathfrak{m}S \subseteq \mathfrak{n}$, we therefore have $\mathfrak{m}^n(I \otimes_R M) \subseteq \mathfrak{n}^n(I \otimes_R M)$ for all $n \geq 1$. By the Krull Intersection Theorem, $\bigcap_{n \geq 1} \mathfrak{n}^n(I \otimes_R M) = 0$ and so $\bigcap_{n \geq 1} \mathfrak{m}^n(I \otimes_R M) = 0$ by containment. $\mathfrak{m}^n(I \otimes_R M)$ is the image of the natural map $\mathfrak{m}^n I \otimes_R M \to I \otimes_R M$ induced by inclusion $\mathfrak{m}^n I \subseteq I$. □

Corollary 5.5.4. *Let R be a Noetherian ring and M a finitely generated R-module. Then, M is flat if and only if $\operatorname{Tor}_1(R/\mathfrak{m}, M) = 0$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$.*

Remark 5.5.5. *This result actually holds without the Noetherian assumption if we require that M is finitely presented. This condition doesn't really affect anything in the above situation since a finitely generated module over a Noetherian ring is automatically finitely presented.*

Proof. This follows from the above theorem and the fact that Tor localizes. □

5.6 Noetherian and Artinian Rings and Modules

A ring R is Noetherian if it satisfies any of the following equivalent criteria.

(i) Every ascending chain of ideals in R terminates.

(ii) Every ideal of R is finitely generated.

(iii) Every nonempty collection of ideals of R has an element maximal with respect to inclusion.

The first condition is called the Ascending Chain Condition (ACC). There is a similar Descending Chain Condition (DCC) which gives rise to Artinian rings. Both concepts extend to modules very naturally and have the "two-out-of-three" property for short exact sequences. It is immediate that a ring R is Noetherian (resp. Artinian) if and only if every finitely generated R-module is Noetherian (resp. Artinian).

What do Noetherian modules look like? The homomorphic image of a Noetherian module is also Noetherian, so localizations and quotients of Noetherian modules are Noetherian (the same holds true with Noetherian replaced by Artinian). Note, however, that being Noetherian is not a local

property – given a field k, the ring $R := k^{\mathbb{N}}$ is not Noetherian but all of its prime localizations are Noetherian. One very important input is the following theorem.

Theorem 5.6.1 (Hilbert Basis Theorem)**.** *Let R be a Noetherian ring. Then, $R[x]$ is a Noetherian ring.*

PIDs and Dedekind domains (such as DVRs) provide many commonly encountered examples of Noetherian rings.

Theorem 5.6.2 (Eakin-Nagata)**.** *Let $R \subseteq S$ be a ring extension such that S is a finitely generated R-module. Then, R is Noetherian if and only if S is Noetherian.*

What about Artinian rings and modules? What do they look like? Here are some examples.

- Finite rings
- Fields
- $k[t]/(t^n)$ for k a field
- $k[x,y]/(x^2, y^3, xy^2)$ for k a field
- A/I is a principal Artinian ring for A a Dedekind domain and I a nonzero ideal

The ring $\mathbb{Z}$ is a good example of a ring that is Noetherian but not Artinian. We shall see shortly that there are no examples of Artinian rings that are not Noetherian (a somewhat surprising conclusion given the resemblance in definition of both notions).

As with groups, for modules we have a notion of composition series and an analogue of the Jordan-Hölder Theorem. The **length** of a module M, denoted $\ell(M)$, is taken to be the length of any composition series for M. Note that there are plenty of examples where this is infinite. We shall see in a second that the choice of composition series does not matter.

Existence of composition series satisfies the two-out-of-three property for short exact sequences. Moreover, length is additive on short exact sequences.

Theorem 5.6.3 (Jordan-Hölder for Modules)**.** *Let M be an R-module.*

(1) *M has a finite composition series if and only if M is both Artinian and Noetherian.*

(2) *Suppose that M has a composition series with length n.*

   (a) *$\ell(M)$ is well-defined. In fact, every chain of submodules of M has length $\leq n$ and can be refined to a composition series.*

   (b) *There is a natural isomorphism*
   $$M \cong \bigoplus_{\mathfrak{m}} M_{\mathfrak{m}}$$
   with each $\mathfrak{m}$ arising from $M_i/M_{i+1} \cong R/\mathfrak{m}$ in a composition series. This is independent of the choice of composition series.

   (c) *$M = M_{\mathfrak{m}}$ if and only if M is annihilated by some power of $\mathfrak{m}$.*

Theorem 5.6.4 (Classification of Artinian Rings)**.** *TFAE:*

(i) *R is Noetherian and all prime ideals are maximal (i.e.,* $\dim R = 0$*).*

(ii) *$\ell(R)$ is finite.*

(iii) *R is Artinian.*

Hence, any Artinian ring is a finite direct product of local Artinian rings (so, in particular, has finitely many maximal ideals). This product decomposition is unique up to permutation and isomorphism of the factors.

It is also true that an Artinian ring has a nilpotent nilradical. For Noetherian local rings, the above classification has a very simple form.

Theorem 5.6.5. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. TFAE:*

(i) $\dim R = 0$.

(ii) $\mathrm{nil}(R) = \mathfrak{m}$.

(iii) *$\mathfrak{m}$ is nilpotent.*

(iv) *R is Artinian.*

Note that we specifically make a Noetherian assumption as opposed to before.

Theorem 5.6.6 (Classification of Modules of Finite Length)**.** *Let R be a Noetherian ring and M a finitely generated R-module. TFAE:*

(i) *$\ell(M)$ is finite.*

(ii) *Some finite product of maximal ideals $\mathfrak{m}_1 \times \cdots \times \mathfrak{m}_n$ annihilates M.*

(iii) *All primes containing $\mathrm{Ann}_R(M)$ are maximal.*

(iv) *$R/\mathrm{Ann}_R(M)$ is an Artinian ring.*

5.7 Associated Primes and Primary Decomposition

The **associated primes** of M are primes of R that are annihilators of elements of M:

$$\mathrm{Ass}(M) = \mathrm{Ass}_R(M) := \{\mathfrak{p} \in \mathrm{Spec}(R) : \text{ there exists } m \in M \text{ such that } \mathfrak{p} = \mathrm{Ann}_R(m)\}.$$

It is tradition to define $\mathrm{Ass}(I) := \mathrm{Ass}(R/I)$ for $I \subseteq R$ an ideal, even though this creates a minor inconsistency.

Lemma 5.7.1 (Prime Avoidance)**.** *Let $I_1, \ldots, I_n, J \subseteq R$ be ideals such that $J \subseteq I_1 \cup \cdots \cup I_n$. If R contains an infinite field **or** at most two of the I_k are not prime then J is contained in one of the I_k.*

Theorem 5.7.2. *Let R be a Noetherian ring and M a nonzero finitely generated R-module.*

(1) *Every element of $\mathrm{Ass}(M)$ contains $\mathrm{Ann}_R(M)$.*

(2) *$\mathrm{Ass}(M)$ contains all primes minimal among primes containing $\mathrm{Ann}_R(M)$ and so, a fortiori, is nonempty.*

(3) $\mathrm{Ass}(M)$ *is finite.*

(4) *The union of primes in* $\mathrm{Ass}(M)$ *is the set of zero-divisors on* M *(we let* 0 *be a zero-divisor).*

(5) *The construction of* Ass *commutes with localization.*

Corollary 5.7.3. *Let* R *be a Noetherian ring and* $I \subseteq R$ *an ideal. Then,* R *has finitely many minimal prime ideals over* I*.*

There are of course other ways to see this. By Zorn's Lemma, the radical of I is the intersection of all prime ideals containing I. Since R is Noetherian, this intersection is finite. All of the same arguments go through with prime ideal replaced by minimal prime ideal.

Corollary 5.7.4. *Let* R *be a Noetherian ring and* M *a nonzero finitely generated* R*-module. Let* I *be an ideal of* R *consisting entirely of zero-divisors on* M*. Then,* I *annihilates some element of* M *– i.e., there exists* $m \in M$ *such that* $I \subseteq \mathrm{Ann}_R(m)$*.*

Proof. By the previous theorem, I is contained in the union of primes in $\mathrm{Ass}(M)$. Thus it must be contained in one of them by the Prime Avoidance Lemma. □

Corollary 5.7.5. *Let* R *be a Noetherian ring and* $\mathfrak{p} \in \mathrm{Spec}(R)$*. Then, there exists* $f \notin \mathfrak{p}$ *such that* R_f *injects into* $R_\mathfrak{p}$*.*

Proof. If $R = 0$ then there is nothing to prove so we assume R is nonzero. Define $I := \ker(R \to R_\mathfrak{p}$, which is finitely generated since R is Noetherian. I consists precisely of $r \in R$ such that $ur = 0$ for some $u \notin \mathfrak{p}$, so I consists entirely of zero-divisors on R. By the previous corollary, there exists $f \in R$ such that I annihilates f. This is equivalent to the statement that R_f injects into $R_\mathfrak{p}$. □

5.8 Heights and Dimension

A **chain** of prime ideals is defined to be a sequence

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

in $\mathrm{Spec}(R)$. The integer n here is the **length** of the chain. Given $\mathfrak{p} \in \mathrm{Spec}(R)$, the **height** of $\mathfrak{p}$, denoted $\mathrm{ht}(\mathfrak{p})$, is the supremum of all lengths of chains of prime ideals ending with $\mathfrak{p}$. The **Krull dimension** of R, denoted $\dim R$, is in turn given by

$$\dim R := \sup_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathrm{ht}(\mathfrak{p}).$$

It is immediate that $\mathrm{ht}(\mathfrak{p}) = \dim R_\mathfrak{p}$.

If R is Noetherian then every prime ideal has finite height (this is a somewhat nontrivial fact that we will discuss in more detail below). There are examples, however, of Noetherian rings with infinite Krull dimension. We see immediately that fields have Krull dimension 0 since they have no proper nonzero ideals. PIDs which are not fields are also quickly seen to have Krull dimension 1.

Theorem 5.8.1 (Krull Principal Ideal Theorem)**.** *Let R be a Noetherian ring and $x \in R$ a non-unit. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be minimal among primes containing x. Then, $\operatorname{ht}(\mathfrak{p}) \leq 1$, with equality if x is a non-zero-divisor (NZD).*

The proof rests on the classification of Artinian rings, Krull's Intersection Theorem, and Nakayama's Lemma.

Krull's Principal Ideal Theorem admits a nice generalization. Let R be a Noetherian ring and $I = (x_1, \ldots, x_n)$ an ideal of R. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be minimal among primes containing I. Then, $\operatorname{ht}(\mathfrak{p}) \leq n$. When do we have equality? Precisely when $x_1, \ldots, x_n$ is a **regular sequence** – i.e., each x_i acts as an NZD on $R/(x_1, \ldots, x_{i-1})$. The geometry of regular sequences is captured in the notion of locally complete intersection.

Recall that $R \subseteq S$ is an integral extension of rings if every nonzero element of S satisfies a monic polynomial with coefficients in R. Our goal is to compare prime ideals, and thus chains of prime ideals, in both R and S. To that end, $\mathfrak{q} \in \operatorname{Spec}(S)$ is said to **lie over** $\mathfrak{p} \in \operatorname{Spec}(R)$ if $\mathfrak{q} \cap R = \mathfrak{p}$. $R \subseteq S$ has the **incomparability property** if, whenever $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec}(S)$ both lie above $\mathfrak{p} \in \operatorname{Spec}(R)$, neither of $\mathfrak{q}, \mathfrak{q}'$ is contained in the other (i.e., "they cannot be compared"). These notions all extend nicely to general ring maps $\varphi : R \to S$ with R playing the role of $\varphi(R)$ and preimages replacing intersections.

Theorem 5.8.2. *Let $\varphi : R \to S$ be an integral ring map. Let $\mathfrak{q} \in \operatorname{Spec}(S)$ lying over $\mathfrak{p} \in \operatorname{Spec}(R)$. Then, $\operatorname{ht}(\mathfrak{q}) \leq \operatorname{ht}(\mathfrak{p})$.*

It follows that $\dim S \leq \dim R$ for S an integral R-algebra.

Theorem 5.8.3 (Lying over)**.** *Let $\varphi : R \to S$ be an injective integral ring map. Then, $\varphi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ is surjective.*

Theorem 5.8.4 (Incomparability)**.** *Let $\varphi : R \to S$ be an injective integral ring map. Then, φ has the incomparability property.*

The notion of lying over extends easily to chains of prime ideals.

Theorem 5.8.5 (Going up)**.** *Let $\varphi : R \to S$ be an injective integral ring map. Let P be a chain of primes in R of length n and Q' a chain of primes in S of length m lying over (part of) P (so $m < n$). Then, Q' extends to a chain of primes Q of length n lying over P.*

By Incomparability and the Going up Theorem, maximal ideals in R correspond to maximal ideals in S and $\dim R = \dim S$. This is called the Going up Theorem because we work our way "up" the chain in the direction of ascending indices. One might also hope to work "down" the chain in the direction of decreasing indices. This is possible under more restrictive hypotheses.

Theorem 5.8.6 (Going down)**.** *Let $\varphi : R \to S$ be a ring map such that either of the following conditions is satisfied:*

(1) *φ endows S with a flat R-module structure.*

(2) *φ is injective integral and R, S are both normal integral domains.*

Then, φ has the going down property.

Lemma 5.8.7. *Let R be a Noetherian ring and $I \subseteq R$ an ideal generated by n elements.*

(a) *Let $\mathfrak{p}$ be a minimal prime over I. Then,* $\operatorname{ht}(\mathfrak{p}) \leq n$.

(b) *Suppose $(R, \mathfrak{m}, k)$ is also local. Then,* $\dim R$ *is finite with* $\dim R \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Statement (a) is the generalization of Krull's Principal Ideal Theorem mentioned above. Statement (b) follows directly from statement (a) and Nakayama's Lemma. If equality holds in (b) above then R is called a **regular** local ring.[2]

Lemma 5.8.8. *Let $(R, \mathfrak{m})$ be a Noetherian local ring with $f \in \mathfrak{m}$. Then,* $\dim R/f \geq \dim R - 1$, *with equality if f is not contained in any minimal prime ideal of R.*

Theorem 5.8.9. *Let R be a Noetherian ring, $\mathfrak{m} \subseteq R$ a maximal ideal, and $\mathfrak{n} \subseteq R[x_1, \ldots, x_n]$ a maximal ideal such that $\mathfrak{n} \cap R = \mathfrak{m}$. Then,*

$$\operatorname{ht}(\mathfrak{n}) = \operatorname{ht}(\mathfrak{m}) + n.$$

Corollary 5.8.10. *Given any ring R, we always have*

$$\dim R + 1 \leq \dim R[t] \leq 2 \dim R + 1,$$

with both bounds optimal. If R is Noetherian then $\dim R[t] = \dim R + 1$.

Computation of Krull dimension directly from the definition is sometimes quite challenging, so it is helpful to relate Krull dimension to other notions of dimension. A field extension K/k is said to be of **finite transcendence degree** if K is algebraic over a subextension isomorphic to $k(x_1, \ldots, x_d)$. The integer d is unique and is called the **transcendence degree** of K/k, written $\operatorname{trdeg}_k K$. The images of $x_1, \ldots, x_d$ form a **transcendence basis** for K. K is **purely transcendental** if it is isomorphic to $k(x_1, \ldots, x_d)$. By Noether's Normalization Lemma, the field of fractions of any finitely generated integral domain over k has finite transcendence degree.

Note that transcendence degree is additive on triples: given $k \subseteq K \subseteq L$ field extensions,

$$\operatorname{trdeg}_k L = \operatorname{trdeg}_K L + \operatorname{trdeg}_k K.$$

Theorem 5.8.11. *Let X be an integral algebraic k-variety and $U \subseteq X$ a nonempty open subvariety. Then,*

$$\dim U = \dim X = \operatorname{trdeg}_k K(X).$$

Theorem 5.8.12. *Let R be a finitely generated integral domain over a field k and $\mathfrak{p} \in \operatorname{Spec}(R)$.*

(1) *Suppose* $\operatorname{ht}(\mathfrak{p}) = 1$. *Then,* $1 + \dim R/\mathfrak{p} = \dim R$.

(2) *More generally,* $\operatorname{ht}(\mathfrak{p}) + \dim R/\mathfrak{p} = \dim R$.

(3) *Suppose $\mathfrak{p}$ is maximal. Then,* $\dim R_{\mathfrak{p}} = \dim R$.

[2] The vector space $\mathfrak{m}/\mathfrak{m}^2$ is the cotangent space of $\operatorname{Spec}(R)$ at $\mathfrak{m}$. This can be understood in more familiar terms using Jacobians. The cotangent space should be a local object, so it is a good thing that the natural map $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}R_{\mathfrak{m}}/\mathfrak{m}^2 R_{\mathfrak{m}}$ is an isomorphism.

Theorem 5.8.13. *Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a map of local rings. Then,*

$$\dim S \leq \dim R + \dim S/\mathfrak{m}S,$$

with equality if S is flat as an R-module.

Theorem 5.8.14 (Serre)**.** *Let R be a Noetherian integral domain. Then, R is a UFD if and only if every height 1 prime ideal in R is principal.*

Theorem 5.8.15 (Auslander-Buchsbaum)**.** *Let R be a regular local ring. Then, R is a UFD.*

5.9 DVRs

Definition 5.9.1. *A **discrete valuation ring** or **DVR** that is not a field is a ring A satisfying any of the following equivalent conditions.*

(i) *R is a local PID.*

(ii) *R is a Noetherian local domain with principal maximal ideal.*

(iii) *R is a normal Noetherian local ring with dimension 1.*

(iv) *R is a UFD with a unique irreducible element.*

(v) *R is a valuation ring with value group isomorphic to $\mathbb{Z}$.*

(vi) *There exists a discrete valuation v on $K = \operatorname{Frac} R$ such that $R = \{x \in K : v(x) \geq 0\}$.*

A somewhat nontrivial equivalent condition we can add to the mix is that R is a Noetherian regular local ring with dimension 1. This is a very geometrically significant condition because regularity is closely related to smoothness.

Yes, we like definition theorems in these notes! In case it is not obvious, fields are also DVRs. It should be clear that one of the many nice things about DVRs is that lots of properties come for free. Any generator of the maximal ideal is called a **uniformizer** or **uniformizing parameter**. Geometrically, such a parameter serves the role of a local coordinate. It is best to elaborate a bit more on valuation rings.

Definition 5.9.2. *A **valuation ring** is an integral domain R (with field of fractions K) satisfying any of the following equivalent conditions.*

(i) *Given $x \in K^\times$, either $x \in R$ or $x^{-1} \in R$.*

(ii) *The ideals of R are totally ordered by inclusion.*

(iii) *The principal ideals of R are totally ordered by inclusion.*

(iv) *There exists a totally ordered abelian group (**value group**) Γ and surjective group homomorphism (**valuation**) $v : K^\times \to \Gamma$ such that*

$$R = \{x \in K^\times : v(x) \geq 0\} \cup \{0\}.$$

One part of the correspondence is given by taking Γ to be $K^\times/R^\times$, taking v to be the natural projection map, and declaring residue classes of elements of R to be positive.

Example 5.9.3. *Here are some examples of valuation rings.*

- $k[\![x]\!] \subseteq k((x))$
- $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$
- $\mathbb{Z}_p \subseteq \mathbb{Q}_p$
- $\mathcal{O}_{X,p}$ *for* X *a scheme and* $p \in X$ *a regular point*

5.10 Some Algebraic Geometry

Theorem 5.10.1 (Noether's Normalization Lemma)**.** *Let A be a nonzero finitely generated algebra over a field k. Then, there exists an integer $d \geq 0$ and a finite injective homomorphism $k[y_1, \ldots, y_d] \hookrightarrow A$.*

The integer d is uniquely determined and is precisely the Krull dimension of A. If A is an integral domain then this is the transcendence degree of the field of fractions of A over k. This result can be refined somewhat.

Theorem 5.10.2. *Let $I \subseteq k[x_1, \ldots, x_n]$ be a proper ideal. Then, there exists a k-subalgebra $k[s_1, \ldots, s_n]$ of $k[x_1, \ldots, x_n]$ and an integer $0 \leq r \leq n$ such that:*

(a) *$k[x_1, \ldots, x_n]$ is finite over $k[s_1, \ldots, s_n]$;*

(b) *$k[s_1, \ldots, s_n] \cap I = (s_1, \ldots, s_r)$ (taken to be (0) if $r = 0$);*

(c) *$k[s_{r+1}, \ldots, s_n] \to k[x_1, \ldots, x_n]/I$ is finite injective.*

Corollary 5.10.3 (Zariski's Lemma)**.** *Let k be a field, A a finitely generated k-algebra, and $\mathfrak{m}$ a maximal ideal of A. Then, $A/\mathfrak{m}$ is a finite degree field extension of k. Equivalently, given any field extension K/k such that K is a finitely generated k-algebra, K/k is algebraic.*

Let $\mathbb{A}^n_k$ denote affine n-space over k. At the beginning we will think of this as k^n but it will eventually become apparent that this is the same as (the closed points of) $\mathrm{Spec}(k[x_1, \ldots, x_n])$. Geometrically, Noether's Normalization Lemma says that any affine variety is a branched covering of an affine space of the appropriate dimension.

Let $\mathcal{I}_n$ denote the set of ideals of $k[x_1, \ldots, x_n]$ and $\mathcal{S}_n$ the set of subsets of $\mathbb{A}^n_k$. Define $I : \mathcal{S}_n \to \mathcal{I}_n$ by

$$I(S) := \{f \in k[x_1, \ldots, x_n] : f|_S = 0\}$$

and $V : \mathcal{I}_n \to \mathcal{S}_n$ by

$$V(J) := \{x \in \mathbb{A}^n_k : f(x) = 0 \text{ for every } f \in J\}.$$

Proposition 5.10.4. *Let $S \in \mathcal{S}_n$ and $J \in \mathcal{I}_n$.*

(1) $V(J) = V(\sqrt{J})$.

(2) $I(S)$ *is radical.*

(3) $I(V(J))$ *is radical containing* $\sqrt{J}$*.*

If k is algebraically closed then $I(V(J)) = \sqrt{J}$ for every ideal J. In fact:

Theorem 5.10.5 (Nullstellensatz)**.** *Let k be an algebraically closed field. Then, I, V as above define an inclusion-reversing bijection between Zariski-closed subsets of $\mathbb{A}^n_k$ and radical ideals of $k[x_1, \ldots, x_n]$, with singleton sets corresponding to maximal ideals.*

It follows that $k[x_1, \ldots, x_n]/\mathfrak{m} \cong k$ for every maximal ideal $\mathfrak{m}$.

5.11 Normality and Regularity

Integrality is a transitive notion. Integral closure may not be (?).

An integral domain is **integrally closed** or **normal** if it is integrally closed in its field of fractions. The double use of the word integral and the appearance of the overused word normal are both unfortunate.

Example 5.11.1. *Here are some examples of normal rings.*

- *UFDs*
- *Localizations of normal rings at any multiplicative subset*
- $A[x]$ *for A normal*

This last example is worth unpacking in some detail. Let A be a normal domain with fraction field K. Then, $K(x)$ is the fraction field of $A[x]$. Let $f \in K(x)$ be integral over $A[x]$. Then, f is integral over $K[x]$ and so is contained in $K[x]$ (since $K[x]$ is Euclidean $\implies$ PID $\implies$ UFD $\implies$ normal). The coefficients of f are then integral over A and so contained in A – i.e., $f \in A[x]$.

Theorem 5.11.2. *Let R be a normal Noetherian local ring with* $\dim A = 1$*. Then, R is a PID.*

Theorem 5.11.3 (Algebraic Hartog's Lemma)**.** *Let A be a normal Noetherian ring with* $\dim A \geq 1$*. Then,*

$$A = \bigcap_{\mathrm{ht}(\mathfrak{p})=1} A_{\mathfrak{p}}.$$

Theorem 5.11.4. *Let R be an integral domain with field of fractions K and $R \subseteq S$ a ring extension. Given $s \in S$, let $p_s(t) \in K[t]$ be its minimal polynomial over K (defined relative to the field of fractions of S). If s is integral then $p_s(t)$ has coefficients in the integral closure of R in K. Moreover, R is integrally closed if and only $p_s(t)$ has coefficients in R for every $s \in S$ integral over R.*

Note that we can use any S that does the trick. What this tells us is that integrality for integral domains is detected by minimal polynomials.

Proposition 5.11.5. *Let R be an integral domain, K its field of fractions, L/K an algebraic extension, S the integral closure of R in L, and $G := \mathrm{Aut}(L/K)$. Let $\sigma \in G$ and $\mathfrak{q} \in \mathrm{Spec}(S)$.*

(a) $\sigma \in G \implies \sigma(S) = S$.

(b) $\sigma(\mathfrak{q}) \in \mathrm{Spec}(S)$.

(c) $\mathfrak{q} \cap R = \sigma(\mathfrak{q}) \cap R$.

5.12 Some Algebraic Number Theory

Definition 5.12.1. *Let L/K be a finite field extension (and so L is a K-vector space of finite dimension). Define $N_{L/K} : L \to L$ by $a \mapsto \det \mu_\alpha$, where $\mu_\alpha : L \to L$ is the K-linear map given by multiplication by α.*

Proposition 5.12.2. *Let L/K be a finite field extension. Then,*

(a) *the image of $N_{L/K}$ is contained in K;*

(b) *if $\alpha \in K$ then $N_{L/K}(\alpha) = \alpha^{[L:K]}$;*

(c) *$N_{L/K}$ defines a group homomorphism $L^\times \to K^\times$ and hence $N_{L/K}(L^\times) \leq K^\times$;*

(d) *given $K \subseteq E \subseteq L$, $N_{L/K} = N_{E/K} \circ N_{L/E}$;*

(e) *if L/K is Galois and $\alpha \in L$ then $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha$;*[3]

(f) *if L/K is separable and M is the Galois closure of L/K then $N_{L/K} = N_{M/K}|_L$.*

The $AKLB$ setup consists of A a Dedekind domain, K its fraction field, L a finite separable extension of K, and B the integral closure of A in L. Similarly, we have the $AKLBG$ setup in which L/K is additionally assumed to be Galois with Galois group G.

Theorem 5.12.3 (Dedekind-Kummer)**.** *Assume the $AKLB$ setup and let $\mathfrak{p} \in \mathrm{Spec}(A)$. Assume there is $\alpha \in B$ such that $L = K(\alpha)$ and $B = A[\alpha]$ (we can always satisfy the first assumption by the Primitive Element Theorem). Let $f \in A[x]$ be the minimal polynomial of α over K and $g_1, \ldots, g_r \in A[x]$ monic such that $\overline{f} = \overline{g_1}^{e_1} \cdots \overline{g_r}^{e_r}$ in $(A/\mathfrak{p})[x]$. Let $\mathfrak{q}_i$ be the ideal of B generated by $\mathfrak{p}$ and $g_i(\alpha)$. Then, $\mathfrak{p}B$ has prime factorization $\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ and the inertia degree of each $\mathfrak{q}_i$ is $f_i := \deg g_i$.*

[3] There are similar product expressions for the norm in the case that L/K is not separable but we will not need them.