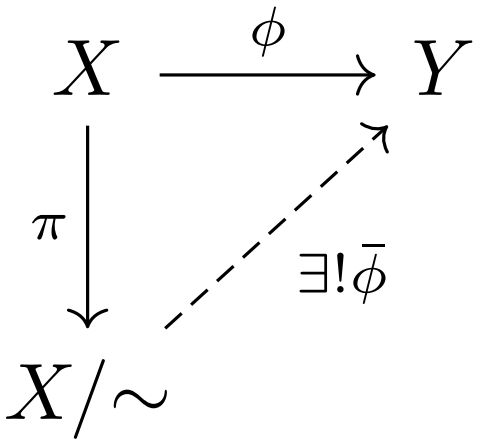
Notes on Algebra

at the Undergraduate Level

Boris Li



Last compiled: December 9, 2023

Foreword

Version 1.0

This document was written in the summer of 2023 for the purpose of helping myself review the material in various classes of algebra. It is based on Prof. Vatsal's MATH 322 (groups) & 323 (rings) in-class notes.

While this does not replace any course notes or the textbook, I have personally found Jacobson's *Basic Algebra* to be overly concise, with too many details hidden within singular paragraphs; and Herstein's *Topics in Algebra* sometimes overly verbose. I aim to lift out definitions from large proofs as to aid my own digestion of the material, and to ease the process of revisiting ideas from group theory.

Morgan suggests that Rotman's *An Introduction to the Theory of Groups* to be a useful book to self-learn from, while I have occasionally seen Justin pick up a copy of Lang's *Algebra* as reference. Both of these are good textbooks, but my current pick still goes to Dummit and Foote's *Abstract Algebra*, as I find it as a great reference book, with neatly numbered theorems, and detailed proofs; but it is currently out of print, so I presume the reader knows where to find such copies. Although I have never been one to absorb knowledge directly from textbooks, the reader must be way more diligent than I am, so go ahead and experiment, go find out the correct textbook for you.

To Madeline: I truly hope that you can find math as beautiful as I thought it is, and find understanding algebra for the first time to be less painful than when I understood it for the first time. I want you to be better at this than I ever was.

To Arsam: Maybe this one course will help you find your true place in math, and can help you decide the direction that you wish to pursue. While we may want rigour for the sake of understanding, it may sometimes get in the way of clarity; choose wisely when it comes to writing proofs.

To Morgan and Aryan: I know the pain of Jacobson not having a search-able PDF copy online, so hopefully this document comes in handy. Or you guys are just too smart and can memorize all those definitions first try.

Boris
August 24, 2023

Version 2.0

This document was continuously worked on over the 2023–2024 academic year in an attempt to fulfill my grand ambition to consolidate all of my knowledge in algebra learnt at the undergraduate level. The new sections are based on course material taught in Prof. Vatsal's MATH 323 (modules), Prof. Silberman's MATH 412 (linear algebra), and Prof. Ramdorai's MATH 422 (fields and Galois theory), with bits and pieces coming from Prof. Bryan's MATH 426 (topology).

A small token of thanks to Justin suggesting that the section on categories can be shifted earlier as to avoid reproving tedious amounts of theorems later on.

Boris
Date?

Contents

0 Prerequisite Material

Remark 0.0.1. There is a huge amount of prerequisite material that is needed, and it is never possible to study algebra independently of other subjects. We need skills like doing proofs by induction, contradiction, and contraposition, and we also need a basic understanding of numbers in general, and perhaps a good deal of geometric intuition would be nice; occasionally some proofs might also involve a non-trivial amount of analysis. But we need a starting point, and for me that starting point is the material that perhaps was never formally covered in Science One math and second year linear algebra and calculus, or maybe was a topic that was last taught in high school.

0.1 Relations

Definition 0.1.1. A relation is a denotion on two elements of a set X. More specifically, if a relation $R \subset X \times X$, then we write aRb if $(a, b) \in R$.

Definition 0.1.2. An equivalence relation $\sim$ is a relation that has three properties:

(i) reflexive $\forall x \in X, x \sim x$;

(ii) symmetric $\forall x, y \in X, x \sim y \implies y \sim x$; and

(iii) transitive $\forall x, y, z \in X, x \sim y \wedge y \sim z \implies x \sim z$.

We say x is related to y if $x \sim y$.

Definition 0.1.3. Suppose we have an equivalence relation $\sim$. The equivalence class of $x \in X$ is $[x] = \{y \in X : y \sim x\}$.

Lemma 0.1.4. An element is in its own equivalence class; $x \in [x]$.

Proof. By reflexivity.

Theorem 0.1.5. $x \sim y \iff [x] = [y]$; two related elements must have the same equivalence class.

Proof. If $x \sim y$, then $[x]$ consists of all elements z that are related to x, so $z \sim x$, and transitivity gives us $z \sim y$, so $z \in [y]$, and hence $[x] \subset [y]$. Reversing the argument gives us $[y] \subset [x]$, so $[x] = [y]$.

If $[x] = [y]$, then $y \in [x]$, so by definition $y \sim x$.

Corollary 0.1.6. For all elements $\{x, y\} \in X$, either $[x] = [y]$ or $[x] \cap [y] = \varnothing$.

Proof. Suppose $[x] \cap [y] \neq \varnothing$. Then there exists some element $z \in [x]$ and $z \in [y]$. But then $z \sim x$ and $z \sim y$, so $x \sim y$ by transitivity, which by our theorem gives $[x] = [y]$.

Theorem 0.1.7. The set of equivalence classes $X/\sim$ partition X.

Proof. From the lemma, each element must belong in an equivalence class. The above corollary tells us equivalence classes do not overlap.

0.2 Sets

Axiom 0.2.1 (Axiom of Choice)**.** Suppose we have a collection of nonempty sets $\{S_i\}_{i \in I}$ and I an index set; it is possible to form a set $\{x_i\}_{i \in I}$ such that $x_i \in S_i$. In other words, we can choose an element from every set no matter how many sets we have.

Definition 0.2.2. A partial order relation $\leq$ is a relation that has three properties:

(i) reflexive $x \leq x$;

(ii) antisymmetric $x \leq y \wedge y \leq x \implies x = y$; and

(iii) transitive $x \leq y \wedge y \leq z \implies x \leq z$.

Note that there possibly exists elements that are neither $x \leq y$ or $x \geq y$.

Definition 0.2.3. A partially ordered set, or a poset, is a tuple $(S, \leq)$, such that S is a set, and $\leq$ is a partial order relation. A totally ordered set is a poset $(S, \leq)$ with the additional condition that every pair of element x, y is comparable, so it can be $x \leq y$ or $x \geq y$ (or both).

Definition 0.2.4. A chain is a subset of a poset $(S, \leq)$ such that under the same order, the subset is totally ordered.

Axiom 0.2.5 (Zorn's Lemma)**.** A partially ordered set containing an upper bound for every chain must contain at least one maximal element.

Axiom 0.2.6 (Well-Ordering Principle)**.** Suppose $S \neq \varnothing$ is a set. There exists a well ordering on S, i.e. there exists a total order $\leq$ such that every nonempty subset $A \subseteq S$ has a smallest element $a \in A$ where $a \leq b$ for all $b \in A$.

Theorem 0.2.7. The above three axioms

(a) the axiom of choice;

(b) Zorn's lemma; and

(c) the well-ordering principle

are equivalent in Zermelo-Fraenkel set theory, and are independent from any other ZF axiom.

Proof. This is a result in set theory, and hence we shall omit the proof, and use the result as is.

0.3 Functions

Definition 0.3.1. A function f that maps elements in A to B is denoted $f\colon A \to B$. A is the domain, and B is the codomain. The range $f(A)$ is the set of all possible outputs of the function, namely $f(A) = \{b \in B : \exists a \in A, f(a) = b\}$.

Definition 0.3.2. Suppose $A' \subset A$ and $B' \subset B$. The image of A' is the set of all possible outputs given elements in A', denoted $f(A') = \{f(a) \in B : a \in A'\}$. The preimage of B' is the set of all possible inputs that result in an element in B', denoted $f^{-1}(B') = \{x \in A : f(x) \in B'\}$.

Definition 0.3.3. A function is 1-to-1 or injective when each point in the range (or codomain) only corresponds to (at most) one point in the domain. That is, $\forall x, y \in A, f(x) = f(y) \implies x = y$.

Definition 0.3.4. A function is onto or surjective when every point in the codomain corresponds to at least one point in the domain, i.e. the codomain is the range. That is, $\forall y \in B, \exists x \in A, f(x) = y$.

Definition 0.3.5. A function is bijective if it is both injective and surjective.

Theorem 0.3.6 (Pigeonhole Principle)**.** Suppose two finite sets A, B have the same cardinality $|A| = |B|$. Then $f\colon A \to B$ is injective if and only if it is surjective.

Proof. Suppose f is injective but not surjective. Then if $|A| = n$, then there are n elements in B that are in the range. Lack of surjectivity implies that there exists at least one element that is not in the range. Hence $|B| > n$, which is a contradiction.

Suppose f is surjective but not injective. Then if $|B| = n$, then there are at least n elements in A. But no injectivity implies there must be some two elements $x, y \in A$ that map to the same point $f(x) = f(y)$, which so forces us to conclude $|A| \geq n + 1$, which is a contradiction.

Theorem 0.3.7. Suppose $f = f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1$. If f is injective, then f_1 is injective.

Proof. Suppose, by way of contradiction, that f_1 is not injective. Then there exists x, y in the domain of f_1 such that $f_1(x) = f_1(y)$. But that implies $f(x) = f(y)$, which contradicts that f is injective.

Theorem 0.3.8. Suppose $f = f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1$. If f is surjective, then f_n is surjective.

Proof. Suppose, by way of contradiction, that f_n is not surjective. Then there exists y in the codomain of f_n such that for all x in the domain of f_n, $f_n(x) \neq y$. But then there exists y in the codomain of f such that $f(x) \neq y$, which contradicts that f is surjective.

0.4 Integers

Definition 0.4.1. Suppose we have integers a, b. The greatest common denominator, or gcd is the largest integer n such that $n \mid a$ and $n \mid b$. This is often denoted $\gcd(a, b)$ or simply (a, b). The least common multiple, or lcm is the smallest integer m such that $a \mid m$ and $b \mid m$. This is often denoted $\text{lcm}(a, b)$ or simply $[a, b]$.

Theorem 0.4.2 (Euclid's Lemma)**.** Suppose we have prime p and integers a, b. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Suppose $p \nmid a$. Since $p \mid ab$, there exists an integer q such that $pq = ab$.

We first prove the base case, supposing that $ab = 2$. Then the only prime that divides it is 2, and we know that $a = 1$ and $b = 2$, so clearly $p \mid b$.

Now proceeding by induction, suppose that all values smaller than ab are proven. If $p < a$, then $pq - pb = ab - pb$, which gives us $p(q - b) = (a - p)b$, i.e. $p \mid (a - p)b$. Notice that $p \nmid a - p$, and that $(a - p)b < ab$, so Euclid's lemma holds by the induction hypothesis. If $p > a$, then $pb - npq = pb - nab$, which gives us $p(b - nq) = (p - na)b$, i.e. $p \mid (p - na)b$. Notice that $p \nmid p - a$, and that there exists an n such that $(p - na)b < ab$, which completes our proof.

Remark 0.4.3. This is essentially how the Euclidean algorithm for finding gcd works. We know that by subtracting off the other number, the gcd does not change, which allows us to reduce the problem to a smaller case.

Theorem 0.4.4 (Bézout's Identity)**.** Suppose $\gcd(a, b) = d$. Then there exists $m, n \in \mathbb{Z}$ such that $ma+nb = d$. Moreover, for any $p, q \in \mathbb{Z}$ we have $d \mid pa + qb$.

Proof. Without loss of generality, let $a \leq b$. If $a = b$, then clearly $d = a = b$ which is in our desired form. If not, then since we know that we can find some $b - na \leq a$, which reduces the case down to a smaller number while always keeping the numbers that we are taking the gcd of in the form $ma + nb$. Eventually, d must equal one of these numbers.

Then we write $pa + qb = (p - m)a + (q - n)b + ma + nb = (p - m)a + (q - n)b + d$. Since $d \mid a$ and $d \mid b$, we have our desired result.

Remark 0.4.5. One might use Bézout's identity to prove Euclid's lemma, but both proofs essentially come from the Euclidean algorithm.

Theorem 0.4.6 (Fundamental Theorem of Arithmetic)**.** Every integer greater than 1 factors uniquely into a product of primes. That is, we can write any integer $n > 1$ as

$$n = \prod_{i=1}^{k} p_i^{n_i}$$

where p_i are distinct primes.

Proof. We first prove such a prime factorization exists. We can see that 2 is prime. Proceeding by induction, assume all integers between 2 and n have a prime decomposition. If n is prime, we are done. If n is not prime, then it must be represented by $n = ab$, where a, b must both be smaller, and by the inductive hypothesis, have prime decompositions.

Now we prove that prime factorization is unique. Assume the contrary, and let n be the smallest such integer without unique factorization. Then we write $n = \prod_{i=1}^{k} p_i = \prod_{i=1}^{k'} q_i$, two distinct factorizations. By Euclid's lemma we see that p_1 divides some q_i, which without loss of generality say this is q_1. Then $p_1 = q_1$. So $n/p_1 = \prod_{i=2}^{k} p_i = \prod_{i=2}^{k'} q_i$ is also an integer without unique factorization, which contradicts our assumption that n is the smallest.

1 Groups

1.1 Basic Definitions

Definition 1.1.1. A group is a triple $(G, \cdot, 1)$, where $G \neq \varnothing$ is a set equipped with a multiplicative operation $\cdot$ with an identity 1, with these four properties:

(i) closure $\cdot\colon G \times G \to G$;

(ii) associativity $\forall \{a, b, c\} \subset G, (ab)c = a(bc)$;

(iii) identity $\exists 1 \in G, \forall g \in G, 1g = g1 = g$; and

(iv) inverse $\forall g \in G, \exists h \in G, gh = hg = 1$, which we usually denote $g^{-1} = h$.

Remark 1.1.2. If we think of groups as objects that we use to describe actions that preserve symmetry, these are exactly the four criteria that we require: any composition of two actions must also be an action (closure), you must be able to compose actions in any order (associativity), the act of doing nothing preserves symmetry (identity), and reversing an action also preserves symmetry (inverse).

Definition 1.1.3. A monoid is a triple $(X, \cdot, 1)$, where $X \neq \varnothing$ is a set equipped with a multiplicative operation $\cdot$ with an identity 1, with the first three properties of a group, that is, closure, associativity, and identity.

Definition 1.1.4. Suppose G is a group. The order of an element $g \in G$ is the smallest positive integer n such that $g^n = 1$. If no such n exists, we say the order of g is infinite. This is often denoted $|g| = \operatorname{ord} g = \#g = n$.

Definition 1.1.5. The order of a group G, also the cardinality of a group, is the number of elements in a group G. If G has infinitely many elements, we say the order of G is infinite. This is often denoted $|G| = \operatorname{ord} G = \#G$.

Definition 1.1.6. The exponent of a group G is $\exp(G) = \operatorname{lcm}\{|g| : g \in G\}$, the least common multiple of the orders of all elements of G.

Definition 1.1.7. A commutative group or an abelian group is a group G with a commutative operation $\cdot$, that is, $gh = hg$ for all $\{g, h\} \subset G$.

Remark 1.1.8. We sometimes denote abelian groups with additive notation, where $(G, +, 0)$ is a group.

1.2 Transformation Groups

Definition 1.2.1. Suppose we have a set X. G is a group of transformations on X if all elements of G are bijective functions that map $X \to X$, with multiplication being function composition.

Remark 1.2.2. It is worth remembering that X can be any set. Sometimes X indeed carries more structure, namely being a group X, but remember that a group is but a set of elements with some additional rules.

Definition 1.2.3. The rotations and reflections on an n-gon trivially form a transformation group. These are transformations on n vertices that preserve adjacency. This is often denoted as D_n, the dihedral group of an n-gon.

Proposition 1.2.4. D_n is a group of order $|D_n| = 2n$, with elements

$$D_n = \{1, \tau, \tau^2, \ldots, \tau^{n-1}, \sigma, \sigma\tau, \sigma\tau^2, \ldots, \sigma\tau^{n-1}\}$$

in which $\tau^n = \sigma^2 = 1$ and $\sigma\tau = \tau^{-1}\sigma$.

Proof. We think of τ as a rotation by $2\pi/n$, and σ as a reflection.

We prove that all such elements are distinct. Clearly by definition, all τ^j are distinct when $j \in [0, n-1]$. Moreover, all $\sigma\tau^j$ are distinct when $j \in [0, n-1]$ because if $\sigma\tau^i = \sigma\tau^j$, then $\sigma^2\tau^i = \sigma^2\tau^j$, which implies $\tau^i = \tau^j$. Lastly, if $\sigma\tau^i = \tau^j$, then $\sigma\tau^i\tau^{-j} = \tau^j\tau^{-j} = 1$, which would imply there is $\sigma = \tau^{j-i}$, a contradiction, as reflections are not rotations.

With this, we also prove that all $\sigma\tau^j$ are reflections.

Definition 1.2.5. A (group) homomorphism or a homomorphic function is $\phi\colon G_1 \to G_2$, where G_1, G_2 are groups, with the properties that $\phi(gh) = \phi(g)\phi(h)$, and $\phi(1)$ is the identity on G_2. ϕ provides a correspondence between the multiplication in G_1 and G_2. We call the set of all homomorphisms between G_1 and G_2 the hom-set $\mathrm{Hom}(G_1, G_2)$.

Definition 1.2.6. Injective homomorphisms are called monomorphisms. Surjective homomorphisms are called epimorphisms. And most importantly, bijective homomorphisms are called isomorphisms. Two groups G, H that are isomorphic to each other are denoted $G \cong H$.

Definition 1.2.7. Isomorphisms that map $G \to G$ are called automorphisms; the set of all automorphisms of G is the automorphism group $\mathrm{Aut}(G)$. The homomorphism that map a group $G \to \{1\}$ by mapping all elements to 1 is called the trivial homomorphism.

Theorem 1.2.8 (Cayley's Theorem)**.** Suppose G is a finite group. Then we can find a set X such that G can be represented as a transformation group on X. More specifically, we can find a transformation group H on X such that $G \cong H$.

Proof. We consider $X = G$, i.e. G potentially being isomorphic to a group that transforms all elements of itself.

We first define a function $\ell_a\colon G \to G,\ x \mapsto ax$, which we choose some a that multiply some element $x \in G$ on the left. This is clearly a permutation on G, i.e. it is a bijection $G \to G$, because if $\ell_a(x) = \ell_a(y)$ for some $\{x, y\} \subset G$ hence $ax = ay$, then $a^{-1}ax = a^{-1}ay$, and $x = y$, which proves that this is an injection; the pigeonhole principle proves that this is a surjection.

For every element $g \in G$, we can create a function ℓ_g. We let $H = \{\ell_g : g \in G\}$ be the set of all such left permutations. We claim that H is a group, with function composition as multiplication, and ℓ_1 being the identity. We have closure because $\ell_a\ell_b$ will map $x \mapsto bx \mapsto abx$, which is equivalent to ℓ_{ab}. Function composition is naturally associative, so we get that for free. The inverse mapping from $ax \to x$ is achieved by left multiplying by a^{-1}, which itself is equivalent to $\ell_{a^{-1}}$. Lastly, the identity works, because $\ell_a\ell_1$ maps $x \mapsto 1x = x \mapsto ax$ which is equivalent to ℓ_a, and similarly with $\ell_1\ell_a = \ell_a$.

We then want to prove that the mapping from $a \to \ell_a$ is an isomorphism. Suppose $\phi\colon G \to H,\ a \mapsto \ell_a$. This is a homomorphism because

$$\phi(ab) = \ell_{ab} = \ell_a\ell_b = \phi(a)\phi(b)$$

And by construction, this is a bijection, because if $\phi(a) = \phi(b)$, then $\ell_a = \ell_b$, which implies $ax = bx$ for all $x \in G$, and hence $axx^{-1} = bxx^{-1}$, so $a = b$, which gives us injectivity; the pigeonhole principle again gives us surjectivity.

We have now found a transformation group H that acts on a set G, and that G is isomorphic to the transformation group H.

Remark 1.2.9. One can repeat the entire proof with right multiplication instead, it is equally valid.

1.3 Cyclic Groups

Definition 1.3.1. Suppose G is a group. A subgroup H of G is a subset $H \subseteq G$, with $1 \in H$, and properties of a group hold. We call the group $\{1\}$ the trivial subgroup.

Definition 1.3.2. Suppose we have a group G, and some non-empty subset $S \subseteq G$. The subgroup generated by S is the group of all elements that can be formed by the products of elements in S and their inverses. We denote it as $\langle S\rangle = \{\prod_i s_i : s_i \in S \vee s_i^{-1} \in S\}$.

Remark 1.3.3. One can think of this as almost like how a vector space spanned by a set of basis vectors.

Lemma 1.3.4. Suppose G is a group, and $H_i \subseteq G$ subgroups. Then $\bigcap_i H_i$ is also a subgroup of G.

Proof. If $\{a, b\} \subset \bigcap_i H_i$, then $\{a, b\} \subset H_i$ for all i, and hence $ab \in H_i$, which gives us closure $ab \in \bigcap_i H_i$.
Associativity is inherited from G.
The identity must be in each of H_i, so it must also be in $\bigcap_i H_i$.
Lastly, if $a \in \bigcap_i H_i$, then $a \in H_i$ for all i, so $a^{-1} \in H_i$ for all i, so we have inverses as $a^{-1} \in \bigcap_i H_i$.

Proposition 1.3.5. $\langle S\rangle = \bigcap_i H_i$, where H_i is any subgroup of G containing S.

Proof. We first need to prove that $\bigcap_i H_i \subseteq \langle S\rangle$, which it is sufficient to prove that $\langle S\rangle$ is any subgroup of G containing S, i.e. $\langle S\rangle$ corresponds to some H_i, since the intersection must be contained in any H_i. It is trivial to see that $1 \in \langle S\rangle$ by choosing $s_2 = s_1^{-1}$, which gives us 1. Closure and associativity is inherited from G, so we need not prove anything. Inverses exist since it is easy to check that $(s_1 s_2 \dots s_n)^{-1} = s_n^{-1} \dots s_2^{-1} s_1^{-1}$. Hence $\langle S\rangle \subseteq G$ is a subgroup, which must contain S by construction.

We then see that $H_i \subseteq G$, so every element of $\langle S\rangle$ is in H_i, as it is closed under multiplication and inversion. Hence we have $\langle S\rangle \subseteq \bigcap_i H_i$, and subsequently $\langle S\rangle = \bigcap_i H_i$.

Definition 1.3.6. Suppose we have a group G, and some element $g \in G$. The subgroup generated by one element, otherwise known as the cyclic group generated by g, is denoted $\langle g\rangle = \{g^n : n \in \mathbb{Z}\}$.

Proposition 1.3.7. Cyclic groups are abelian.

Proof. g will always commute with itself.

Theorem 1.3.8. Cyclic groups of the same order (finite or infinite) are isomorphic.

Proof. Suppose we have a cyclic group $\langle g\rangle$. We first attempt to construct a homomorphism $\phi\colon (\mathbb{Z}, +, 0) \to \langle g\rangle,\ n \mapsto g^n$. A quick proof shows us that it is indeed a homomorphism, with $\phi(0) = g^0 = 1$, and

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n)$$

We also see that this is surjective by construction, but not necessarily injective, if the order of g is finite.

We first consider the case of infinite order of g. Then it is clear that no two integers will map to the same element, and hence ϕ is injective, and therefore and isomorphism. This proves the part where we claim that all infinite cyclic groups are isomorphic, and specifically with $(\mathbb{Z}, +, 0)$.

We now consider some g with order $|g| = d$. Then clearly $\phi(d) = \phi(0) = g^d = 1$, which shows us that ϕ is not injective. We can however show that $\{1, g, g^2, \dots, g^{d-1}\}$ are all distinct, which proves that $(\mathbb{Z}/d\mathbb{Z}, +, 0) \cong \langle g\rangle$. We proceed by contradiction, assuming that there exists some $0 \le i < j < d$ such that $g^i = g^j$. But then we know $g^{j-i} = g^j g^{-i} = g^i g^{-i} = 1$, which tells us there exists some number $j - i < d$ such that $g^{j-i} = 1$, contradicting that $|g| = d$. Hence all cyclic groups with order d are isomorphic to $\mathbb{Z}/d\mathbb{Z}, +, 0$, which in turn are isomorphic to each other.

Definition 1.3.9. C_n is the cyclic group with order $|C_n| = n$. It is also sometimes denoted $C_n = Z_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n) = \mathbb{Z}/n$.

Theorem 1.3.10. Any subgroup of a cyclic group is cyclic. In particular, if $H \subseteq G$ a finite cyclic group, $|H| \mid |G|$.

Proof. Suppose $G = \langle g\rangle$ is generated by this element. Then all elements of H can be written as some power of g. We pick the smallest such integer s such that $g^s \in H$. We claim that $H = \langle g^s\rangle$. No matter what element we pick in H, we can write it as $g^{s'}$. Via long division, we write $s' = qs + r$, with $0 \le r < s$, so we know our element is $g^{s'} = g^{qs+r} = (g^s)^q g^r$. Since $g^s \in H$, by closure we have $(g^s)^q \in H$; which gives us $g^r = ((g^s)^q)^{-1} g^{s'} \in H$. But if $r \neq 0$, we will have found a smaller integer than s such that $g^r \in H$, which itself is a contradiction. We are then forced to conclude that $r = 0$, so all elements in H must be written as $g^{s'} = g^{qs} = (g^s)^q \in \langle g^s\rangle$, and hence $H \subseteq \langle g^s\rangle$. But obviously, $g^s \in H$, so $(g^s)^q \in H$, and we have $\langle g^s\rangle \subseteq H$. We then have our claim of equality $H = \langle g^s\rangle$, which is generated by a single element.

For the second part of the theorem, it is sufficient to prove that $|g^s| \mid |g|$. Suppose $|g^s| = d$ and $|g| = n$. Then we know that $g^{sd} = 1$, which we apply long division on. $sd = qn + r$, with $0 \le r < n$, so $g^{sd} = g^{qn} g^r = (g^n)^q g^r = g^r = 1$, which gives us $r = 0$, because r is smaller than the order of g. This tells us that $sd \mid n$. Now, we know that d is the smallest number that we need to multiply s by to obtain a multiple of n, which tells us d is the product of all the factors that n has, but s has not (counted with multiplicity). A simple decomposition of $n = \gcd(s, n) \cdot n/\gcd(s, n)$ tells us that the gcd must be the factors that n and s share, so the other part must be the ones n has, but s has not, meaning $d = n/\gcd(s, n)$. But by definition, these are factors of n, so $d \mid n$.

Corollary 1.3.11. $|g^s| = |g|/\gcd(s, |g|)$.

Remark 1.3.12. The above theorem gives us the ability to find the order of a given subgroup of a cyclic group. But to do the reverse, given an order finding a subgroup, each order might correspond to multiple generators, which means we need to prove the next theorem.

Theorem 1.3.13. Suppose $G = \langle g \rangle$, with $|g| = n$. Given that $d \mid n$, the subgroup of order d is unique.

Proof. Let $s = n/d$. We first see that $H = \langle g^s \rangle$ is one such subgroup of order d, since the corollary gives us $|H| = n/\gcd(n/d, n) = n/\gcd(n/d) = d$.

Now suppose we have another subgroup $H' \subseteq G$ with order d. Then from the above theorem, we know that $H' = \langle g^{s'} \rangle$ is cyclic. By the corollary, we get

$$d = \frac{n}{\gcd(n, s')} \implies s = \frac{n}{d} = \gcd(n, s')$$

with $s \mid s'$ by definition of gcd. Hence s' is a multiple of s, so $g^{s'} \in H$, and therefore $H' \subseteq H$. But as the orders are the same, the pigeonhole principle gives us $H' = H$.

Theorem 1.3.14. Suppose g and h commute ($gh = hg$), with $m = |g|$, $n = |h|$, m, n coprime ($\gcd(m, n) = 1$). Then $|gh| = mn = |g||h|$.

Proof. Let $d = |gh|$. We first notice that $(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = 1$, so $d \mid mn$.

Now we claim that mn is minimal. Suppose we have a $0 < d < mn$ such that $(gh)^d = g^d h^d = 1$, so we know that $g^d = h^{-d}$. Since their orders are coprime, unless one of the groups is $\{1\}$, they are not subgroups of each other, so we have $1 = g^d = h^{-d}$, and $m \mid d$ and $n \mid d$. But then d must be some multiple of $\operatorname{lcm}(m, n) = mn$, which is impossible within the range $0 < d < mn$. Hence $d = mn$.

Remark 1.3.15. In general, g and h will not commute, so it is impossble to relate $|gh|$ to $|g||h|$, since you would have to understand the groups $\langle g \rangle$ and $\langle h \rangle$ together.

1.4 Permutations

Definition 1.4.1. Let $X = \mathbb{N}_n = \{1, 2, 3, \ldots, n\}$ a set (any set) of n elements. We call a bijective function $\sigma \colon X \to X$ a permutation.

Proposition 1.4.2. The set of all possible permutations, with function composition as multiplication and the identity mapping as the identity, forms a group of order $n!$.

Proof. It is easy to see that the composition of two bijections is also a bijection, which gives us closure. We inherit associativity from function composition, and the identity mapping works as intended on both the left and the right side. Lastly, the inverse of a bijection must also be a bijection.

To count all the ways we can construct such permutations, we see that for any given σ, there are n possible elements that we can map 1 to, and after that choice is taken, $n - 1$ possible elements that we can map 2 to, and so forth until there is only one choice for what we can map n to. This gives us a total of $n(n-1)\ldots(2)(1) = n!$ choices.

Definition 1.4.3. It is clear that the groups of permutations of any two sets of n items are isomorphic to each other. We call this group S_n, the symmetric group of n elements.

Definition 1.4.4. We can write elements of S_n as disjoint cycles $(a_1 a_2 \ldots a_p)\ldots(b_1 b_2 \ldots b_q)$ where this permutation will map $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, and so on until $a_p \to a_1$, repeating this process for every cycle. We will often omit cycles of length 1.

Remark 1.4.5. It is worth noting that disjoint cycles commute.

Definition 1.4.6. We call $\tau = (ab)$ a cycle of two elements a flip or a transposition.

Lemma 1.4.7 (Breaking the cycle)**.** Suppose $\rho = (ac_1 \dots c_m b d_1 \dots d_n)$ is a cycle of length $m+n+2$. Then $\rho = (ab)(ac_1 \dots c_m)(bd_1 \dots d_n)$.

Proof. This is equivalent to proving that $(ab)\rho = (ac_1 \dots c_m)(bd_1 \dots d_n)$. We can see that ρ maps the following way, so $(ab)\rho$ must simply swap all occurrences of a with b in the results, and vice versa.

$$\rho = \begin{cases} a \mapsto c_1 & \\ c_i \mapsto c_{i+1} & i < m \\ c_m \mapsto b & \\ b \mapsto d_1 & \\ d_j \mapsto d_{j+1} & j < n \\ d_n \mapsto a & \end{cases} \qquad (ab)\rho = \begin{cases} a \mapsto c_1 & \\ c_i \mapsto c_{i+1} & i < m \\ c_m \mapsto a & \\ b \mapsto d_1 & \\ d_j \mapsto d_{j+1} & j < n \\ d_n \mapsto b & \end{cases}$$

Theorem 1.4.8. Any $\sigma \in S_n$ is a non-unique product of transpositions.

Proof. We write $\sigma = \gamma_1 \dots \gamma_n$ as disjoint cycles. We now decompose each of γ_i. First suppose γ_i is a transposition already. Then there is no need to do anything.

Now suppose $\gamma_i = (abc)$ is of length 3. Then by our lemma above, $\gamma_i = (ac)(ab)(c) = (ac)(ab)$ and we have a product of transpositions.

Then suppose $\gamma_i = (abcd)$ is of length 4. By our lemma above, $\gamma_i = (ac)(ab)(cd)$ and we have a product of transpositions.

Applying the induction step, assume that $\gamma_i = (abc_1 \dots c_n)$ is a cycle of $n+2$, and the case of cycles of length n is already proven. Then we know by our lemma $\gamma_i = (ac_1)(ab)(c_1 \dots c_n)$, so we have two transpositions and a cycle of length n, which by the inductive hypothesis can be decomposed into transpositions.

This representation is not unique, since if $\sigma = \tau_1 \dots \tau_n$, and τ' is another transposition, we can write $\sigma = \tau'\tau'^{-1}\tau_1 \dots \tau_n = \tau'\tau'\tau_1 \dots \tau_n$ a different representation.

Proposition 1.4.9. Suppose $\sigma \in S_n$. Then $\sigma(n_1 n_2 \dots n_d)\sigma^{-1} = (\sigma(n_1)\sigma(n_2) \dots \sigma(n_d))$.

Proof. Since all σ can be written a a product of transpositions (Theorem 1.4.8), it is sufficient to consider $\tau(n_1 n_2 \dots n_d)\tau^{-1}$. Suppose we have $(ab)\rho(ab)$, and $\rho = (ac_1 \dots c_m b d_1 \dots d_n)$ Then we have

$$(ab) = \begin{cases} a \mapsto b \\ c_i \mapsto c_i \\ b \mapsto a \\ d_j \mapsto d_j \end{cases} \qquad \rho(ab) = \begin{cases} a \mapsto d_1 & \\ c_i \mapsto c_{i+1} & i < m \\ c_m \mapsto bb \mapsto c_1 & \\ d_j \mapsto d_{j+1} & j < n \\ d_n \mapsto a & \end{cases}$$

which in cycle notation is $\rho(ab) = (ad_1 \dots d_n)(bc_1 \dots c_m)$, and if we break the cycle we get $(ab)\rho(ab) = (ad_1 \dots d_n b c_1 \dots c_m)$ which is exactly as desired, swapping the positions of a and b.

Definition 1.4.10. Suppose $\sigma = \gamma_1\gamma_2 \dots \gamma_n$ is a permutation written in disjoint cycle notation, with γ_i having length d_i. Then we define the sign of the permutation as

$$\operatorname{sgn}(\sigma) = (-1)^{\sum_{i=1}^{n}(d_i - 1)} = \prod_{i=1}^{n} (-1)^{(d_i - 1)}$$

If $\operatorname{sgn}(\sigma) = 1$, σ is called even; conversely, if $\operatorname{sgn}(\sigma) = -1$, σ is called odd.

Remark 1.4.11. It is worth noting that cycles of odd length are even, and cycles of even length are odd. Then cycles of length 1 (identity) are even, so it does not change sign.

Proposition 1.4.12. Suppose $\tau = (ab)$ is a transposition, and $\sigma \in S_n$. Then $\operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}(\sigma)$.

Proof. We write $\sigma = \gamma_1 \dots \gamma_r$ as disjoint cycles, inclding 1-cycles. We first consider the case that a, b are in the same cycle, so without loss of generality let a, b be in γ_1, which has length $m+n+2$. Then we have, by the lemma

$$\tau\sigma = (ab)(ac_1 \dots c_m bd_1 \dots d_n)\gamma_2 \dots \gamma_r = (ac_1 \dots c_m)(bd_1 \dots d_n)\gamma_2 \dots \gamma_r$$
$$\operatorname{sgn}(\tau\sigma) = (-1)^m(-1)^n \prod_{i=2}^{r}(-1)^{(d_i-1)} = (-1)^{m+n}\prod_{i=2}^{r}(-1)^{(d_i-1)} = -(-1)^{m+n+1}\prod_{i=2}^{r}(-1)^{(d_i-1)} = -\operatorname{sgn}(\sigma)$$

Now consider the case that a, b are in different cycles, so without loss of generality let a be in γ_1 of length $m+1$, and b be in γ_2 of length $n+1$. By the lemma again

$$\tau\sigma = (ab)(ac_1 \dots c_m)(bd_1 \dots d_n)\gamma_3 \dots \gamma_r = (ac_1 \dots c_m bd_1 \dots d_n)\gamma_3 \dots \gamma_r$$
$$\operatorname{sgn}(\tau\sigma) = (-1)^{m+n+1}\prod_{i=3}^{r}(-1)^{(d_i-1)} = -(-1)^{m+n}\prod_{i=3}^{r}(-1)^{(d_i-1)} = -(-1)^m(-1)^n\prod_{i=2}^{r}(-1)^{(d_i-1)} = -\operatorname{sgn}(\sigma)$$

Corollary 1.4.13. Suppose $\sigma = \tau_1\tau_2\cdots\tau_k$ written as a product of transpositions. Then $\operatorname{sgn}(\sigma) = (-1)^k$.

Proof. $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1\tau_2\cdots\tau_k) = (-1)\operatorname{sgn}(\tau_2\cdots\tau_k) = \cdots = (-1)^{k-1}\operatorname{sgn}(\tau_k) = (-1)^k$

Remark 1.4.14. Since the sign of a permutation is either odd or even, this tells us that the number of transpositions might not be unique, but whether there are an odd or even number of them is inherent to each permutation.

Theorem 1.4.15. $\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$.

Proof. Suppose $\sigma_1 = \tau_1 \dots \tau_m$, and $\sigma_2 = \tau_1' \dots \tau_n'$. Then by the corollary above,

$$\begin{aligned}\operatorname{sgn}(\sigma_1\sigma_2) &= \operatorname{sgn}(\tau_1 \dots \tau_m\tau_1' \dots \tau_n') = (-1)^{m+n} = (-1)^m(-1)^n \\ &= \operatorname{sgn}(\tau_1 \dots \tau_m)\operatorname{sgn}(\tau_1' \dots \tau_m') = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)\end{aligned}$$

Corollary 1.4.16. The even permutations form a subgroup of S_n.

Proof. Suppose σ_1, σ_2 are both even, Then since $\operatorname{sgn}(\sigma_1) = \operatorname{sgn}(\sigma_2) = 1$, we have $\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2) = 1$. We have closure.

The identity is also even, because $\operatorname{sgn}(\sigma) = \operatorname{sgn}(1\sigma) = \operatorname{sgn}(1)\operatorname{sgn}(\sigma)$, which gives us $\operatorname{sgn}(1) = 1$, an even permutation.

Lastly, if σ is even, then σ^{-1} is too, because if $\sigma = 1$, then $1 = \operatorname{sgn}(1) = \operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma^{-1})$.

Definition 1.4.17. We call the subgroup of even permutations of S_n the alternating group of n elements, usually denoted as A_n.

1.5 Cosets

Proposition 1.5.1. Suppose G is a transformation group of some set X. For any $\{x, y\} \subset X$, if we define a relation $x \sim y$ to be when there exists some $g \in G$ such that $g(x) = y$, such a relation is an equivalence relation.

Proof. This is reflexive because $1 \in G$, and $1(x) = x$, so $x \sim x$. This is symmetric because suppose $x \sim y$, then there exists some $g \in G$ such that $g(x) = y$; it is easy to see that then $g^{-1}(y) = x$, so we have $y \sim x$. This is transitive because if $x \sim y$ and $y \sim z$, then there exists $g(x) = y$ and $h(y) = z$, and since $hg \in G$, $(hg)(x) = h(y) = z$, so $x \sim z$.

Definition 1.5.2. We call the equivalence class of $x \in X$ the orbit of x, which is often denoted as $\text{orb}(x) = Gx = \{g(x) : g \in G\}$. If this is the entire set, i.e. there exists some $x \in X$ (and therefore all $x \in X$ by Theorem 0.1.7) such that $Gx = X$, we call G a transitive transformation group.

Proposition 1.5.3. Suppose G is a group, and $H \subseteq G$ some subgroup. For any $\{g_1, g_2\} \subset G$, if we define a relation $g_1 \sim g_2$ to be when there exists some $h \in H$ such that $g_2 = g_1 h$, such a relation is an equivalence relation.

Proof. This is reflexive because $1 \in H$, and $g_1 = g_1 1$, so $g_1 \sim g_1$. This is symmetric because suppose $g_1 \sim g_2$, then there exists $h \in H$ such that $g_2 = g_1 h$; it is easy to see that $g_1 = g_2 h^{-1}$, so we have $g_2 \sim g_1$. This is transitive because if $g_1 \sim g_2$ and $g_2 \sim g_3$, then there exists h_1 and h_2 such that $g_2 = g_1 h_1$ and $g_3 = g_2 h_2$, so $g_3 = g_1 h_1 h_2$, and hence $g_1 \sim g_3$.

Definition 1.5.4. We call the equivalence class of $g \in G$ a left coset of H in G, which is denoted $gH = \{gh : h \in H\}$. We can similarly define a right coset of H in G, which is denoted $Hg = \{hg : h \in H\}$.

Definition 1.5.5. The set of all left cosets is denoted G/H, while the set of all right cosets is denoted $H\backslash G$.

Definition 1.5.6. The number of left cosets is called the index of H in G and is denoted $|G/H| = [G : H]$.

Lemma 1.5.7. Suppose G a group, and $H \subseteq G$ some subgroup. Then for any $g \in G$, the cosets are the same size, and in particular $|gH| = |H|$.

Proof. We write the left multiplication function $\ell_g \colon H \to gH$, $h \mapsto gh$. We can show that it is injective, because if $gh_1 = gh_2$, then $g^{-1}gh_1 = g^{-1}gh_2$, so $h_1 = h_2$. We can also show that it is surjective, because for every element $gh \in gH$, clearly $h \mapsto gh$ and $h \in H$ by definition. Hence ℓ_g is a bijection, which shows that $|H| = |gH|$.

Theorem 1.5.8 (Lagrange's Theorem)**.** For some finite group G, and $H \subseteq G$ any subgroup, $|G| = |H|[G : H]$.

Proof. By definition, there are a total of $[G : H]$ cosets, and the subgroup itself is a coset $H = 1H$. Since cosets are equivalence classes, they partition G, so the order of G must be the sum of the orders of the cosets. But we also know that all the cosets are the of size $|H|$ from the lemma above, so we have $|G| = |H|[G : H]$.

Corollary 1.5.9. Suppose $|G| = p$ some prime order. Then if $H \subseteq G$ is a subgroup, either $H = \{1\}$ or $H = G$, and in the second case, H is generated by any element $g \in G$ when $g \neq 1$.

Proof. Since from the theorem above we have $|H| \mid |G|$, $|H|$ is either 1 or p. If $|H| = 1$, since all groups must have the identity, $H = \{1\}$.

On the other hand, if $|H| = p$, then it must be the whole group, so $H = G$. Now pick any $g \in G$. We know that $\langle g \rangle \subseteq G$ is a subgroup, and if $g \neq 1$, we cannot have $\langle g \rangle = \{1\}$, so we are forced to conclude otherwise, and we have $\langle g \rangle = G$.

Corollary 1.5.10. Suppose G is a finite group, with $g \in G$. If $n = |G|$, then $g^n = 1$.

Proof. Suppose $|g| = m$, so $g^m = 1$. By the theorem above, we know that $m \mid n$, so there exists some $r \in \mathbb{N}$ such that $n = mr$. Hence $g^n = g^{mr} = (g^m)^r = 1^r = 1$.

Corollary 1.5.11. $|A_n| = n!/2$.

Proof. The even and odd permutations form two cosets in S_n, since multiplying by even permutations (and hence by elements of A_n) do not change sign by Theorem 1.4.15. Then we have $|S_n| = |A_n|[S_n : A_n]$, so $|A_n| = |S_n|/2 = n!/2$.

1.6 Normal Subgroups

Definition 1.6.1. Suppose G is a group, and $H \subseteq G$ some subgroup. H is a normal subgroup of G if for all $g \in G$ and $h \in H$, $ghg^{-1} \in H$. We often denote this as $H \lhd G$.

Theorem 1.6.2. If $H \lhd G$, then the set of left cosets G/H forms a group, and in particular, there exists a epimorphism from G to G/H.

Proof. We attempt to write a function $\phi\colon G \to G/H$, $g \mapsto gH$ that maps every element into its coset. By definition, this is a surjective mapping, since every coset must have some element, and those elements must be in G.

We also see that every coset must be represented by some element, so in the following, let $g_i' \in G$ represent the coset g_iH; by definition of a coset we have $g_i = g_i'h_i$ for some $h_i \in H$. A simple proof of the homomorphism shows that $\phi(g_1g_2) = (g_1g_2)H$ which is the coset of g_1g_2, and $\phi(g_1)\phi(g_2) = (g_1H)(g_2H)$ which is the coset of the representatives $g_1'g_2'$. For them to be in the same coset, we see $g_1g_2 = g_1'h_1g_2'h_2 = g_1'g_2'((g_2')^{-1}h_1g_2')h_2$ needs to be written in the form gH, so we want $(g_2')^{-1}h_1g_2' \in H$ for every possible $g_2' \in G$ and $h_1 \in H$. But this is exactly the condition that normal subgroups provide, and hence there exists an epimorphism from G to G/H, which shows that G/H forms a group, inheriting the identity as the coset of $1 \in G$, and the multiplication itself from G.

Definition 1.6.3. Suppose G some group, and $H \lhd G$. We call G/H the quotient group of G by H.

Proposition 1.6.4. Subgroups of abelian groups must be normal.

Proof. Suppose G is our abelian group, and $H \subseteq G$ our subgroup. Then for all $g \in G$ and $h \in H$, we realize that both g, h are elements of G, and hence will commute, so we have $ghg^{-1} = gg^{-1}h = h \in H$, and hence $H \lhd G$.

Theorem 1.6.5. $H \lhd G$ is a normal subgroup if and only if the left and right cosets are identical, that is, $gH = Hg$ for all $g \in G$.

Proof. In the forward direction, assuming a normal subgroup, by definition we have for all $g \in G$ and $h \in H$,, $ghg^{-1} \in H$, which tells us that there exists some $h' \in H$ such that $ghg^{-1} = h'$. When we right-multiply by g on both sides, we get $gh = h'g$. This tells us that for all elements $g \in G$ and $h \in H$ $gh \in Hg$, so we get $gH \subseteq Hg$. Similarly, we can left-multiply by g^{-1} on both sides, and get $hg^{-1} = g^{-1}h'$, which tells us for all $g \in G$ and $h \in H$, $hg \in gH$, so we get $Hg \subseteq gH$. Combining these two statements, we get $gH = Hg$.

In the reverse direction, assuming that left and right cosets are equal, we reverse the argument to see that for all $g \in G$ and $h \in H$, $gh \in Hg$, so there exists some $h' \in H$ such that $gh = h'g$, which implies $ghg^{-1} = h' \in H$.

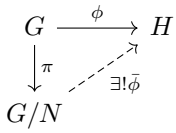
Remark 1.6.6. It is good to remind ourselves that $gH \subseteq G$, cosets are subsets of the whole group; but $gH \in G/H$, these are now elements of the quotient group.

1.7 Homomorphisms and Isomorphisms

Definition 1.7.1. Suppose we have a group homomorphism $\phi\colon G \to H$. We call the preimage of the identity $\phi^{-1}(1)$ the kernel of ϕ, sometimes denoted $\ker(\phi) = \{g \in G : \phi(g) = 1\}$.

Theorem 1.7.2 (Universal Property of Quotient Groups)**.** Let G, H be groups, and $N \lhd G$ be a normal subgroup. Suppose $\pi\colon G \to G/N$ is the quotient homomorphism and $\phi\colon G \to H$ is any group homomorphism with $N \subseteq \ker(\phi)$. Then there exists a unique group homomorphism $\bar{\phi}\colon G/N \to H$ such that $\phi = \bar{\phi} \circ \pi$.

This is represented by the following commutative diagram:



Proof. This universal property asserts that both the existence and and the uniqueness of $\bar{\phi}$, which needs to be proven separately. We will write our proof in reverse order, first proving the uniqueness assuming existence, and then proving existence without any assumptions.

Suppose $\phi = \bar{\phi} \circ \pi = \bar{\phi}' \circ \pi$. Since $N \subseteq \ker(\phi)$, all elements $n \in N$ obey $\phi(n) = 1$. Knowing that all elements in G belong to some coset gN, all $g' \in gN$ maps to $\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g)$, which tells us the image of each coset is a single element $\phi(gN) = \{\phi(g)\}$. Now, seeing that π maps $g' \mapsto gN$, its coset, by definition of a quotient mapping if $\bar{\phi} \neq \bar{\phi}'$, there must be one such coset gN that $\bar{\phi}(gN) \neq \bar{\phi}'(gN)$ disagrees on. However, this is a contradiction, because for all $g' \in gN \subseteq G$, $\bar{\phi}'(gN) = \bar{\phi}'(\pi(g')) = \phi(g') = \bar{\phi}(\pi(g')) = \bar{\phi}(gN)$, contradicting with our assumed inequality above. Hence we have established uniqueness of $\bar{\phi}$.

We will now prove existence by constructing such a homomorphism. Let $\bar{\phi}\colon G/N \to H,\ gN \mapsto \phi(g)$, mapping all cosets gN to the function output of its coset representative. Suppose some arbitrary element $g' \in gN \subseteq G$ in an arbitrary coset. Then we know that there exists $n \in N$ such that $g' = gn$, which allows us to conclude that

$$\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g) = \bar{\phi}(gN) = \bar{\phi}(\pi(g'))$$

Remark 1.7.3. Logically speaking, the existence part is proven before the uniqueness part in the sense that one requires existence to prove uniqueness. However, it is convenient to write universal property proofs in the reverse order because during the proof of uniqueness, we often demonstrate criteria that must be followed by our unique function $\bar{\phi}$, which greatly helps us in deciding how to construct $\bar{\phi}$ during the proof of existence.

Remark 1.7.4. Jacobson here groups all the statements below into something known as the Fundamental Theorem of Homomorphisms of Groups and the Isomorphism Theorems. We will group the theorems differently, following the convention as given in Rotman and Dummit & Foote, and with the correspondence theorem denoted the Fourth Isomorphism Theorem. Nevertheless, armed with the universal property, these are much easier to prove now.

Remark 1.7.5. The next four isomorphism theorems do also apply for monoids and submonoids. The proofs are in fact part of proving the group isomorphism theorems, just slightly simpler.

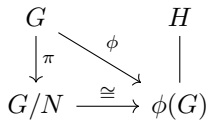
Theorem 1.7.6 (First Isomorphism Theorem for Groups)**.** Suppose $\phi\colon G \to H$ is a group homomorphism, and $N = \ker(\phi)$. We have:

(a) $N \lhd G$, the kernel is a normal subgroup;

(b) $\phi(G) \subseteq H$, the image is a subgroup; and

(c) $\phi(G) \cong G/N$, the image is uniquely isomorphic to the quotient group.

This is represented by the following commutative diagram:



Proof. We first prove that the preimage of the identity forms a subgroup of H. Suppose $\{g_1, g_2\} \subset \phi^{-1}(1)$. Then we know $\phi(g_1) = \phi(g_2) = 1$, which gives us closure with $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = 1$. Associativity is inherited from the multiplication of G_1, while the identity by definition must obey $\phi(1) = 1$. Lastly we have $1 = \phi(1) = \phi(g_1 g_1^{-1}) = \phi(g_1)\phi(g_1^{-1})$, which forces us to conclude that $g_1^{-1} \in \phi^{-1}(1)$, giving us an inverse. Hence $\phi^{-1}(1)$ is a group.

Now to prove that this is a normal subgroup, suppose we have some arbitrary element $g \in G$, and $h \in \phi^{-1}(1)$. We see that $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1) = 1$, which implies $ghg^{-1} \in \phi^{-1}(1)$, exactly the definition of a normal subgroup, which proves statement (a).

If $\{\phi(x), \phi(y)\} \subset \phi(G)$, then $\phi(x)\phi(y) = \phi(xy) \in \phi(G)$, and thus we have closure. Then $\phi(1_G) \in \phi(G)$ which must be the identity by definition of a homomorphism. Associativity is obtained for free when we equate the multiplicative operation between G and $\phi(G)$. Lastly the inverse must be given by $1_H = \phi(1_G) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. Hence $\phi(G)$ forms a subgroup of H, which proves statement (b).

By the universal property, there exists a unique homomorphism $\bar{\phi}\colon G/N \to \phi(G)$ such that $\phi = \bar{\phi} \circ \pi$, where π is the quotient homomorphism. Since by definition, ϕ is a surjective mapping from G to its image $\phi(G)$, $\bar{\phi}$ must also be a surjection.

Again taking the same definition for $\bar{\phi}$ as in the universal property, $\bar{\phi}\colon G/N \to \phi(G)$, $gN \mapsto \phi(g)$, suppose we have two cosets g_1N and g_2N. such that $\bar{\phi}(g_1N) = \bar{\phi}(g_2N)$, giving us $\phi(g_1) = \bar{\phi}(\pi(g_1)) = \bar{\phi}(g_1N) = \bar{\phi}(g_2N) = \bar{\phi}(\pi(g_2)) = \phi(g_2)$ But then we have $1 = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1g_2^{-1})$, implying that $g_1g_2^{-1} \in N$, the kernel. Hence we have $g_1 \in g_2N$, which gives us $g_1N \subseteq g_2N$, so without loss of generality, $g_2N \subseteq g_1N$, giving us $g_1N = g_2N$, the cosets must be equal. This proves injectivity.

Combining surjection and injection gives us our required bijective homomorphism, which is an isomorphism, proving statement (c).

Definition 1.7.7. Suppose G is a group, and $S, T \subseteq G$ some subgroups. We define the product to be $ST = \{st : s \in S, t \in T\}$.

Theorem 1.7.8 (Second Isomorphism Theorem for Groups)**.** Suppose G is a group, $S \subseteq G$ some subgroup, and $N \lhd G$ a normal subgroup. We have:

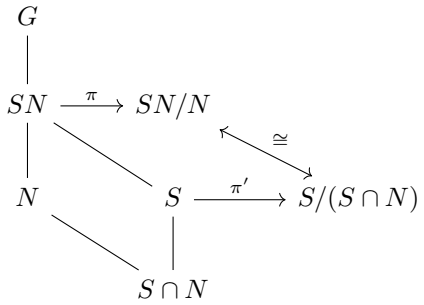
(a) $SN \subseteq G$, the product is a subgroup;

(b) $N \lhd SN$, the normal subgroup is also normal to the product;

(c) $S \cap N \lhd S$, the intersection is normal to the subset; and

(d) $SN/N \cong S/(S \cap N)$, these two quotients are isomorphic.

This is represented by the following commutative diagram:



Proof. We can see that for all $s_in_i \in SN$, $s_1n_1s_2n_2 = s_1s_2s_2^{-1}n_1s_2n_2 \in SN$, since $s_2^{-1}n_1s_2 \in N$ by definition of normal, and we have closure. Associativity is inherited from G, and the identity 1 is in both S and N. Lastly, $(sn)^{-1} = n^{-1}s^{-1} = s^{-1}sn^{-1}s^{-1} \in SN$, since $sn^{-1}s^{-1} \in SN$ by definiton of normal, which gives us inverse. Therefore $SN \subseteq G$ forms a group, giving us statement (a).

Now, clearly $N \subseteq SN$, because every element $n \in N$ multiplied by $1 \in S$ gives us an element of SN. To prove normality, we need to prove that for all $s \in S$ and $n_i \in N$, $sn_1n_2(sn_1)^{-1} \in N$. This is easy because $sn_1n_2(sn_1)^{-1} = s(n_1n_2n_1^{-1})s^{-1} \in N$ by definition of $N \lhd G$. Hence $N \lhd SN$, proving statement (b).

Also, clearly $S \cap N \subseteq S$, because by definition $g \in S \cap N$ implies $g \in S$ (and $g \in N$). Now it is sufficient to prove that for all $g \in S \cap N$ and $s \in S$, $sgs^{-1} \in S \cap N$. It is clear that since both g, s are elements of S, $sgs^{-1} \in S$. Then since $g \in N$, and $s \in S \subseteq G$, we have $sgs^{-1} \in N$ since $N \lhd G$. Hence $sgs^{-1} \in S \cap N$, so we have $S \cap N \lhd S$, proving statement (c).

We now attempt to construct a homomorphism $\phi\colon S \to SN/N$, $s \mapsto sN$. We demonstrate that this is a valid homomorphism, by showing that

$$\phi(s_1s_2) = (s_1s_2)N = (s_1N)(s_2N) = \phi(s_1)\phi(s_2)$$

since s_1, s_2 are elements of G, so same logic as the quotient subgroup epimorphism applies.

We now want to show that ϕ is surjective. The elements $sn \in SN$ must belong in some coset snN, which we can see is equivalent to sN. By definition, ϕ maps $s \mapsto sN$, so every coset is covered by ϕ, and therefore it is an epimorphism.

We can then demonstrate that $\ker(\phi) = S \cap N$. We can see that if $g \in S \cap N$, then $g \in N$, so $\phi(g) = gN = N$, which gives us $S \cap N \subseteq \ker(\phi)$. On the other hand, if $g \in \ker(\phi)$, then $\phi(g) = gN \subseteq N$, which requires $g \in N$, giving us $\ker(\phi) \subseteq S \cap N$. Hence $\ker(\phi) = S \cap N$.

Lastly, we can apply the first isomorphism theorem, and prove that there exists a unique isomorphism between $S/(S \cap N) \cong SN/N$.

Theorem 1.7.9 (Third Isomorphism Theorem for Groups)**.** Suppose G is a group, $N \lhd G$ a normal subgroup. Then:

(a) if K is a subgroup such that $N \subseteq K \subseteq G$, then $K/N \subseteq G/N$ is a subgroup;

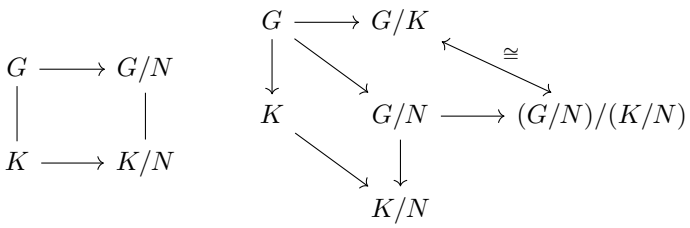
(b) a subgroup of G/N must be of the form K/N such that K is a subgroup with $N \subseteq K \subseteq G$;

(c) if K is a normal subgroup such that $N \subseteq K \subseteq G$, then $K/N \lhd G/N$ is a normal subgroup;

(d) a normal subgroup of G/N must be of the form K/N where $K \lhd G$ is a normal subgroup with $N \subseteq K \subseteq G$; and

(e) if $K \lhd G$ is a normal subgroup such that $N \subseteq K \subseteq G$, then $(G/N)/(K/N) \cong G/K$.

This is represented by the following commutative diagrams:



Proof. We first have to prove that $N \lhd K$, which is obvious because by definition of normality, for all $n \in N$ and $g \in G$, $gng^{-1} \in N$, which can be restricted to $g \in K \subseteq G$.

It is now easy to see that with the quotient homomorphism $\pi\colon G \to G/N$, the image of the subgroup $\pi(K) = K/N$, so by the first isomorphism theorem K/N forms a subgroup. This proves statement (a).

Suppose $K' \subseteq G/N$ is a subgroup. We can look at the preimage $\pi^{-1}(K')$, which since $1 \in K'$, we have $K' \supseteq \ker(\pi) = N$. Notice that the preimage of a group is still a group: suppose $\phi\colon G' \to H'$ is a homomorphism, since $\{x, y\} \subseteq \phi^{-1}(H')$ implies $\phi(xy) = \phi(x)\phi(y) \in H'$ (closure), $1 \in \ker(\phi) \subseteq \phi^{-1}(H')$ (identity), associativity inherited from G', and $x \in \pi^{-1}(H')$ implies $\pi(x)^{-1} = \pi(x^{-1}) \in H'$ (inverse). This proves statement (b).

It is now sufficient to prove the normality condition. $K \lhd G$ tells us that for all $g \in G$, $gKg^{-1} \subseteq K$, which under mapping is $\pi(gKg^{-1}) = \pi(g)\pi(K)\pi(g)^{-1}$. Notice that by Theorem 1.6.5, $\pi(g)\pi(K) = \pi(K)\pi(g)$, which allows us to cancel out the g and its inverse, letting us conclude that $\pi(gKg^{-1}) \subseteq \pi(K)$, giving us $\pi(K) = K/N \lhd G/N$. This proves statement (c).

Similarly, assume $K' \lhd G/N$; then for all $x \in G/N$, $xK'x^{-1} \subseteq K'$. No matter what element $g \in G$, $k \in \pi^{-1}(K')$ we choose, we have $\pi(gkg^{-1}) = \pi(g)\pi(k)\pi(g)^{-1} \in K'$ by definition of normality in G/N, so $ghg^{-1} \in \pi^{-1}(K')$, and the preimage is normal. This proves statement (d).

We can now attempt to construct a homomorphism $\phi\colon G/N \to G/K$, $gN \mapsto gK$. This is valid because by the universal property, we have $\pi\colon G \to G/N$ and $\eta\colon G \to G/K$, so there is a unique homomorphism that makes $\eta = \phi \circ \pi$. We can also show that this is surjective, since the K-cosets partition G, so each K-coset must have some element gK that represents it, and clearly this element gN in the N-cosets must get sent to it, alongside all other elements in that N-coset.

We claim the kernel is $\ker(\phi) = K/N$. Observe that $\ker(\eta) = K$ and $\ker(\pi) = N$, so ϕ must map all the N-cosets that are represented by elements of K into 1.

Lastly, we invoke the first isomorphism theorem, which gives us $\ker(\phi) = K/N \lhd G/N$, making our quotient $(G/N)/(K/N)$ valid; and also that $(G/N)/\ker(\phi) = (G/N)/(K/N) \cong G/K$, proving statement (e).

Theorem 1.7.10 (Fourth Isomorphism Theorem for Groups)**.** Suppose G is a group, $N \lhd G$ some normal subgroup, and $\pi\colon G \to G/N,\ g \mapsto gN$ the quotient homomorphism. Then π is a bijection between the subgroups of G/N and the subgroups of G containing N; and is also a bijection between normal subgroups of G/N and normal subgroups of G containing N.

Proof. This is merely a corollary of the third isomorphism theorem. Statements (a) and (b) prove the correspondence between subgroups, while statements (c) and (d) prove the correspondence between normal subgroups.

1.8 Action on Sets

Definition 1.8.1. Suppose X is a set of n elements. The group of all possible permutations (guaranteed by Proposition 1.4.2) is denoted S_X, which is of course isomorphic to S_n.

Definition 1.8.2. Suppose G a group, and X some set. The action of G on X is a homomorphism $\phi\colon G \to S_X$.

Remark 1.8.3. Notice that by Cayley's theorem, every finite group is a transformation group on itself. With this knowledge, we can formally say that we can let G act on itself by left multiplication, where the homomorphism is $\phi\colon G \to S_G,\ g \mapsto \ell_g$, and $\ell_g\colon G \to G,\ \alpha \mapsto g\alpha$. Beware that when considering actions, the homomorphism $\phi(g)$ outputs a function on the set X that we are acting on, so in general $\phi(g)(x) = \phi_g(x)$ are both valid notation, the former focusing on that we have a homomorphism $\phi(g)$, and the latter focusing on that we have a function ϕ_g.

Proposition 1.8.4 (Action by Conjugation)**.** Suppose G is a group. G can act on itself by conjugation, that is, $\phi\colon G \to S_G,\ g \mapsto \gamma_g$ where $\gamma_g\colon G \to G,\ \alpha \mapsto g\alpha g^{-1}$.

Proof. We need to first prove that γ_g is a bijection. Suppose $\{\alpha, \beta\} \subset G$, $g\alpha g^{-1} = g\beta g^{-1}$; then $\alpha = g^{-1}g\alpha g^{-1}g = g^{-1}g\beta g^{-1}g = \beta$, which implies γ_g is an injection. Now, clearly, for every element $x \in G$, we can map $\gamma_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x$, which implies γ_g is a surjection. Hence γ_g is a bijection.

We now then prove that ϕ is a homomorphism. Clearly γ_1 is the identity mapping $\alpha \mapsto 1\alpha 1^{-1} = \alpha$.

$$\gamma_{gh}(\alpha) = (gh)\alpha(gh)^{-1} = gh\alpha h^{-1}g^{-1} = \gamma_g(h\alpha h^{-1}) = \gamma_g(\gamma_h(\alpha))$$

We have showed that $\phi(gh) = \gamma_{gh} = \gamma_g \circ \gamma_h = \phi(g)\phi(h)$, which proves homomorphism.

Definition 1.8.5. Suppose G is a group that acts on some set X via the homomorphism $\phi\colon G \to S_X$. The stabilizer of some element $x \in X$ is the set of all actions that fix x, $\operatorname{stab}(x) = \{g \in G : \phi_g(x) = x\}$.

Proposition 1.8.6. The stabilizer $\operatorname{stab}(x)$ is a subgroup of G.

Proof. Suppose our action is $\phi\colon G \to S_G,\ g \mapsto \phi_g$, where $\phi_g\colon G \to G$ is a permutation. Then the stabilizer is a set of all g such that $\phi_g(x) = x$. Suppose $\phi_g(x) = \phi_h(x) = x$; then $\phi_{gh}(x) = \phi_g(x)\phi_h(x) = x$, so the stabilizer is closed under multiplication. Associativity is given to us for free with function composition, and $\phi_1(x) = x$ is trivially the identity mapping. Lastly if $\phi_g(x) = x$, we know that $x = \phi_1(x) = \phi_g(x)\phi_{g^{-1}}(x) = \phi_{g^{-1}}(x)$ which gives us an inverse.

Definition 1.8.7. Suppose G is a group and $x \in G$ some element in the group. The centralizer of the element is the set of all elements in G that commute with it, $\mathrm{C}(x) = \{g \in G : gx = xg\}$. Similarly, the centralizer of a subset $S \subseteq G$ is the set of all elements in G that commute with every element in S, $\mathrm{C}(S) = \mathrm{C}_G(S) = \{g \in G : \forall x \in S, gx = xg\}$.

Proposition 1.8.8. Suppose G acts on itself by conjugation. Then for any $x \in G$, $\mathrm{C}(x) = \operatorname{stab}(x)$.

Proof. $\operatorname{stab}(x) = \{g \in G : \gamma_g(x) = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = \mathrm{C}(x)$.

Corollary 1.8.9. The centralizer $\mathrm{C}(S) \subseteq G$ is a subgroup.

Proof. We first observe that $\mathrm{C}(S) = \bigcap_{s\in S} \mathrm{C}(s)$, because it should include all elements that commute with every element of S. Then we know from the proposition above that $\mathrm{C}(s) = \mathrm{stab}(s)$, which are subgroups by Proposition 1.8.6. Lastly, from Lemma 1.3.4 we know the intersection of subgroups is a subgroup.

Definition 1.8.10. We sometimes call the centralizer of the entire group $\mathrm{C}(G)$ the center of the group $\mathrm{Z}(G)$. It consists of the elements that commute with everything in the group.

Proposition 1.8.11. Suppose G acts on itself by conjugation. Then the kernel of the homomorphism is the centralizer of the group, $\ker(\phi) = \mathrm{Z}(G)$.

Proof. $\ker(\phi) = \{g \in G : \phi(g) = 1\} = \{g \in G : \gamma_g = \gamma_1\} = \{g \in G : \forall x \in G, gxg^{-1} = x\} = \mathrm{Z}(G)$.

Remark 1.8.12. The centralizer tells us what and how many elements of G commute with everything, so in a sense, self-action by conjugation allows us to 'measure' the noncommutativity of G.

Definition 1.8.13. Suppose G is a group and $S \subseteq G$ some subset of the group. The normalizer of the subset is the set of elements that fix S under conjugation, i.e. conjugation by the normalizer sends elements of S to (potentially other) elements of S. This is denoted $\mathrm{N}(S) = \mathrm{N}_G(S) = \{g \in G : gSg^{-1} = S\}$.

Proposition 1.8.14. The normalizer $\mathrm{N}(S) \subseteq G$ is a subgroup.

Proof. We clearly have closure with $(gh)S(gh)^{-1} = ghSh^{-1}g^{-1} = gSg^{-1} = S$. Associativity and identity is given to us, as per usual, for free. Since $gSg^{-1} = S$, then $S = g^{-1}gSg^{-1}g = g^{-1}Sg$, and we get inverse.

Remark 1.8.15. Recall from the definition of cosets and orbits in Section 1.5 that the actions of G form orbits, which are equivalence classes demonstrating that there exists an action $g \in G$ such that $\phi_g(x) = y$ for all $\{x, y\} \subset X$ in the same orbit. If we allows G to act on itself, these now define equivalence classes on G itself, which allow us to deduce facts about subgroups of G. In particular, under self-action, the set of orbits $G/\sim$ partition G.

Definition 1.8.16. Suppose G acts on a set X by conjugation. The orbits of X are equivalence classes, which we call conjugacy classes, sometimes denoted $[x] = \{\gamma_g(x) = gxg^{-1} : g \in G\}$.

Definition 1.8.17. Suppose G acts on two sets X and Y via $\phi\colon G \to S_X,\ g \mapsto \phi_g$ and $\psi\colon G \to S_Y,\ g \mapsto \psi_g$ respectively. We say X is equivalent to Y under G-action if there exists a bijection $f\colon X \to Y$ such that $f(\phi_g(x)) = \psi_g(f(x))$ for all $x \in X$ and $g \in G$.

This can be summarized by the following commutative diagram:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow{\scriptstyle \phi_g} & & \downarrow{\scriptstyle \psi_g} \\ X & \xrightarrow{f} & Y \end{array}$$

Lemma 1.8.18. Suppose G acts on X transitively (there is only one orbit). Then there exists a subgroup $H \subseteq G$ such that X is equivalent to G/H.

Proof. Suppose the action of G on X is $\phi\colon G \to S_X,\ g \mapsto \phi_g$. To prove such an equivalence, first we have to construct H. Choosing some arbitrary $x \in X$, let us find its stabilizer $H = \mathrm{stab}(x) = \{g \in G : \phi_g(x) = x\}$, which by Proposition 1.8.6 we know is a subgroup.

Now, suppose G acts on G/H by left multiplication, so that we have $\psi\colon G \to S_{G/H},\ g \mapsto \ell_g$, where $\ell_g\colon G/H \to G/H,\ rH \mapsto grH$. Note that G/H here is not a quotient group, but rather the set of all left cosets. We claim that the function $f\colon X \to G/H,\ \phi_g(x) \mapsto gH$ forms a bijection. We first see that this is a completely valid definition, because the action is transitive, so $\phi_g(x)$ covers all of X. We then have to check that if $\phi_{g_1}(x) = \phi_{g_2}(x)$, $g_1H = g_2H$; this is obvious because $\phi_{g_2}^{-1} \circ \phi_{g_1}(x) = x$, and $g_2^{-1}g_1 \in H$, so $g_2 \in g_1H$, and without loss of generality we also have $g_1 \in g_2H$. f is injective because if $g_1H = g_2H$, then

$(g_2^{-1}g_1)H = H$, so $\phi_{g_2^{-1}g_1}(x) = \phi_{g_2}^{-1} \circ \phi_{g_1}(x) = x$, and hence $\phi_{g_1}(x) = \phi_{g_2}(x)$. f is surjective also because for every gH, at least gx will map to it. Therefore, f is a bijection.

We will now check the equivalence under multiplication. For some arbitrary $r \in G$, and hence some arbitrary $\phi_r(x) \in X$,

$$\ell_g(f(\phi_r(x))) = \ell_g(rH) = grH = f(\phi_{gr}(x)) = f(\phi_g(\phi_r(x)))$$

We can conclude that there is equivalency between X and G/H.

Corollary 1.8.19 (Orbit-Stabilizer Theorem)**.** Suppose G is a group that acts on a finite set X. Let $x \in X$ denote an arbitrary element. Then we have an equivalence between the size of the orbit of x and the index of the stabilizer in G, that is, $|\text{orb}(x)| = [G : \text{stab}(x)]$.

Proof. We shall restrict the action on G on X to only acting onto the subset $\text{orb}(x) \subseteq X$. This new action is now by definition transitive. The lemma above asserts an equivalence between $\text{orb}(x)$ and $G/\text{stab}(x)$, that is, a bijection between elements of these two sets. Hence we can equate the cardinality of these two sets.

Corollary 1.8.20. If G acts on X transitively, then $|X| \mid |G|$.

Proof. From the lemma above, since there is a bijection between X and G/H we know that $|X| = |G/H|$. But Lagrange's theorem guarantees that the number of cosets is $|G/H| = [G : H] \mid |G|$.

Theorem 1.8.21 (Class Equation)**.** Suppose G acts on X. Then $|X| = \sum_i |X_i| = \sum_i |G/H_i|$, where $H_i \subseteq G$ subgroups, and hence $|G/H_i| \mid |G|$.

Proof. Suppose the orbits of X are disjoint sets X_i. Then if we restrict to any subset $X_i \subseteq X$, G acts on X_i transitively. By the lemma above, X_i is equivalent to G/H_i, so $|X_i| = |G/H_i|$. Now, since orbits partition X, $|X| = \sum |X_i|$.

Corollary 1.8.22. $|G| = |\text{Z}(G)| + \sum_i n_i$ where $n_i \mid |G|$.

Proof. Let G act on itself by conjugation. For the elements $x \in G$ that get fixed by conjugation, i.e. they commute with all $g \in G$, their orbits (conjugacy classes) are a single element $[x] = \{\gamma_g(x) = gxg^{-1} : g \in G\} = [x] = \{x\}$. Together, all these elements form the center $\text{Z}(G)$.

Then all other conjugacy classes (with more than one element) are equivalent to G/H_i by the class equation, which are divisors of $|G|$.

Theorem 1.8.23. Suppose G is a finite group, with order $|G| = p^r$ where p is prime. Then G has a nontrivial center, that is, $\text{Z}(G) \neq \{1\}$.

Proof. Suppose we have a trivial center. Then the class equation tells us that $p^r = 1 + \sum_i p^{r_i}$, since the order is $|G| = p^r$, $|\text{Z}(G)| = 1$, and all divisors of p^r must be some power of p, with $r_i \neq 0$, as those orbits cannot be trivial. But clearly the left side is a multiple of p, and the right side has a multiple of p plus 1, which is a contradiction.

Corollary 1.8.24. Suppose G is a group with order $|G| = p^2$, where p is prime. Then G is abelian.

Proof. We know from the theorem above that it has a nontrivial center ($|\text{Z}(G)| \neq 1$), so if the order of some element is p^2, then it generates the entire group, and it must be cyclic (abelian).

Now suppose there are no elements of order p^2; then all elements other than the identity must have order p, which implies the center must also be a subgroup (Corollary 1.8.9) that is cyclic with order p (Theorem 1.5.8). Let $\text{Z}(G) = \langle g \rangle$, where $|g| = p$. Clearly there is another element $k \in G$, but $k \neq g^r$ such that $|k| = p$. If $gk = kg$, then a simple counting argument gives us $\langle g, k \rangle$ a group of order p^2, since every element can be written in the form $g^i k^j$, i, j each having p choices each. If on the other hand, $gk \neq kg$, then $\langle g, k \rangle$ must include all previously mentioned p^2 elements, and also kg, which implies $|\langle g, k \rangle| > p^2$, and contradicts the fact that $\langle g, k \rangle \subseteq G$. Hence $gk = kg$, and any power of g commutes with any power of k, so all elements of G commute with each other.

Theorem 1.8.25. Conjugacy classes in S_n are the cycle types; same cycle types are in the same conjugacy class, and different cycle types are in different conjugacy classes.

Proof. Suppose we have a d-cycle $(n_1 n_2 \dots n_d)$. We know that for all $g \in S_n$, $n_i \in \{1, \dots, n\}$, any $g(n_1 n_2 \dots n_d)g^{-1} = (g(n_1)g(n_2)\dots g(n_d))$ by Proposition 1.4.9. This is also a d-cycle. As all elements of S_n are disjoint cycles, all such disjoint cycle types must only ever map to their own cycle type under conjugation.

Remark 1.8.26. In general it is difficult to determine exactly the conjugacy classes of a group.

1.9 Sylow's Theorems

Theorem 1.9.1 (Cauchy's Theorem)**.** Suppose G is a finite abelian group, and there is some prime $p \mid |G|$ that divides the order of the group. Then there exists an element $g \in G$ of order $|g| = p$.

Proof. We first consider the base case where $|G| = p$. By Corollary 1.5.9, we know that there exists a subgroup $\langle g \rangle \subseteq G$ where $g \in G$ is any arbitrary element $g \neq 1$.

We now proceed by strong induction on the order of the group. Suppose $|G| = mp$, where $m \in \mathbb{N}$, and that for all $k < m$ Cauchy's Theorem for order kp is proven. Let us arbitrarily pick some $x \neq 1$, $x \in G$. Suppose the order of this element is some $|x| = n$. If $p \mid n$, then Theorem 1.3.13 guarantees us that there exists a subgroup $\langle x^m \rangle \subseteq \langle x \rangle$ with order $|x^m| = p$. If $p \nmid n$, then we can construct a subgroup $G/\langle x \rangle$ ($\langle x \rangle$ guaranteed to be normal by Proposition 1.6.4), which by Lagrange's theorem has order $|G/\langle x \rangle| = |G|/|x| = mp/n$, and Euclid's lemma tells us $p \mid mp/n$. Then clearly $m/n \in \mathbb{N}$, specifically $m/n < m$, so the induction hypothesis applies.

Theorem 1.9.2 (Sylow's First Theorem)**.** Suppose G a finite group, p a prime number, and that the order is $|G| = Np^s$, with $\gcd(N, p) = 1$ coprime (that is, p^s is the largest power of p that divides $|G|$). Then for all $0 \leq t \leq s$, G contains a subgroup of order p^t.

Proof. We first consider the case where G is abelian. Trivially, G itself is a subgroup of order $|G| = Np^s$, which we will use as our base case.

We now suppose, by way of weak induction, that we have a subgroup H_k of order $|H_k| = Np^k$ (for $k \geq 1$). We wish to prove that a subgroup H_{k-1} of order $|H_{k-1}| = Np^{k-1}$ exists. By Cauchy's theorem, we can find an $x_k \in H_k$ of order $|x_k| = p$. Proposition 1.6.4 tells us that $\langle x_k \rangle \lhd H_k$, so $H_k/\langle x_k \rangle$ is a subgroup, with Lagrange's theorem telling us its order is $|H_k/\langle x_k \rangle| = |H_k|/|x_k| = Np^k/p = Np^{k-1}$. This allows us to conclude that there are subgroups of G with orders Np^r where $0 \leq r \leq s$.

Again invoking Proposition 1.6.4, $H_{s-t} \lhd G$ for all $0 \leq t \leq s$. Hence G/H_{s-t} is a subgroup, with its order determined by Lagrange's theorem to be $|G/H_{s-t}| = |G|/|H_{s-t}| = (Np^s)/(Np^{s-t}) = p^t$.

Now consider the case where G is not abelian. Then clearly there are elements that do not commute, so $\mathrm{Z}(G) \subsetneq G$. We can write down the class equation $|G| = |\mathrm{Z}(G)| + \sum_i [G : H_i]$, where there is at least one i in the summation.

We can first prove the simplest case when $|G| = p^s$. It suffices to consider G not abelian, since the abelian case is already proven above. The center of the group $\mathrm{Z}(G)$ is a subgroup (Corollary 1.8.9), so its order must divide the order of the whole group ($|\mathrm{Z}(G)| \mid |G| = p^s$, Lagrange's theorem), which implies $p \mid |\mathrm{Z}(G)|$. Then Cauchy's theorem tells us that we can find an element $x \in \mathrm{Z}(G) \subsetneq G$ such that $|x| = p$. Proceeding similarly to the induction in the abelian case, we see that $\langle x \rangle \lhd \mathrm{Z}(G)$ (Proposition 1.6.4), and in fact $\langle x \rangle \lhd G$, simply because $g \in \mathrm{Z}(G)$, and will commute with every element of G ($gx^r g^{-1} = x^r g g^{-1} = x^r \in \langle x \rangle$). Hence $G/\langle x \rangle$ is a subgroup with order $|G|/|x| = p^{s-1}$ (Lagrange). Recursively applying this process on the quotient group generates subgroups of order $1, p, p^2, \dots, p^s$.

Let us then go back to the general case of $|G| = Np^s$. We shall additionally assume, by way of strong induction, that any group of order mp^s, where $m < N$ has subgroups of order $1, p, p^2, \dots, p^s$. Suppose there exists a subgroup H_i in the class equation such that $p^s \mid |H_i|$. Then clearly $|H_i| = mp^s$, $m < N$, so the induction hypothesis immediately gives our desired result.

Suppose otherwise, when $p^s \nmid |H_i|$; we can then see that $p \mid [G : H_i]$ for all i, since Lagrange's theorem guarantees $Np^s = |G| = |H_i|[G : H_i]$, and our supposition tells us that the prime factorization of $|H_i|$ includes at most p^{s-1}, and therefore $[G : H_i]$ prime factorizes to include at least one p. Then every term in the

summation inside the class equation is divisible by p, and the left side is Np^s, which also is divisible by p, so the remaining term, the centralizer must also be $p \mid |\mathrm{Z}(G)|$. But this condition means we can follow the proof as in the previous paragraph; given some group H_k of order Np^k, we can find an element x_k of order p such that $H_{k-1} = H_k/\langle x_k \rangle$ is a group of order $|H_{k-1}| = Np^{k-1}$. The natural quotient homomorphism $\pi_k \colon H_k \to H_{k-1}$ has a kernel of order p. It is then possible to construct a chain of homomorphisms $\pi_{s-r} \circ \pi_{s-r+1} \circ \cdots \circ \pi_s$, which has a kernel of order p^r; and as we know from the first isomorphism theorem the kernel is a group, which gets us our desired result.

Remark 1.9.3. This theorem does not hold for order d^s when d is not prime.

Corollary 1.9.4 (Cauchy's Theorem)**.** Suppose G is a finite group, abelian or not, and there is a some prime $p \mid |G|$ that divides the order of the group. Then there exists an element $g \in G$ of order $|g| = p$.

Proof. Special case of the theorem above, with $t = 1$.

Definition 1.9.5. A group with prime power order, that is, $|G| = p^r$ for some $r \in \mathbb{N}$, is called a p-group.

Corollary 1.9.6. There exists subgroups of all possible orders that divide the order of a p-group.

Proof. The order of a p-group is p^s, so the theorem above applies.

Definition 1.9.7. Suppose G is a finite group with order Np^s, $\gcd(N, p) = 1$. A subgroup of order p^s (maximal prime power order) is often called a Sylow p-subgroup of G, and less often called a p-Sylow subgroup of G.

Lemma 1.9.8. Suppose G is a finite group with $|G| = Np^s$, $\gcd(N, p) = 1$, with $P \subseteq G$ a Sylow p-subgroup. If $K \subseteq \mathrm{N}(P)$ a subgroup, and $|K| = p^t$, then $K \subseteq P \subseteq \mathrm{N}(P)$.

Proof. By definition of a normalizer, if $g \in \mathrm{N}(P)$, we have $gPg^{-1} \subseteq P$, so $P \lhd \mathrm{N}(P)$.

Since $P \subseteq \mathrm{N}(P) \subseteq G$, Lagrange's theorem gives us $\mathrm{N}(P) = mp^s$, $m \mid N$. We form a quotient group $\mathrm{N}(P)/P$, which has an order $mp^s/p^s = m$, which is coprime to p since N is already coprime to p. The natural quotient homomorphism is $\pi \colon \mathrm{N}(P) \to \mathrm{N}(P)/P$. We now inspect the image $\pi(K)$, which by the first isomorphism theorem is a subgroup of $\mathrm{N}(P)/P$.

Now, as elements of $k \in K$ have $k^{p^t} = 1$ by Corollary 1.5.10, under the homomorphism we should have $\pi(k)^{p^t} = 1$, so the order $|\pi(k)| \mid p^t$. But the order also $|\pi(k)| \mid m$, because it should divide the order of the codomain group; since m, p coprime, m, p^t also coprime, so the order must be $|\pi(k)| = 1$, and therefore the image must be $\pi(K) = \{1\}$. Hence we can conclude that $K \subseteq \ker(\pi) = P$.

Theorem 1.9.9 (Sylow's Second Theorem)**.** Suppose G is a finite group, p a prime number, and that the order is $|G| = Np^s$, with $\gcd(N, p) = 1$. Let us denote P and P' as arbitrary Sylow p-subgroups. Then the following will hold:

(a) Any two Sylow p-subgroups are conjugate, that is, if $|P| = |P'| = p^s$, then there exists a $g \in G$ such that $gPg^{-1} = P'$;

(b) Let the number of Sylow p-subgroups be n, then $n \mid [G : P] = N$ and $n \equiv 1 \pmod{p}$; and

(c) If $K \subseteq G$ is a subgroup with order $|K| = p^t$, $0 \leq t \leq s$, then $K \subseteq P$ a subgroup of a Sylow p-subgroup.

Proof. Let Π be the set of all Sylow p-subgroups, that is, the set of all subgroups of order p^s. By Sylow's first theorem, this set is not empty $\Pi \neq \varnothing$. Allow us to let G act on Π by conjugation.

Let us fix a singular Sylow subgroup $P \in \Pi$. We can clearly see that the stabilizer here is also the normalizer, since $\mathrm{N}(P) = \mathrm{stab}(P) = \{g \in G : gPg^{-1} = P\}$. Then the orbit-stabilizer theorem gives us that $|\mathrm{orb}_G(P)| = |G|/|\mathrm{N}(P)|$. By Proposition 1.8.14 and Lemma 1.9.8 we know that $P \subseteq \mathrm{N}(P) \subseteq G$, so Lagrange's theorem tells us $p^s \mid |\mathrm{N}(P)|$, and $|\mathrm{N}(P)| \mid Np^s$, and hence we can write $|\mathrm{N}(P)| = mp^s$ where $m \mid N$. If we now were to assume that statement (a) is true, then G-conjugation on Π is transitive, so $\mathrm{orb}_G(P) = X$, and we have $|X| = (Np^s)/(mp^s) = N/m$, and therefore the number of Sylow p-subgroups is $|X| \mid N$, proving the first part of statement (b).

The orbit of P under G-conjugation is a set of groups, which we will denote $\Sigma = \text{orb}_G(P) \subseteq \Pi$ below. Restricting our action such that P acts on Σ by conjugation, by closure of group multiplication, we can see that any $g \in P$ gives us $gPg^{-1} = P$, so the orbit of P under P-conjugation is $\text{orb}_P(P) = \{P\} \subseteq \Sigma$, which must only contain itself. The class equation now tells us that $|\Sigma| = |\text{orb}_P(P)| + \sum_i |\text{orb}_P(X_i)|$, where $X_i \subseteq \Sigma$, and $|\text{orb}_P(P)| = 1$ as seen above.

From our assumptions, we know that the terms in the summation must divide the order $|P|$, so they must be powers of p, that is, $\text{orb}_P(X_i) = p^r$, $r \geq 0$. We claim that the order of those are at least p, that is, $\text{orb}_P(X_i) = p^r$ where $r \geq 1$. Suppose, by way of contradiction, that there exists some other $P' \in \Sigma$, $P' \neq P$ such that $\text{orb}_P(P') = \{P'\}$. Then going back to the definition of an orbit, we have for all $g \in P$, $gP'g^{-1} = P'$, which implies $g \in \text{N}(P')$, i.e. $P \subseteq \text{N}(P')$. As $|P| = p^s$, we can invoke the above lemma and conclude that $P \subseteq P' \subseteq \text{N}(P')$. In particular, since $|P| = |P'|$, we can see that $P = P'$, which contradicts our premise, implying that the orbits $|\text{orb}_P(X_i)| > 1$. This allows us to say that all terms in the summation must be divisible by p, allowing us to write the class equation as $|\Sigma| = 1 + \sum_i r_i p \equiv 1 \pmod{p}$; again, if we assume statement (a) is true, then $|\Pi| = |\Sigma|$, which gives us $|\Pi| \equiv 1 \pmod{p}$, proving the second part of statement (b).

Going back to statement (a), it is sufficient to prove that there exists only one orbit under conjugation. Suppose, by way of contradiction, that there is some Sylow p-subgroup $Q \in (\Pi - \Sigma)$. Then we will restrict the action by conjugation such that Q acts on Σ. Following a similar argument as P' in the previous paragraph, we know each individual Q-orbit has order p^r, $r \geq 0$. We again claim that each orbit is at least order p. If not, there exists some $Q' \in \Sigma$ such that $\text{orb}_Q(Q') = \{Q'\}$, which implies for all $g \in Q$, $gQ'g^{-1} = Q'$, giving us $g \in \text{N}(Q')$, and hence $Q \subseteq \text{N}(Q')$. Invoking the above lemma, we get $Q \subseteq Q' \subseteq \text{N}(Q')$, which since $|Q| = |Q'|$, we have $Q = Q'$, contradicting the fact that $Q' \in \Sigma$, but $Q \notin \Sigma$. Hence we are forced to conclude that all Q-orbits have cardinalities that are multiples of p, implying $p \mid |\Sigma|$. But that itself contradicts the class equation $|\Sigma| = 1 + \sum_i r_i p \equiv 1 \pmod{p}$, which tells us $p \nmid |\Sigma|$. Therefore we are forced to conclude that Q does not exist, and $\Pi - \Sigma = \varnothing$. There is only one G-orbit, so G acts by conjugation on the set of Sylow p-subgroups transitively, which implies we can send any two $\{P, P'\} \subset \Pi$ to each other via conjugation, $gPg^{-1} = P'$ for some $g \in G$. This proves statement (a).

Armed with statements (a) and (b), we now let K act on Π via conjugation. The class equation tells us that $|\Pi| = \sum_i |X_i|$, where the orbits X_i must have orders $|X_i| \mid |K| = p^t$, so all orbits are powers of p. But statement (b) tells us that $|\Pi| \equiv 1 \pmod{p}$, so there must be at least one K-orbit that is of size 1. Suppose $P \in \Pi$ has $|\text{orb}_K(P)| = 1$. Then we see that for all $k \in K$, $kPk^{-1} = P$, so $k \in \text{N}(P)$, and $K \subseteq \text{N}(P)$. We can use the lemma above one last time to see that $K \subseteq P \subseteq \text{N}(P)$. This proves statement (c).

2 Rings

2.1 Basic Definitions

Definition 2.1.1. A ring is a quintuple $(R, +, \cdot, 0, 1)$, where $R \neq \varnothing$ is a set equipped with two operations $+, \cdot$, each with their identity $0, 1$ respectively, with the following three properties:

(i) $(R, +, 0)$ forms an abelian group;

(ii) $(R^\star, \cdot, 1)$, where $R^\star = R - \{0\}$ forms a monoid; and

(iii) $\forall \{a, x, y\} \subset R$, the distributive laws $a(x + y) = ax + ay$ and $(x + y)a = xa + ya$ hold.

Proposition 2.1.2. In a nondegenerate ring R, where $R \neq \{0\}$, $0 \neq 1$.

Proof. For all $x \in R$, we know $0 = x + (-x)$. Suppose, by way of contradiction, that $0 = 1$. Then we have $x = 1x = (x + (-x))x = x^2 + (-x^2) = 0$, implying that $R = \{0\}$.

Definition 2.1.3. Suppose $(R, +, \cdot, 0, 1)$ is a ring. Then $S \subseteq R$ is a subring if:

(i) $(S, +, 0) \subseteq (R, +, 0)$ is a subgroup; and

(ii) $(S^\star, \cdot, 1) \subseteq (R^\star, \cdot, 1)$ is a submonoid.

Lemma 2.1.4. Suppose R is a ring, and $S_i \subseteq R$ subrings. Then $\bigcap_i S_i$ is also a subring of R

Proof. Lemma 1.3.4 gives us that the intersection of additive groups are subgroups, and the intersection of multiplicative monoids are submonoids.

Definition 2.1.5. Suppose R is a ring, and $X \subseteq R$ is a subset. The subring generated by X is the intersection of all subrings R' that contain X, that is, $S = \bigcap_{R \supset R' \supset X} R'$.

Proposition 2.1.6. The subring generated by a subset is the ring of all possible sums and products of elements of the subset.

Proof. Apply Proposition 1.3.5 twice, to both the additive group and the multiplicative monoid.

Definition 2.1.7. A ring homomorphism is a function $f\colon R_1 \to R_2$ where R_1, R_2 are rings, with the properties that:

(i) $f\colon (R_1, +, 0) \to (R_2, +, 0)$ is a group homomorphism; and

(ii) $f\colon (R_1^\star, \cdot, 1) \to (R_2^\star, \cdot, 1)$ is a monoid homomorphism.

Proposition 2.1.8. For every ring R, there exists a unique homomorphism $\zeta\colon \mathbb{Z} \to R$.

Proof. We attempt to define ζ starting with the simplest requirements. We know that ζ must map $0 \mapsto 0_R$ and $1 \mapsto 1_R$, By addition, and inversion, we can clearly define for any $n \in \mathbb{Z}$,

$$\zeta(n) = \zeta(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}) = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} = n_R$$

It is now sufficient to prove existence by checking that this homomorphism is valid under multiplication.

$$\zeta(m)\zeta(n) = \underbrace{(1_R + 1_R + \cdots + 1_R)}_{m \text{ times}} \underbrace{(1_R + 1_R + \cdots + 1_R)}_{n \text{ times}} = \underbrace{1_R + 1_R + \cdots + 1_R}_{mn \text{ times}} = \zeta(mn)$$

Now suppose, by way of contradiction, that there exists another homomorphism $\phi\colon \mathbb{Z} \to R$. Then for them to be different, there exists some $n \in \mathbb{Z}$ such that $\phi(n) \neq \zeta(n)$. But clearly, by definition of ζ,

$$\phi(n) = \phi(\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}) = \underbrace{\phi(1) + \phi(1) + \cdots + \phi(1)}_{n \text{ times}} = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} = \zeta(n)$$

which is a contradiction, since $\phi(1) = 1_R$ by definition of ring homomorphism.

Definition 2.1.9. The homomorphism $\zeta\colon \mathbb{Z} \to R$ is the canonical homomorphism.

Remark 2.1.10. In notation for rings, we might sometimes write some number n and an element $x \in R$ as $nx \in R$, which by strict definition means 'adding up x, n times', which makes $nx = \zeta(n)x$.

Definition 2.1.11. If the multiplicative monoid $(R^\star, \cdot, 1)$ is a group, i.e. there exists multiplicative inverses for every element, then R is a division ring.

Definition 2.1.12. If the multiplicative monoid $(R^\star, \cdot, 1)$ is an abelian group, i.e. there exists multiplicative inverses, and multiplication is commutative, then R is a field.

Definition 2.1.13. If the multiplicative monoid $(R^\star, \cdot, 1)$ is commutative, then R is a commutative ring.

Proposition 2.1.14 (Binomial Theorem)**.** In any commutative ring (and therefore a field), $(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}$, where $\binom{n}{r}$ is the usual binomial coefficient given by $\binom{n}{r} = (n!)/(r!(n-r)!)$.

Proof. ~~Simple proof by induction.~~ *Fine, I'll give you the proof.*
Clearly $x + y = \binom{1}{0}x + \binom{1}{1}y$, as $\binom{1}{0} = 1 = \binom{1}{1}$ by simple computation.
Now, suppose the binomial theorem holds for case k. Then we have

$$\begin{aligned}(x+y)^{k+1} &= x(x+y)^k + y(x+y)^k = \sum_{r=0}^{k} \binom{k}{r} x^{r+1} y^{k-r} + \sum_{r=0}^{k} \binom{k}{r} x^r y^{k-r+1} \\ &= \sum_{r=1}^{k+1} \binom{k}{r} x^r y^{k-r+1} + \sum_{r=0}^{k} \binom{k}{r} x^r y^{k-r+1} = \sum_{r=0}^{k+1} \left[\binom{k}{r} + \binom{k}{r-1} \right] x^r y^{k-r+1}\end{aligned}$$

since $\binom{k}{r-1} = \binom{k}{k+1} = 0$ by usual definition. It is now sufficient to prove the sum of binomial coefficients.

$$\binom{k}{r} + \binom{k}{r-1} = \frac{k!}{r!(k-r)!} + \frac{k!}{(r-1)!(k-r+1)!} = \frac{k!(k-r+1)+k!r}{r!(k-r+1)!} = \frac{k!(k+1)}{r!(k+1-r)!} = \frac{(k+1)!}{r!(k+1-r)!}$$

Definition 2.1.15. Suppose R is a ring, and $x \in R$ some element. x is a left zero divisor if there exists some $y \neq 0$ such that $xy = 0$; x is a right zero divisor if there exists some $y \neq 0$ such that $yx = 0$.

Definition 2.1.16. R is an integral domain if $xy = 0$ implies $x = 0$ or $y = 0$ for all $\{x, y\} \subset R$. That is, the only zero divisor is $0 \in R$.

Definition 2.1.17. Suppose R is a ring, and $x \in R$ some element. x is a unit if there exists $y \in R$ such that $xy = yx = 1_R$, i.e. there exists a multiplicative inverse. This implies that we can use cancellation when dealing with units, since we can multiply on both the left and the right its multiplicative inverse $x^{-1} = y$.

Remark 2.1.18. The word 'unit' here is significantly different as the word 'unit' in analysis; units need not have a norm equal to 1 here, for example when in a field, every nonzero element has a multiplicative inverse by definition, and hence is a 'unit' in algebra, but don't you dare write in your analysis homework that 2 is a unit.

Proposition 2.1.19. The set of units in R is a subgroup of the multiplicative monoid $(R^\star, \cdot, 1)$.

Proof. Suppose x, y are units; then x^{-1}, y^{-1} exist. By definition of a unit, 0 is not a unit, so all units are in $R^\star$. There is closure, since $(xy)^{-1} = y^{-1}x^{-1}$. Associativity is inherited, and 1 is its own inverse by definition. Lastly, it is obvious that $(x^{-1})^{-1} = x$, just by definition, so inverses exist.

2.2 Matrix Rings

Remark 2.2.1. We shall establish the following convention in this section:

(i) a a lowercase symbol denotes a generic element in a set;
(ii) $\underline{a}$ an underlined symbol denotes a vector; and
(iii) $\mathbf{A}$ a bold symbol (usually uppercase) denotes a matrix quantity.

Note that sometimes these definitions are blurry, as such quantities can be expressed in different ways; in that case, these notations are merely the way the author thinks of them.

Proposition 2.2.2. Suppose R is a ring. Then $R^{n\times n}$, the set of $n \times n$ matrices with entries in R, forms a ring with entry-wise addition and the usual matrix multiplication.

Proof. Check the ring axioms yourself.

Remark 2.2.3. We shall use bold fonts to represent matrices in this document. In particular, $\mathbf{I} = \mathbf{I}_n$ is the $n \times n$ identity matrix, and $\mathbf{0} = \mathbf{0}_n$ is the $n \times n$ zero matrix. $\mathbf{e}_{ij}$ will represent a matrix with 1 at the ith row and jth column, with zeroes everywhere else; so we can write $(a_{ij}) = \sum_{ij} a_{ij}\mathbf{e}_{ij}$.

Remark 2.2.4. For ease of reference, we shall write down the rules of matrix multiplication. Suppose $\mathbf{A} = (a_{ij}) \in R^{m\times n}$ and $\mathbf{B} = (b_{ij}) \in R^{n\times p}$, then $\mathbf{C} = \mathbf{AB} = (c_{ij}) \in R^{m\times p}$ is given by

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

Definition 2.2.5. Suppose R is a commutative ring. A function $\det\colon R^{n\times n} \to R$ is called a determinant if it is defined by the following three rules:

(a) $\det \mathbf{I} = 1$;

(b) If $\sigma \in S_n$ is a row permutation, and $\mathbf{A} \in R^{n\times n}$, then $\det(\sigma\mathbf{A}) = \operatorname{sgn}(\sigma)\det(\mathbf{A})$; and

(c) det is an n-linear function with respect to rows, that is, for some arbitrary ith row, assuming all other rows are the same,

$$\det \begin{bmatrix} \vdots \\ au + bv \\ \vdots \end{bmatrix} = a \det \begin{bmatrix} \vdots \\ u \\ \vdots \end{bmatrix} + b \det \begin{bmatrix} \vdots \\ v \\ \vdots \end{bmatrix}$$

Proposition 2.2.6 (Uniqueness of the determinant)**.** The determinant exists and is unique.

Proof. We claim that if $\mathbf{A} = (a_{ij})$, then

$$\det(\mathbf{A}) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}a_{2\sigma(2)}\dots a_{n\sigma(n)}$$

is a determinant.

We can first check that $\det(\mathbf{I}) = 1$ since $a_{ij} = 0$ if and only if $i \neq j$, so any σ that is not the identity inside the sum produces 0.

Now suppose we permute the rows by $\tau \in S_n$. Then we are simply sending all $a_{ij} \mapsto a_{\tau(i)j}$, so via a change of variables $\upsilon\tau = \sigma$, and as the sum over the $\tau(i)$ is the same as sum over i,

$$\begin{aligned}\det(\tau\mathbf{A}) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{\tau(i)\sigma(i)} = \sum_{\upsilon\in S_n} \operatorname{sgn}(\upsilon\tau) \prod_{i=1}^{n} a_{\tau(i)\upsilon\tau(i)} \\ &= \operatorname{sgn}(\tau) \sum_{\upsilon\in S_n} \operatorname{sgn}(\upsilon) \prod_{i=1}^{n} a_{i\upsilon(i)} = \operatorname{sgn}(\tau)\det(\mathbf{A})\end{aligned}$$

The n-linear condition is obvious from the definition of the determinant, since every summand $\prod a_{i\sigma(i)}$ contains exactly one term from the the ith row. Hence, when all other rows are kept the same, the determinant is a sum of a constant coefficient times the ith row term, which is by definition, linear. Combined together this proves existence.

To prove uniqueness, suppose $\mathbf{A} = (a_{ij})$ again. Then the ith row is a vector $\underline{a}_{i\star} = a_{i1}\underline{e}_1 + \dots + a_{in}\underline{e}_n$, where $\underline{e}_j$ is a basis row vector for the jth coordinate. Then the determinant must be

$$\det(\mathbf{A}) = \det \begin{bmatrix} \sum_t a_{1t}\underline{e}_t \\ \sum_t a_{2t}\underline{e}_t \\ \vdots \\ \sum_t a_{nt}\underline{e}_t \end{bmatrix}$$

which by the n-linear condition means the determinant must be a linear combination of $\det\left(\begin{bmatrix} \underline{e}_{\alpha_1} & \dots & \underline{e}_{\alpha_n} \end{bmatrix}^\intercal\right)$, where α_i is a choice between 1 to n. Since we have to accomodate all permutations (by condition (b)), all combinations must be in there, and we need to sign of the permutation to be part of the coefficient. Lastly, since the identity must return 1, we are forced to conclude that we cannot have another factor in there, so the coefficient must only be the sign.

Remark 2.2.7. We shall discuss the determinant, especially with how it is algorithmically defined, further in Section **??** for linear algebra.

Definition 2.2.8. Suppose $\mathbf{A} \in R^{n\times n}$. We denote the submatrix formed by removing the ith row and the jth column as $\mathbf{M}_{ij}^{\mathbf{A}}$ or simply $\mathbf{M}_{ij}$. The determinant of this submatrix is called a minor, or sometimes a first minor $m_{ij} = m_{ij}^{\mathbf{A}} = \det \mathbf{M}_{ij}^{\mathbf{A}}$. We can similarly define a second, third, or kth minor by removing two, three, or k rows and columns from $\mathbf{A}$.

Theorem 2.2.9 (Laplace Expansion for the Determinant)**.** Suppose $\mathbf{A} = (a_{ij}) \in R^{n\times n}$. Then

$$\det \mathbf{A} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} m_{ij}$$

for any $1 \le i \le n$.

Proof. We shall first prove the case of expansion along the first row. We denote $\tau_k = (1k)$ and $tau_1 = 1 \in S_n$ as swapping the first row with the others, and S_{n-1} as the permutation of all rows except the first. Then we can clearly write the determinant as

$$\det \mathbf{A} = \sum_{k=1}^{n} \sum_{\sigma\in S_{n-1}} \operatorname{sgn}(\tau_k\sigma) \prod_{i=1}^{n} a_{i\tau_k\sigma(i)} = \sum_{k=1}^{n} \operatorname{sgn}(\tau_k) a_{1k} \sum_{\sigma\in S_{n-1}} \operatorname{sgn}(\sigma) \prod_{i=2}^{n} a_{i\tau_k\sigma(i)}$$

But the second summation is effectively the definition of the determinant, but with the first row, and the kth column removed. Notice that there is a sign change since the effective odd/even column numbering has changed for the first $k-1$ rows, which we know to be a $(k-1)$-cycle that has a sign $(-1)^{k-2} = (-1)^k$. This completes the first part of the proof as

$$\det \mathbf{A} = a_{11}m_{11} + \sum_{k=2}^{n} \operatorname{sgn}(\tau_k) a_{1k} (-1)^k m_{1k} = \sum_{k=1}^{n} (-1)^{1+k} a_{1k} m_{1k}$$

The expansion along the ith row is simply an expansion along the first row after shuffling the first i rows, which is a permutation of sign $i-1$. Hence we multiply by $(-1)^{i-1}$ by the definition of the determinant and that yields our final answer.

$$\det \mathbf{A} = (-1)^{i-1} \sum_{k=1}^{n} (-1)^{1+k} a_{ik} m_{ik} = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} m_{ik}$$

Definition 2.2.10. Suppose R is a commutative ring, and $\mathbf{A} \in R^{n\times n}$ is a square matrix. We call the matrix $\operatorname{adj} \mathbf{A} \in R^{n\times n}$ that makes $(\operatorname{adj} \mathbf{A})\mathbf{A} = \mathbf{A}(\operatorname{adj} \mathbf{A}) = (\det \mathbf{A})\mathbf{I}$ the adjugate matrix, or the classical adjoint. This is not to be confused with the more common notion of an adjoint, which is the conjugate transpose of a matrix.

Proposition 2.2.11. The adjugate is given by the transpose of the cofactor matrix $\mathbf{C}$. More specifically, if $\mathbf{C} = (c_{ij})$, then its entries are $c_{ij} = (-1)^{i+j} m_{ij}$.

Proof. Clearly $\operatorname{adj} \mathbf{A} = (d_{ij})$ where $d_{ij} = (-1)^{i+j} m_{ji}$. If $\mathbf{A} = (a_{ij})$, then by definition of matrix multiplication we have $\mathbf{A}(\operatorname{adj} \mathbf{A}) = (b_{ij})$, with

$$b_{ij} = \sum_{k=1}^{n} a_{ik} d_{kj} = \sum_{k=1}^{n} a_{ik} (-1)^{k+j} m_{jk} = \sum_{k=1}^{n} (-1)^{j+k} a_{ik} m_{jk}$$

Notice that if $i = j$, then this is exactly the definition of the determinant by Laplace's expansion. Hence the entries on the main diagonal must be equal to $\det(\mathbf{A})$.

Now it suffices to prove that all off-diagonals are 0. Since $i \neq j$, we can replace row j with row i in $\mathbf{A}$, which we will denote this new matrix a $\mathbf{A}'$; as the minor m_{jk} removes the jth row anyways, $m_{jk}^{\mathbf{A}} = m_{jk}^{\mathbf{A}'}$. But since the ith row of the old matrix $\mathbf{A}$ is the jth row of the new matrix $\mathbf{A}'$, $a_{ik} = a'_{jk}$, so b_{ij} is again, by Laplace's expansion, the determinant of the new matrix $\det \mathbf{A}'$. But clearly $\det \mathbf{A}' = 0$, as it has a duplicate row.

Left multiplication by the adjugate yields the same result by simple computation.

Theorem 2.2.12. Suppose R is a commutative ring, and $\mathbf{A} \in R^{n\times n}$. Then $\mathbf{A}^{-1} \in R^{n\times n}$ exists if and only if $(\det \mathbf{A})^{-1} \in R$ exists.

Proof. By the definition of the adjugate, $(\det \mathbf{A})^{-1} \operatorname{adj} \mathbf{A} = \mathbf{A}^{-1}$. It is now clear that one cannot exist without the other.

2.3 Quaternions

Lemma 2.3.1. There exists solutions to polynomial equations with real-valued coefficients that do not reside in the reals. That is, $\mathbb{R}$ is not an algebraically closed field.

Proof. The counterexample is $x^2 + 1 = 0$, requiring $\pm\sqrt{-1}$ as solutions.

Remark 2.3.2. This is historically the motivation as to constructing the complex numbers $\mathbb{C}$. However, it does not seem possible to construct even larger fields via this method.

Theorem 2.3.3 (Fundamental Theorem of Algebra)**.** For a polynomial equation of degree n with complex-valued coefficients, there exists exactly n solutions in $\mathbb{C}$ counted with multiplicity. That is, $\mathbb{C}$ is algebraically closed.

Proof. We shall first formalize the above statement. Suppose we have a polynomial $p(z) = \sum_{i=0}^{n} a_i z^i$. We wish to prove that this has n solutions, but it is sufficient to prove that it has one solution, because by factoring out that solution, one would obtain a polynomial one degree lower, and by induction that would complete our argument.

We can assume a monic polynomial $a_n = 1$, since multiplication by a factor does not change the roots. Let $\mu = \inf_{z\in\mathbb{C}} |p(z)|$. We wish to show that $\mu = 0$, and that the infimum is attained at some $z_0 \in \mathbb{C}$. For some arbitrary $|z| = R$ on a circle,

$$|p(z)| = |z|^n \left|1 + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n}\right| \geq |z|^n \left(1 - \frac{|a_{n-1}|}{|z|} - \cdots - \frac{|a_0|}{|z|^n}\right) = R^n \left(1 - \frac{|a_{n-1}|}{|z|} - \cdots - \frac{|a_0|}{|z|^n}\right)$$

which tends to infinity as $R \to \infty$. Hence we can conclude there exists some $R_0 > 0$ such that $|p(z)| \geq \mu + 1$. Focusing on inside this circle of radius R_0, $|p|$ is continuous, and $\{z : |z| \leq R_0\}$ is compact, so analysis tells us the infimum of $|p|$ inside this region is attained; tacked on the fact that the infimum outside of the circle must be larger, the global infimum μ must be the same as the one inside the circle.

Now suppose, by way of contradiction, that $\mu > 0$. Let $q(z) = p(z_0 + z)/p(z_0)$, and $q(0) = 1$. As we know $q(z)$ is also a polynomial of degree n, we can write $q(z) = 1 + b_k z^k + \cdots + b_n z^n$, where b_k is the first nonzero coefficient. We see that $|q(z)| = |p(z_0 + z)|/\mu \geq 1$; but on the other hand, $|q(z)| = \left|1 + b_k z^k + \cdots + b_n z^n\right| \leq \left|1 + b_k z^k\right| + \sum_{m=k+1}^{n} |b_m||z|^m$. Writing $b_k z^k = |b_k| \frac{b_k}{|b_k|} z^k$, where $\frac{b_k}{|b_k|} = e^{it}$ for some t, and $z = re^{i\theta}$, this yields us $b_k z^k = |b_k| r^k e^{i(t+k\theta)}$. We can choose a value $\theta = (\pi - t)/k$, which evaluates to $b_k z^k = |b_k| r^k e^{i\pi} = -|b_k| r^k$, which will be strictly within -1 and 0 for r small enough. Then we have

$$|q(z)| = \left|q(re^{i\theta})\right| \leq 1 - |b_k| r^k + \sum_{m=k+1}^{n} |b_k| r^m = 1 - r^k \left(|b_k| - \sum_{m=k+1}^{n} |b_k| r^m\right) < 1$$

since the quantity inside the brackets is positive for r small enough. This is a contradiction, so $\mu = 0$, and there must be a root.

Remark 2.3.4. Despite the name, the Fundamemtal Theorem of Algebra is not a fundamental theorem in the study of algebra, but rather a theorem in analysis. A purely analytic proof is always provided in any analysis textbook at the undergraduate level; however, a partially algebraic proof is possible if we assume some facts from analysis, such as continuity and the intermediate value theorem.

Definition 2.3.5. The quaternions are a noncommutative division ring $\mathbb{H} = \{\left[\begin{smallmatrix} a & b \\ -\bar{b} & \bar{a} \end{smallmatrix}\right] : a, b \in \mathbb{C}\} \subseteq \mathbb{C}^{2\times 2}$.

Remark 2.3.6. This might not be the usual way people define quaternions, but it is equivalent, and lends itself to obviously being a matrix ring. The inverse is given by $\left[\begin{smallmatrix} a & b \\ -\bar{b} & a \end{smallmatrix}\right]^{-1} = \frac{1}{|a|^2+|b|^2}\left[\begin{smallmatrix} \bar{a} & -b \\ \bar{b} & a \end{smallmatrix}\right]$.

Proposition 2.3.7. The quaternions $\mathbb{H}$ can also be thought of as a 4-dimensional vector space over the reals $\mathbb{R}^4$ with the unit vectors $1, i, j, k$.

Proof. We shall write a quaternion as $\left[\begin{smallmatrix} a+ib & c+id \\ -c+id & a-ib \end{smallmatrix}\right]$, with $a, b, c, d \in \mathbb{R}$; then by simple verification one can find $a + bi + cj + dk$ with the multiplication table $i^2 = j^2 = k^2 = ijk = -1$, since we can represent the following:

$$i = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{bmatrix} \qquad j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad k = \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}$$

Definition 2.3.8. Suppose $q = \left[\begin{smallmatrix} a & b \\ -\bar{b} & a \end{smallmatrix}\right] \in \mathbb{H}$. The quaternion norm is defined as $\mathrm{N}(q) = |a|^2 + |b|^2$.

2.4 Ideals

Definition 2.4.1. A ring homomorphism is a function $\phi\colon R \to S$, where R, S are rings, with the properties

(i) $\phi\colon (R, +, 0) \to (S, +, 0)$ is a group homomorphism; and

(ii) $\phi\colon (R^\star, \cdot, 1) \to (S^\star, \cdot, 1)$ is a monoid homomorphism.

Definition 2.4.2. The kernel of a ring homomorphism is the preimage of 0, that is, $\ker(\phi) = \phi^{-1}(0)$. Note that this is a subgroup of $(R, +, 0)$.

Definition 2.4.3. Suppose R is a ring, and $I \subseteq R$. I is an ideal if it fits the following criteria:

(i) $I \subseteq (R, +, 0)$ is a subgroup; and

(ii) $\forall x \in I, \forall y \in R, \{xy, yx\} \subset I$.

Note that an ideal does not necessarily contain the unit 1, and therefore is not always a ring. A left ideal is defined with only $yx \in I$, and a right ideal is defined with only $xy \in I$. We shall sometimes denote this as $I \lhd R$, as one shall soon see its similarity to normal subgroups.

Definition 2.4.4. Suppose R is a ring, and $r \in R$ some arbitrary element. The left principal ideal is $Rr = \{yr : y \in R\}$, and the right principal ideal is $rR = \{ry : y \in R\}$. These two definitions coincide with R is a commutative ring, and we call it the principal ideal.

Lemma 2.4.5. Suppose R is a commutative ring, and $r \in R$. If $f\colon R \to R$, $x \mapsto xr$ (or rx) is a mapping, then f is surjective if and only if r is a unit.

Proof. Suppose r is a unit. Then for some $y \in R$, clearly $yr^{-1} \mapsto yr^{-1}r = y$. This is therefore surjective.

Suppose f is surjective. Then for all $y \in R$, there exists an element $x \in R$ such that $xr = y$. In particular, let $y = 1$ and we see that there is an inverse.

Remark 2.4.6. Ideals are typically generated by a set of generators $x_i \in S$, so elements are of the form $I = \{\sum_i r_i x_i : r_i \in R, x_i \in S\}$.

Definition 2.4.7. A Noetherian ring is a ring with every ideal being finitely generated.

Lemma 2.4.8. Suppose R is a ring, and $I \lhd R$ is an ideal. Then R/I forms a ring via $(x+I)(y+I) = (xy+I)$.

Proof. Clearly $(R, +, 0)/I$ readily forms an additive group, since I is an additive subgroup, and Proposition 1.6.4 informs us that it is normal.

Now suppose $\{r, r'\} \subset I$. Clearly $(x + r)(y + r') = xy + xr' + ry + rr' \in I$, since the last three terms are all in I; we are guaranteed closure. Next up the multiplicative unit is $1 + I$, which since $(1 + I)(x + I) = 1x + I = x + I = x1 + I = (x + I)(1 + I)$ gives us the identity. Associativity is inherited.

Corollary 2.4.9. $\pi\colon R \to R/I,\ x \mapsto x + I$ is the quotient homomorphism.

Proof. All properties are inherited, and it forms a ring.

Proposition 2.4.10. Suppoose R is a commutative ring, and I and J are ideals. The $I \cap J$, $I + J = \{x + y : x \in I, y \in J\}$, and $IJ = \{\sum_i x_i y_i : x_i \in I, y_i \in J\} \subseteq I \cap J$ are all ideals.

Proof. Suppose $\{x, y\} \subset I \cap J$. Then clearly the intersection is a subgroup. Moreover, by closure of each of I and J, xy is in both I and J. This proves $I \cap J$ is an ideal.

Suppose $\{x, x'\} \subset I$, and $\{y, y'\} \subset J$. Any $(x + y) + (x' + y') = (x + x') + (y + y') \in I + J$, associativity is given by R, $0 \in I$ and $0 \in J$ so $0 = 0 + 0 \in I + J$, and inverse is clearly $-x - y \in I + J$; $I + J$ is therefore an additive subgroup. Moreover, $(x + y)(x' + y') = xx' + xy' + yx' + yy' \in I + J$, since $xx' + xy' \in I$ and $yx' + yy' \in J$. This proves $I + J$ is an ideal.

Lastly, again suppose $x \in I$ and $y \in J$. We have closure simply by the summation definition, associativity is inherited from R, the empty sum is $0 \in IJ$, and the inverse is just $\sum_i -x_i y_i$, which since $-x_i \in I$, gives us the inverse; IJ is therefore an additive subgroup. It is also clear that this is in I and in J. Moreover, $(\sum_i x_i y_i)(\sum_j x_j y_j) = \sum_{ij} x_i y_i x_j y_j$ and since $y_i x_j y_j \in J$, we have closure under multiplication. This proves IJ is an ideal.

Proposition 2.4.11. Suppose $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is an ascending chain of ideals. Then $I = \bigcup_{i=1}^{\infty} I_i$ is an ideal.

Proof. Suppose $\{x, y\} \subset I$. Then $x \in I_m$ and $y \in I_n$ for some m, n. Without loss of generality let $I_m \subseteq I_n$, then $\{x, y\} \subset I_n$, so we have closure inside I_n, and hence inside I. Associativity is as per usual inherited from R. The identity $0 \in I_1 \subseteq I$. And lastly, if $x \in I$, then $x \in I_n$ for some n, so $-x \in I_n \subseteq I$. This proves that I is an additive subgroup.

Now suppose $x \in I$, and $r \in R$. Clearly $x \in I_n$ for some n and therefore $xr \in I_n \subseteq I$.

Definition 2.4.12. Suppose R is a ring, and $S \subseteq R$ a subset. The ideal generated by S is $(S) = \{\sum_i r_i s_i r_i' : s_i \in S, \{r_i, r_i'\} \subset R\}$. We call an ideal I finitely generated if $I = (S)$ for some finite S.

Definition 2.4.13. Suppose R is a ring, and $I \lhd R$ an ideal. We call I maximal (in R) if there are no ideals $J \lhd R$ such that $I \subseteq J \subseteq R$.

Proposition 2.4.14. Suppose R is a commutative ring. Then R is a field if and only if R has no nonzero proper ideals.

Proof. Suppose R is a field and I an ideal. If there exists an element $x \in I$, $x \neq 0$, by the definition of a field we have $x^{-1} \in R$. Then by definition of an ideal $1 = xx^{-1} \in I$, and again by closure, any element $r \in R$ woud therefore be $r = 1r \in I$. Hence $I = R$ is not a proper ideal.

Now suppose R has no proper ideals. Then if $x \in R$, then xR is an ideal, so if $xR \neq \{0\}$, $xR = R$, so there exists $y \in R$ such that $xy = 1$. We have found an inverse $x^{-1} = y$.

Corollary 2.4.15. Suppose R is a commutative ring, and I a maximal ideal. Then R/I is a field.

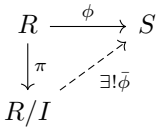
Proof. Since I maximal ideal, there does not exist any intermediate ideal $J \subseteq R$. By the third isomorphism theorem (proven below) there is no intermediate ideal J/I between the quotient ring R/I and $I/I = \{0\}$.

2.5 Homomorphisms and Isomorphisms

Remark 2.5.1. The isomorphism theorems work in a lot of algebraic structures (formally, it works in any universal algebra). We will number them the same way as we did for groups.

Theorem 2.5.2 (Universal Property of Quotient Rings)**.** Let R, S be commutative rings, and $I \lhd R$ be an ideal. Suppose $\pi\colon R \to R/I$ is the quotient homomorphism and $\phi\colon R \to S$ is any ring homomorphism with $I \subseteq \ker(\phi)$. Then there exists a unique ring homomorphism $\bar{\phi}\colon R/I \to S$ such that $\phi = \bar{\phi} \circ \pi$.

This is represented by the following commutative diagram:



Proof. We wish to prove uniqueness by assuming existence. Suppose $\phi = \bar{\phi} \circ \pi = \bar{\phi}' \circ \pi$. Since $I \subseteq \ker(\phi)$, all elements $x \in I$ obey $\phi(x) = 0$. Knowing that all elements in R belong in some coset $r + I$, all $r' \in r + I$ maps to $\phi(r') = \phi(r + x) = \phi(r) + \phi(x) = \phi(r)$, which tells us the image of each coset is a single element $\phi(r + I) = \{\phi(r)\}$. Now, seeing that π maps $r' \mapsto r + I$, its coset, by definition of a quotient mapping, if $\bar{\phi} \neq \bar{\phi}'$, there must be one such coset $r + I$ thata $\bar{\phi}(r + I) \neq \bar{\phi}'(r + I)$ disagrees on. However, this is a contradiction, because for all $r' \in r + I \subseteq R$, $\bar{\phi}'(r+I) = \bar{\phi}'(\pi(r')) = \phi(r') = \bar{\phi}(\pi(r')) = \bar{\phi}(r+I)$, contradicting with our assumed inequality above. Hence we have established uniqueness of $\bar{\phi}$.

We will now prove existence by constructing such a homomorphism. Let $\bar{\phi}\colon R/I \to S,\ r + I \mapsto \phi(r)$, mapping all cosets $r + I$ to the function output of its coset representative. Suppose some arbitrary element $r' \in r + I \subseteq R$ in an arbitrary coset. Then we know that there exists $x \in I$ such that $r' = r + x$, which allows us to conclude that

$$\phi(r') = \phi(r + x) = \phi(r) + \phi(x) = \phi(r) = \bar{\phi}(r + I) = \bar{\phi}(\pi(r'))$$

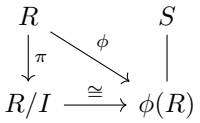
Theorem 2.5.3 (First Isomorphism Theorem for Rings)**.** Suppose $\phi\colon R \to S$ is a ring homomorphism, and $I = \ker(\phi)$. We have:

(a) $I \lhd R$, the kernel is an ideal;

(b) $\phi(R) \subseteq S$, the image is a subring; and

(c) $\phi(R) \cong R/I$, the image is uniquely isomorphic to the quotient ring.

This is represented by the following commutative diagram:



Proof. By the simple fact that ϕ is also an additive group homomorphism, the first group isomorphism theorem gives us that the kernel is an additive subgroup.

Now suppose some arbitrary $x \in \ker(\phi)$, and $y \in R$. Then clearly $\phi(xy) = \phi(x)\phi(y) = 0\phi(y) = 0 = \phi(y)0 = \phi(y)\phi(x) = \phi(yx)$. This proves statement (a).

Secondly, the homomorphism inherits all its properties from R, so its image must form a subring. In particular, the first group (monoid) isomorphism theorem guarantees us that the image will be an additive subgroup, and a multiplicative monoid. This proves statement (b).

The universal property guarantees a unique homomorphism $\bar{\phi}\colon R/I \to \phi(R)$ such that $\phi = \bar{\phi} \circ \pi$, π being the quotient homomorphism. By the first group isomorphism theorem, when applied to the additive group, we see that it is an isomorphism. This proves statement (c).

Theorem 2.5.4 (Second Isomorphism Theorem for Rings)**.** Suppose R is a ring, $S \subseteq R$ some subring, and $I \lhd R$ an ideal. We have:

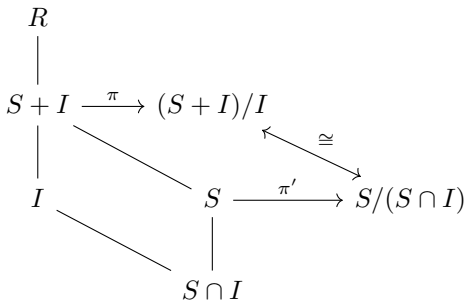
(a) $S + I = \{s + x : x \in S, x \in I\} \subseteq R$, the sum is a subring;

(b) $I \lhd S + I$, the ideal is also and ideal of the sum;

(c) $S \cap I \lhd S$, the intersection is an ideal of the subring; and

(d) $(S + I)/I \cong S/(S \cap I)$, these two quotients are isomorphic.

This is represented by the following commutative diagram:



Proof. By the second group isomorphism theorem, $S+I$ forms an additive subgroup. For $\{s, s'\} \subset S$ and $\{x, x'\} \subset I$, we see that $(s+x)(s'+x') = ss' + xs' + sx' + xx' \in S+I$, since $ss' \in S$ and $xs' + sx' + xx' \in I$, which gives us closure. Associativity is inherited from R, and the identity is $0 + 1 \in S + I$. This proves statement (a).

I already forms a group, and clearly $I = 0 + I \subseteq S + I$, so it is already a subgroup. By definition of an ideal, for all $x \in I$ and $y \in R$, $\{xy, yx\} \subset I$, so more specifically this holds for $y \in S + I \subseteq R$. This proves statement (b).

Suppose $\{x, x'\} \in S \cap I$. Then $x + x' \in S \cap I$, since there is closure for both S as a group, and I as an ideal (which is also a group). Associativity is always inherited, and the identity is $0 =\in S \cap I$ as $0 \in S$ and $0 \in I$ by definition. Lastly, additive inverses always exist in a subgroups S, I, so $-x \in S \cap I$. Hence $S \cap I \subseteq S$ is a subgroup.

Now, we need to check the multiplicative condition. Suppose $x \in S \cap I$, and $y \in S$. We see that by the definition of a subring, $\{xy, yx\} \subset S$; but also $\{xy, yx\} \subset I$ since $I \lhd R$ is an ideal, so it also works for elements $y \in S \subseteq R$. This proves statement (c).

By statements (c) & (d), these two quotients are well-formed. We now attempt to construct a homomorphism $\phi\colon S \to (S+I)/I,\ s \mapsto s + I$. We demonstrate that this a valid homomorphism, by showing that

$$\phi(s_1 s_2) = (s_1 s_2) + I = (s_1 + I)(s_2 + I) = \phi(s_1)\phi(s_2)$$
$$\phi(s_1 + s_2) = s_1 + s_2 + I = (s_1 + I) + (s_2 + I) = \phi(s_1) + \phi(s_2)$$

since s_1, s_2 are elements of R, so same logic as the quotient ring epimorphism applies.

We now want to show that ϕ is surjective. The elements $s + x \in S + I$ must belong in some coset $s + x + I$, which we now see is equivalent to $s + I$. By definition, ϕ maps $s \mapsto s + I$, so every coset is covered by ϕ, and therefore it is an epimorphism.

We can then demonstrate that $\ker(\phi) = S \cap I$. We can see that if $x \in S \cap I$, then $x \in I$, so $\phi(x) = x + I = I$, which gives us $S \cap I \subseteq \ker(\phi)$. On the other hand, if $x \in \ker(\phi)$, then $\phi(x) = x + I \subseteq I$, which requires $x \in I$, giving us $\ker(\phi) \subseteq S \cap I$. Hence $\ker(\phi) = S \cap I$.

Lastly, we apply the first isomorphism theorem, and prove that there exists a unique homomorphism between $S/(S \cap I) \cong (S + I)/I$.

Theorem 2.5.5 (Third Isomorphism Theorem for Rings)**.** Suppose R is a ring, $I \lhd R$ an ideal. Then:

(a) if S is a subring such that $I \subseteq S \subseteq R$, then $S/I \subseteq R/I$ is a subring;

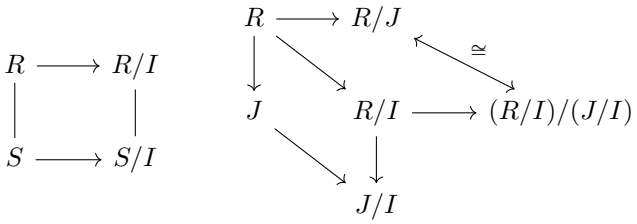
(b) a subring of R/I must be of the form S/I such that S is a subring with $I \subseteq S \subseteq R$;

(c) if J is an ideal such that $I \subseteq J \subseteq R$, then $J/I \lhd R/I$ is an ideal;

(d) an ideal of R/I must be of the form J/I such that $J \lhd R$ is an ideal with $I \subseteq J \subseteq R$; and

(e) if $J \lhd R$ is an ideal such that $I \subseteq J \subseteq R$, then $(R/I)/(J/I) \cong R/J$.

This is represented by the following commutative diagrams:



Proof. We first have to prove that $I \lhd S$, which is obvious because it is already an additive subgroup, and $\{xy, yx\} \in I$ for all $x \in I$ and $y \in R$ can be restricted to $y \in S \subseteq R$.

It is now easy to see that with the quotient homomorphism $\pi\colon R \to R/I$, the image of the subring $\pi(S) = S/I$, so by the first isomorphism theorem S/I forms a subring. This proves statement (a).

Suppose $S' \subseteq R/I$ is a subring. We can look at the preimage $\pi^{-1}(S')$, which since $0 \in S'$, we have $S' \supseteq \ker(\pi) = I$. Notice that the preimage of a ring is still a ring, because the correspondence given by the fourth group (monoid) isomorphism theorem when applied to the additive group and the multiplicative monoid forms a ring. This proves statement (b).

We now look at the quotient homomorphism $\pi\colon R \to R/I$, especially the image of the larger ideal $\pi(J) = J/I$. By the first group isomorphism theorem, $\pi(J)$ forms an additive group, and if $x \in J$ and $r \in R$, $\pi(x)\pi(r) = \pi(xr) \in \pi(J) = J/I$, and similarly this holds for $\pi(r)\pi(x)$. Hence J/I is an ideal, proving statement (c).

Suppose $J' \lhd R/I$ is an ideal. We can look at the preimage $\pi^{-1}(J')$, which since $0 \in J'$, we have $J' \supseteq \ker(\pi) = I$. Notice that the preimage $\pi^{-1}(J') = J' + I$ is an ideal, which is given by Proposition 2.4.10. Hence we have the preimage being an ideal J, so $J' = \pi(J) = J/I$, proving statement (d).

We can now attempt to construct a homomorphism $\phi\colon R/I \to R/J$, $r + I \mapsto r + J$. This is valid because by the universal property, we have $\pi\colon R \to R/I$ and $\eta\colon R \to R/I$, so there is a unique homomorphism that makes $\eta = \phi \circ \pi$. We can show that this is surjective, since the J-cosets partition R, so each J-coset must have some element $r + J$ that represents it, and clearly this element $r + I$ in the I-cosets must get sent to it, alongside all other elements in that I-coset.

We claim the kernel is $\ker(\phi) = J/I$. Observe that $\ker(\eta) = J$ and $\ker(\pi) = I$, so ϕ must map all the I-cosets that are represented by elements of J into 0.

Lastly, we invoke the first isomorphism theorem, which gives us $\ker(\phi) = J/I \lhd R/I$, making our quotient $(R/I)/(J/I)$ valid, and also that $(R/I)/\ker(\phi) = (R/I)/(J/I) \cong R/J$, proving statement (e).

Theorem 2.5.6 (Fourth Isomorphism Theorem for Rings)**.** Suppose R is a ring, $I \lhd R$ some ideal, and $\pi\colon R \to R/I$, $x \mapsto x + I$ the quotient homomorphism. Then π is a bijection between the subrings of R/I and the subrings of R containing I; and is also a bijection between ideals of R/I and ideals (and subrings) of R containing I.

Proof. This is merely a corollary of the third isomorphism theorem. Statements (a) and (b) prove the correspondence between subrings, while statements (c) and (d) prove the correspondence between ideals.

2.6 Field of Fractions

Definition 2.6.1. Suppose R is a ring, and $\zeta\colon \mathbb{Z} \to R$ the canonical homomorphism. If ζ is injective, we call R having characteristic 0. If on the other hand ζ is not injective, then the kernel clearly must be some ideal $\ker(\zeta) = n\mathbb{Z}$, and we call R having characteristic n.

Proposition 2.6.2. Suppose p prime. Then the ring $\mathbb{Z}/p\mathbb{Z}$ must be a field.

Proof. We first prove that $p\mathbb{Z}$ is maximal in $\mathbb{Z}$, i.e. there does not exist an ideal $n\mathbb{Z}$, such that $p\mathbb{Z} \subsetneq n\mathbb{Z} \subsetneq \mathbb{Z}$. Clearly if $p\mathbb{Z} \subseteq n\mathbb{Z}$, then $n \mid p$, which tells us $n = 1$ or p, which is either $\mathbb{Z}$ or $p\mathbb{Z}$. Hence the only ideals of $\mathbb{Z}$ that contain $p\mathbb{Z}$ are $\mathbb{Z}$ and $p\mathbb{Z}$.

By (the contraposition of) the third isomorphism theorem, then the only ideals of $\mathbb{Z}/p\mathbb{Z}$ are itself and $p\mathbb{Z}/p\mathbb{Z} = \{0\}$, so there does not exists proper ideals of $\mathbb{Z}/p\mathbb{Z}$. Then by Proposition 2.4.14, $\mathbb{Z}/p\mathbb{Z}$ is a field.

Definition 2.6.3. For some prime p, we call $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ the finite field of p elements.

Lemma 2.6.4. Fields do not have nonzero zero divisors.

Proof. If $x, y \neq 0$ and $xy = 0$, x^{-1} exists, so $x^{-1}xy = y = 0x^{-1} = 0$ which imply $y = 0$, which is a contradiction in itself.

Lemma 2.6.5. Suppose F is a field, and $\zeta\colon \mathbb{Z} \to F$ is the canonical homomorphism. Then either ζ is injective, or $\ker(\zeta) = p\mathbb{Z}$ for some prime p.

Proof. If ζ is not injective, then clearly the kernel is some $\ker(\zeta) = n\mathbb{Z}$. Suppose, by way of contradiction, that $n = ab$ such that $1 < a, b < n$. Then $0 = \zeta(n) = \zeta(ab) = \zeta(a)\zeta(b)$, and since a, b are not elements of $n\mathbb{Z}$, $\zeta(a), \zeta(b)$ are nonzero, and in particular, they are zero divisors. But that contradicts the lemma above. Hence n must be prime.

Theorem 2.6.6. The characteristic of a field is unique, and it is either 0 or a prime p.

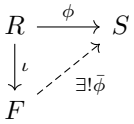
Proof. The lemma above already proves that the characteristic is either 0 or prime. It is now sufficient to prove uniqueness. Suppose $\mathbb{F}_p, \mathbb{F}_q \subseteq F$ some field. then $\mathbb{F}_p \subseteq F$ implies $p1 = 0$, while $\mathbb{F}_q \subseteq F$ implies $q1 = 0$, But $\gcd(p, q) = 1$, which implies $1 = 0$, which is considered a trivial ring and not a field.

Definition 2.6.7 (Universal Property of Field of Fractions)**.** Suppose R is a commutative domain. We call F its field of fractions or its quotient field if:

(i) there exists an monomorphism $\iota\colon R \to F$; and

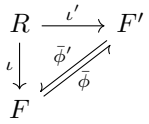
(ii) for any field S, if $\phi\colon R \to S$ is a monomorphism, then there exists a unique $\bar{\phi}\colon F \to S$ such that $\phi = \bar{\phi} \circ \iota$.

This is represented by the following commutative diagram:



Theorem 2.6.8 (Existence and Uniqueness of Field of Fractions)**.** For any commutative domain R, its field of fractions F exists and is unique up to isomorphism.

Proof. Again, as with all universal properties, we first prove uniqueness assuming existence. Suppose, by way of contradiction, that F and F' are both fields of fractions. Then by definition there exists $\iota\colon R \to F$ injective, and for any field S, in particular F', $\iota'\colon R \to F'$ injective such that there exists a unique $\bar{\phi}\colon F \to F'$ where $\iota' = \bar{\phi} \circ \iota$. But same can be said for $\iota'\colon R \to F'$ injective, for any field S, in particular F', $\iota\colon R \to F$ injective such that there exists a unique $\bar{\phi}'\colon F' \to F$ where $\iota = \bar{\phi}' \circ \iota'$.



Then following the definitions, we come to these two conclusions:

$$\bar{\phi}' \circ \bar{\phi} \circ \iota = \bar{\phi}' \circ \iota' = \iota \implies \bar{\phi}' \circ \bar{\phi} = \mathrm{id}_F$$
$$\bar{\phi} \circ \bar{\phi}' \circ \iota' = \bar{\phi} \circ \iota = \iota' \implies \bar{\phi} \circ \bar{\phi}' = \mathrm{id}_{F'}$$

which by definition means $\bar{\phi}' = \bar{\phi}^{-1}$. Hence $\bar{\phi}$ is a bijection, telling us that $F \cong F'$ are isomorphic.

Now we prove existence. Suppose we have tuples $(x, y) \in R \times R^\star$, i.e. the standard condition that the denominator does not equal 0. We shall define an equivalence relation $(a, b) \sim (c, d)$ if $ad = bc$. We check the three conditions: $(a, b) \sim (a, b)$ since $ab = ab$ (reflexive); $(a, b) \sim (c, d)$ implies $ad = bc$ implies $cb = da$ implies

$(c,d) \sim (a,b)$ (symmetric); and $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ implies $ad = bc$ and $cf = de$, so $adcf = bcde$, when cancelling out cd we have $af = be$, which implies $(a,f) \sim (b,e)$ (transitive).

We define $F = (R \times R^\star)/\sim$, i.e. elements are $(x,y) \in R \times R^\star$ without unique representation. We shall denote elements of F as $\overline{(x,y)} \in F$. This forms a ring with addition and multiplication defined as

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)} \qquad \overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$$

The ring axioms are obvious, and essentially encompass the operations on $\mathbb{Q}$.

Lastly, we check that it satisfies the morphisms. We define $\iota\colon R \to F,\ x \mapsto \overline{(x,1)}$, and for some arbitrary $\phi\colon R \to S$, let $\bar{\phi}\colon F \to S,\ \overline{(x,y)} \mapsto \phi(x)\phi(y)^{-1}$. We check that for arbitrary $(x,y) \in R \times R^\star$,

$$\bar{\phi}(\iota(x))\bar{\phi}(\iota(y))^{-1} = \bar{\phi}\overline{(x,1)}\bar{\phi}\overline{(y,1)}^{-1} = \phi(x)\phi(1)^{-1}\phi(y)^{-1}\phi(1) = \phi(x)\phi(y)^{-1}$$

so $\phi = \bar{\phi} \circ \iota$, and our definition is one such set of morphisms, proving existence.

Remark 2.6.9. Notice that this time we use a universal property as a definition for an algebraic structure. This is a way to generalize constructions in terms of morphisms instead of elements, which allow us to define things mostly up to isomorphism.

Remark 2.6.10. Because of how we define $\bar{\phi}$, it is common to write $\overline{(a,b)} = ab^{-1} = a/b$, which is the common notation for fractions.

2.7 Polynomial Rings

Definition 2.7.1. For some commutative ring R, we call the polynomials with coefficients in R the polynomial ring $R[x] = \{\sum_{i=0}^{n} a_i x^i : a_i \in R, n \geq 0\}$. This can be represented as an infinite sequence of coefficients with finitely many nonzero terms (with finite support), i.e. $R[x] \cong \bigoplus_{i=0}^{\infty} R$.

Remark 2.7.2. Notice that the indeterminate x is not restricted to any set, and can be not in R; an analogy is that although we often look at polynomials $\mathbb{R}[x]$, the solutions (and thereofre the indeterminates x that we investigate) are sometimes in the bigger field $\mathbb{C}$.

Remark 2.7.3. We shall again explore more of the direct sum in Section **??** for linear algebra.

Proposition 2.7.4. $R[x]$ forms a ring with addition $\sum a_i x_i + \sum b_i x_i = \sum (a_i + b_i) x_i$ and multiplication $(\sum a_i x_i)(\sum b_j x_j) = \sum_k (\sum_{i+j=k} a_i b_j) x_k$.

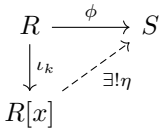
Proof. Addition is term-wise and inherits all properties from R. Multiplication is clearly closed, associative, commutative, and has an identity $1 \in R \subseteq R[x]$.

Theorem 2.7.5 (Universal Property of Polynomial Rings)**.** Suppose R, S are commutative rings, and $R[x]$ is a univariate polynomial ring. For all homomorphisms $\phi\colon R \to S$, and for all $u \in S$, there exists a unique homomorphism $\eta\colon R[x] \to S,\ x \mapsto u$, such that $\phi = \eta \circ \iota_k$ for all $k \in \mathbb{Z}_0^+$.

This can be represented by the logical statement

$$\forall S \in \textbf{Ring},\ \forall \phi \in \mathrm{Hom}(R,S),\ \forall u \in S,\ \exists! \eta\colon R[x] \to S,\ x \mapsto u,\ \phi = \eta \circ \iota_k$$

and the following commutative diagram:



Proof. We prove uniqueness first. Suppose, by way of contradiction, that there exists $\eta \neq \eta'$ that maps $R[x] \to S$. Since we know $R[x] \cong \bigoplus_k R$, any element $p \in R[x]$ can be written as $p = \sum_k \iota_k(a_k)$ for some $a_k \in R$. Assume η and η' differ at p. Then clearly $\eta(p) = \sum_k (\eta \circ \iota_k)(a_k)$, and same goes for η', but that implies $\eta' \circ \iota_k \neq \eta \circ \iota_k = \phi$ at at least one $a_k \in R$, which is a contradiction.

Now we prove existence. Let $\iota_k \colon R \to R[x],\ a \mapsto a_k x^k$, and $\eta \colon R[x] \to S,\ b \mapsto \phi(b),\ x \mapsto u$, i.e. evaluating the polynomial at $x = u$. We see that the morphisms follow as expected:

$$\sum_k \eta(\iota_k(a_k)) = \sum_k \eta(a_k x^k) = \sum_k \eta(a_k)\eta(x)^k = \sum_k \phi(a_k)u^k$$

Definition 2.7.6. Suppose R is a commutative ring. We can inductively define the multivariate polynomial ring as $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$.

Theorem 2.7.7. Suppose R is a commutative ring, $R[x_1, x_2, \ldots, x_n]$ a polynomial ring in n variables and for some permutation of variables $\sigma \in S_n$, $y_i = x_{\sigma(i)}$, $R[y_1, y_2, \ldots, y_n]$ another polynomial ring in n variables. Then $R[x_1, x_2, \ldots, x_n] \cong R[y_1, y_2, \ldots, y_n]$, that is, polynomial rings with the same number of variables are unique up to isomorphism.

Proof. By the universal property, univariate polynomial rings are unique up to isomorphism. Hence we have $R[x_1] \cong R[y_1]$. Then by induction, suppose $R[x_1, x_2, \ldots, x_k] \cong R[y_1, y_2, \ldots, y_k]$. Then clearly we can write a bijection β between these two, and suppose $a_i \in R[x_1, x_2, \ldots, x_k]$. Elements of $R[y_1, y_2, \ldots, y_{k+1}]$ can now be written as $\sum_i \beta(a_i) y_{k+1}^i$, so we have $R[x_1, x_2, \ldots, x_k][y_{k+1}] \cong R[y_1, y_2, \ldots, y_{k+1}]$. By the universal property again, we have $R[x_1, x_2, \ldots, x_{k+1}] \cong R[x_1, x_2, \ldots, x_k][y_{k+1}]$, so $R[x_1, x_2, \ldots, x_{k+1}] \cong R[y_1, y_2, \ldots, y_{k+1}]$.

Definition 2.7.8. Suppose we have $R \subseteq S$ two rings, and a polynomial ring $R[x]$. Choosing an arbitrary element $u \in S$, we can write the evaluation morphism as $\eta_u \colon R[x] \to S,\ x \mapsto u$. We call the image the subring generated by u over R, commonly written as $\eta_u(R[x]) = R[u] \subseteq S$.

Proposition 2.7.9. $R[u] \cong R[x]/I$, where $I = \{p(x) \in R[x] : p(u) = 0\}$.

Proof. A direct consequence of the first isomorphism theorem.

Definition 2.7.10. Suppose $R \subseteq S$ both fields, and $R[x]$ is a polynomial ring. For some arbitrary $u \in S$, consider the evaluation morphism $\eta_u \colon R[x] \to S,\ x \mapsto u$. If the kernel is $\ker(\eta_u) = \{0\}$, then $R[u] \cong R[x]$, and we call u transcendental; if on the other hand, the kernel $I = \ker(\eta_u) \neq \{0\}$, then $R[u] \cong R[x]/I$, and we call u algebraic, in the sense that u satisfies polynomials, in particular the ones in I.

Theorem 2.7.11. Suppose $R \subseteq S$ both fields, and $R[x]$ a polynomial ring. Suppose $I \subseteq R[x]$ is any ideal. If I contains any constant $r \in R$, $r \neq 0$ then it is not a substitution kernel, i.e. it cannot be the kernel for η_u for any $u \in S$.

Proof. By way of contradiction, suppose $r \in I$ and $r \in R$, $r \neq 0$, and that there exists some $u \in S$ such that $R[u] \cong R[x]/I$. Without loss of generality, let us choose the smallest r. Now, this would imply that $r = 0$ in S. Hence S must have characteristic r. Then this tells us R must also have characteristic r, since $R \subseteq S$. But this is a contradiction, as this would make $R \cong S \cong \mathbb{Z}/r\mathbb{Z}$; as $R \subseteq R[u] \subseteq R[x] \subseteq S$, then the kernel must be $\{0\}$.

Definition 2.7.12. We define a function $\deg \colon R[x] \to \mathbb{Z}_0^+$ that gives the degree of a polynomial, which is the largest n such that the coefficient $a_n \neq 0$.

Lemma 2.7.13. Suppose $f(x) = \sum_i a_i x^i$ and $g(x) = \sum_i b_i x^i$ both elements of $R[x]$. Then

(a) $\deg(f + g) \leq \max\{\deg f, \deg g\}$; and

(b) $\deg(fg) = \deg f + \deg g$.

Proof. If $\deg f \neq \deg g$, then clearly under addition, the leading term remains the leading term of the polynomial with the larger degree. If $\deg f = \deg g$, if the two leading terms do not cancel out, the degree remains the same; if they do cancel out, then the degree must be smaller. This proves statement (a).

The product of the leading terms $a_n x^n$ and $b_m x^m$ must be $a_n b_m x^{n+m}$, so the degree is the sum of the leading terms; notice all other terms will multiply to a smaller power of x. This proves statement (b).

Proposition 2.7.14. Suppose R a commutative ring, and $R[x]$ its polynomial ring. Let $f, g \in R[x]$, and we have $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. We can define long division on polynomials as $b_m^k f(x) = q(x)g(x) + r(x)$ for some arbitrary $k \in \mathbb{N}$, and $\{q, r\} \in R[x]$. Along with the degree function, this allows for the Euclidean algorithm to apply, with the criteria that $\deg r < \deg g$ or $r = 0$.

Proof. We first consider the case that $\deg f < \deg g$. Then let $b_m^0 = 1$, and $q(x) = 0$, so $r(x) = f(x)$, and immediately $\deg r = \deg f < \deg g$.

We now consider the case that $\deg f \geq \deg g$. We can construct the first term of $q(x)$ as $q_1(x) = a_n x^{n-m}$, so that

$$f_1(x) = b_m f(x) - a_n x^{n-m} g(x) = \sum_{i=0}^{n} a_i b_m x^i - \sum_{i=n-m}^{n} a_n b_{i-n+m} x^i = \sum_{i=0}^{n-1} a_i b_m x^i - \sum_{i=n-m}^{n-1} a_n b_{i-n+m} x^i$$

leaving us with an f_1 that has at least one degree lower than f. We can recursively repeat this process

$$f_{i+1}(x) = b_m f_i(x) - q_{i+1}(x)g(x) = b_m f_i(x) - a_{\deg f_i} x^{\deg f_i - m} g(x)$$

until the $\deg f_k$ drops below $\deg g$, which allows us to write down $r(x) = f_k(x)$ at that point, and $q(x) = \sum_{i=1}^{k} q_i(x)$.

$$q(x)g(x) + r(x) = \sum_{i=1}^{k} q_i(x)g(x) + f_k(x) = \sum_{i=1}^{k-1} q_i(x)g(x) + b_m f_{k-1}(x) = \cdots = b_m^k f(x)$$

There is at most $n - m + 1$ steps to this induction, so $k \leq n - m + 1$.

Remark 2.7.15. Notice that this long division is not unique, as we can make k arbitrarily larger than the choice above, and we merely have to multiply $q(x)$ by that difference.

Remark 2.7.16. We shall discuss more of Euclidean domains in Section 2.8 for unique factorization domains.

Proposition 2.7.17. Suppose F a field, and $F[x]$ its polynomial ring. Let $f, g \in F[x]$, and we have $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. We can define long division on polynomials as $f(x) = q(x)g(x) + r(x)$, with $\{q, r\} \in F[x]$. Along with the degree function, this allows for the Euclidean algorithm to apply, with the criteria that $\deg r < \deg g$ or $r = 0$.

Proof. We have the same base case as above, where if $\deg f < \deg g$, let $q(x) = 0$, so $r(x) = f(x)$ and $\deg r = \deg f < \deg g$.

Now the inductive case is much easier. Let $f(x) = f_0(x)$. Using the same process, alternately calculate

$$q_i(x) = \frac{a_{\deg f_{i-1}}}{b_m} x^{\deg f_{i-1} - m}$$

$$f_{i+1}(x) = f_i(x) - q_{i+1}(x)g(x) = f_i(x) - \frac{a_{\deg f_{i-1}}}{b_m} x^{\deg f_i - m} \sum_{i=0}^{m} b_i x^i$$

so that the leading term gets cancelled out every time. Repeat this process inductively until $\deg f_k < \deg g$, which is always possible because the degree drops by at least one every step. Again let $f(x) = f_k(x)$ and $q(x) = \sum_{i=1}^{k} q_i(x)$.

$$q(x)g(x) + r(x) = \sum_{i=1}^{k} q_i g(x) + f_k(x) = \sum_{i=1}^{k-1} q_i(x)g(x) + f_{k-1}(x) = \cdots = f_0(x) = f(x)$$

Theorem 2.7.18. Long division in fields is unique.

Proof. Suppose there are $q \neq q'$ and $r \neq r'$ that both satisfy the long division process. Then $f(x) = q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$. Grouping terms together gives us $(q - q')g(x) = r'(x) - r(x)$, so this tells us that $\deg((q - q')g) = \deg(r' - r)$. But the definition of long division requires $\deg r < \deg g$, so Lemma 2.7.13 gives us $\deg(r' - r) \leq \deg g < \deg(q - q') + \deg g = \deg((q - q')g)$, which contradicts our equality above.

Corollary 2.7.19. Suppose F is a field, and $I \subseteq F[x]$ any ideal. Then there exists some element $f \in I$ such that it is generated by that element, $I = (f(x))$, i.e. all elements of I are multiples of $f(x)$.

Proof. Pick any $f(x) \in I$ with the lowest degree. If $g \in I$, by long division, $g(x) = q(x)f(x) + r(x)$, which implies $r(x) = g(x) - q(x)f(x) \in I$. But we also know that $\deg r < \deg f$, which tells us that $r(x) = 0$, giving us $g(x) = q(x)f(x) \in (f(x))$, and hence $I \subseteq (f(x))$. By definition of ideals, $(f(x)) \subseteq I$. Therefore $(f(x)) = I$.

Definition 2.7.20. Suppose R is a commutative domain. We call R a principal ideal domain (PID) if every ideal is generated by a single element.

Remark 2.7.21. In fact, what we have just proven above is that for any field F, $F[x]$ is a PID. More will be discussed on PIDs in Section 2.8 for unique factorization domains.

Proposition 2.7.22. Suppose R is an integral domain. Then $R[x]$ is also an integral domain.

Proof. Suppose we have nonzero $\{f(x), g(x)\} \subset R[x]$ Then we know $\deg f = m > 0$, $\deg g = n > 0$. Then $\deg(fg) = m + n > 0$, so $f(x)g(x) \neq 0$.

Theorem 2.7.23. Suppose F is a field, and $f(x) \in F[x]$. For some $u \in F$, if $f(u) = 0$, then $(x - u) \mid f(x)$; and there exists r distinct elements $\{u_i\}_{i=1}^{r} \subset F$ such that $\prod_{i=1}^{r}(x - u_i) \mid f(x)$, where $r \leq \deg f$.

Proof. Let η_u be the evaluation morphism. If $f(u) = 0$, then $f(x) \in \ker(\eta_u)$, which is an ideal. Since $F[x]$ is a PID by Corollary 2.7.19, these ideals are generated by a single element, and we claim that it is $(x - u)$. Clearly $u - u = 0$ also $(x - u) \in \ker(\eta_u)$, and it is the lowest degree.

We can repeat this process until we cannot find elements in a kernel anymore. As every time we divide by $(x - u_i)$, the degree decreases by one, so we can only do this at most $\deg f$ times.

Remark 2.7.24. Consider the rational polynomials $f(x) \in \mathbb{Q}[x]$. We can extend $\mathbb{Q}$ to a larger field K by adding the solutions of $f(x)$. Let $G = \mathrm{Aut}(K)$ be the automorphism group over K. The study of Galois theory is that there exists a formula for the roots of f if and only if G is a solvable group.

Definition 2.7.25. If F is a field, and $f(x) \in F[x]$ is a polynomial, we call $f(x)$ irreducible if $f(x) = g(x)h(x)$ implies either g or h is constant, i.e. $f(x)$ cannot decompose into something with a lower degree.

Theorem 2.7.26. Let $I = (f(x))$ and $J = (g(x))$ be two ideals in $F[x]$. Then:

(a) $f(x)$ is irreducible if and only if I is maximal; and

(b) $I \subseteq J$ if and only if $g(x) \mid f(x)$.

Proof. We first prove statement (b). Suppose $g(x) \mid f(x)$. Then there exists $h(x) \in F[x]$ such that $f(x) = g(x)h(x)$, and hence $f(x) \in J = (g(x))$, and any multiple of $f(x)$, that is elements of $(f(x))$ is in J; therefore $I \subseteq J$.

Suppose $I \subseteq J$. As elements of J are multiples of $g(x)$, we know that in particular elements of $I \subseteq J$ are multiples of $g(x)$; specifically, as $f(x) \in I \subseteq J$, $g(x) \mid f(x)$. This proves statement (b).

Now suppose I is reducible. Then $f(x) = g(x)h(x)$ some product of polynomials. In particular, $g(x) \mid f(x)$, $\deg g < \deg f$, so there exists some $J = (g(x))$ such that $I \subsetneq J$, as it is obvious that I cannot include elements of degree $\deg g$. But also $\deg g \geq 1$, so $J \subsetneq F[x]$, so we have found an intermediate ideal, and I not maximal.

For the reverse direction, suppose I is not maximal, and there exists some $J = (g(x))$ such that $I \subsetneq J \subsetneq F[x]$. Then $g(x) \mid f(x)$, and as there are some elements in J but not in I, there exists multiples of $g(x)$ that is not a multiple of $f(x)$. Hence $\deg g < \deg f$, because otherwise constant multiplies would work if $\deg g = \deg f$, and therefore $f(x) = g(x)h(x)$, where $\deg h \geq 1$. This proves statement (a).

Remark 2.7.27. From above, if $f(x)$ is irreducible, then I is maximal in $F[x]$, which by the fourth isomorphism theorem, the only ideals of $F[x]/I$ are itself and $\{0\}$, and Proposition 2.4.14 tells us $F[x]/I \supset F$ is now a field. In a sense we are adding the roots of $f(x)$ to F to form $F[x]/I$.

Suppose $f(x) = \prod_i g_i(x)$ factors into irreducible polynomials. If $g_i(x) = x - a$ is linear, then $a \in F$ is a root; if $g_i(x)$ is nonlinear, then there is no root in F, since otherwise it would be able to factor this into linear factors. Hence we only need to consider irreducible polynomials when looking for roots.

Suppose $K = F[x]/I$, where $I = (f(x))$ for some irreducible f. Notice that $x + I \in I$ is always a solution of $f(x)$ in K, as $x - (x + I) = I$ is in the ideal by definition, which is equivalent to $0 \in K$. So if $\alpha = x + I \in K$, we can merely factor out $x - \alpha$ from $f(x)$, and recursively use this construction to build all the roots of $f(x)$.

Polynomial Functions

Definition 2.7.28. Given some polynomial $f(x) \in F[x]$, we can write a function $f\colon F \to F,\ u \mapsto f(u)$, which is the familiar notion of polynomials being treated as functions. Again, the roots of the polynomial is the preimage of zero.

Remark 2.7.29. In general, two different polynomials can give the same function, such as $x = x^2$ when considering $\mathbb{Z}/2\mathbb{Z}$.

Theorem 2.7.30. In infinite fields, distinct polynomials are distinct as functions.

Proof. It is again sufficient to consider monic polynomials, since we know that polynomials that are off by a multiple have the same roots, and are clearly distinct from each other everywhere else.

We prove the contrapositive. Suppose $\{f(x), g(x)\} \subset F[x]$. If $f = g$ as functions, then $f(u) = g(u)$ for all $u \in F$, then $f(u) - g(u) = 0$, so u is a root of $f - g$. But since F has infinitely many roots, which implies $f - g = \prod_{u \in F} a(x - u)$ is not a valid polynomial, unless $a = 0$. Hence $f(x) = g(x)$ as polynomials.

Corollary 2.7.31. If F is an infinite field, and $f(x) \in F[x]$ some nonzero polynomial, then there exists some $u \in F$ such that $f(u) \neq 0$.

Proof. Special case of the theorem above that all polynomials are distinct from 0.

Corollary 2.7.32. If F is an infinite field, and $f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ some nonzero polynomial in n variables, then there exists some $(u_1, u_2, \ldots, u_n) \in F^n$ such that $f(u_1, u_2, \ldots, u_n) \neq 0$.

Proof. We can perform induction on the number of variables, and use the theorem above as our base case. Suppose, by way of induction, that our corollary holds for k variables. We attempt to prove the case for $k + 1$ variables. Suppose $f(x_1, \ldots, x_{k+1}) \in F[x_1, \ldots, x_{k+1}]$ is a nonzero polynomial in $k + 1$ variables. Without loss of generality, assume x_{k+1} is in the expression, since otherwise it is merely a polynomial in k variables, and the inductive hypothesis holds. Then picking some $(u_1, \ldots, u_k) \in F^k$, $u_i \neq 0$, $f(u_1, \ldots, u_k, x_{k+1}) \in F[x_{k+1}]$ is a nonzero polynomial in one variable, so the theorem above holds.

Remark 2.7.33. In general, finding nonzeros is easy, but finding zeros is hard. Hilbert's Nullstellensatz gives us a criteria for where zeros can be found.

Symmetric Polynomials

Definition 2.7.34. Suppose R is a commutative ring (and more often, a field). We call a polynomial $f \in R[x_1, x_2, \ldots, x_n]$ in n variables symmetric if $f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ for any $\sigma \in S_n$, that is, the polynomial remains unchanged under permutation of variables. We denote the set of symmetric polynomials $R[x_1, x_2, \ldots, x_n]^{S_n}$.

Definition 2.7.35. We can write down a set of symmetric polynomials called the elementary symmetric polynomials p_k, $1 \leq k \leq n$. They include all possible combinations of non-repeating products of k indeterminates.

$$p_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k} = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \prod_{j=1}^{k} x_{i_j}$$

In particular we see that $p_1 = \sum_{i=1}^{n} x_i$ and $p_n = \prod_{j=1}^{n} x_j$.

Proposition 2.7.36. The symmetric polynomials $R[x_1, x_2, \ldots, x_n]^{S_n}$ forms a commutative ring. For $n \geq 2$, this is a proper subring $R[x_1, x_2, \ldots, x_n]^{S_n} \subsetneq R[x_1, x_2, \ldots, x_n]$.

Proof. This will become obvious once we prove the following theorem. In the meantime, you can convince yourself by checking the axioms. The second fact is easy, as all univariate polynomials are by definition symmetric, and $f(x_1, \ldots, x_n) = x_1$ is an asymmetric polynomial when $n \geq 2$.

Definition 2.7.37. The total degree of a monomial $a\prod_{i=1}^{n} x_i^{k_i}$ is defined as $\sum_{i=1}^{n} k_i$. We call a polynomial $f \in R[x_1, x_2, \ldots, x_n]$ homogeneous if every monomial it contains has the same total degree.

Lemma 2.7.38. Any $f \in R[x_1, x_2, \ldots, x_n]$ is a sum of homogeneous parts. f is symmetric if and only if each homogeneous part is symmetric.

Proof. The first statement is clear because every monomial has a total degree, and you can simply group them by total degree.

The second statement is also easy, because under permutation of variables, the total degree of a monomial never changes, so it preserves each homogeneous part by themselves.

Definition 2.7.39. We define an order on the monomials by saying $x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n} < x_1^{b_1}x_2^{b_2}\ldots x_n^{b_n}$ when $(a_1, a_2, \ldots, a_n) < (b_1, b_2, \ldots, b_n)$ lexicographically, that is, the earliest index i where $a_i \neq b_i$, and then $a_i < b_i$.

Definition 2.7.40. For homogeneous polynomials, we call the monomial with the largest such order the leading term.

Lemma 2.7.41. $p_1^{d_1}p_2^{d_2}\ldots p_n^{d_n}$ has a leading term $x_1^{d_1+d_2+\cdots+d_n}x_2^{d_2+\cdots+d_n}\ldots x_n^{d_n}$.

Proof. We first see that for each i, $p_i^{d_i}$ has a leading term $x_1^{d_i}\ldots x_i^{d_i}$. We now claim that the leading term of a product of monomials is the product of the leading terms of the monomials. To see that, if $x_1^{\alpha_1}\ldots x_n^{\alpha_n} > x_1^{\beta_1}\ldots x_n^{\beta_n}$ and $x_1^{\gamma_1}\ldots x_n^{\gamma_n} > x_1^{\delta_1}\ldots x_n^{\delta_n}$, then $x_1^{\alpha_1+\gamma_1}\ldots x_n^{\alpha_n+\delta_n} > x_1^{\beta_1+\delta_1}\ldots x_n^{\beta_n+\delta_n}$, since without loss of generality let $i \leq j$, for the first indices where $\alpha_i \neq \beta_i$ and $\gamma_j \neq \delta_j$, and $\alpha_i > \beta_i$ implies $\alpha_i + \gamma_i > \beta_i + \delta_i$. We have proven that multiplication preserves the order, so if the leading terms are the largest out of all monomials, the product will still be the largest, and hence we can merely multiply the leading terms.

Theorem 2.7.42 (Fundamental Theorem of Symmetric Polynomials)**.** Every symmetric polynomial $f \in R[x_1, x_2, \ldots, x_n]^{S_n}$ can be uniquely represented by a polynomial $g \in R[p_1, p_2, \ldots, p_n]$ with variates being the elementary symmetric polynomials.

Proof. We provide an algorithm to convert symmetric polynomials into polynomials over p_i. By the first lemma above, it is sufficient to consider f homogeneous symmetric. With the above definitions, we can perform steps that are similar to polynomial long division by choosing our polynomials correctly.

We first claim that we can always write the leading term of f as $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ where $k_1 \geq k_2 \geq \cdots \geq k_n$. We observe that since f is symmetric, any permutation of the variates for our leading term also exists, so we can simply sort the k_i for our leading monomial into a descending sequence, and we realize that there exists that permutation of variables already in f, and we can choose that as our leading term.

We then construct $g = ap_1^{k_1-k_2}p_2^{k_2-k_3}\ldots p_{n-1}^{k_{n-1}-k_n}p_n^{k_n}$, which by the second lemma above has a leading term $ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$, as all the sums of exponents are telescoping. We can subtract $f - g = r$ to get a remainder, which has a lower leading term, allowing us to repeat this process on r.

We know this process terminates in finite steps, because there are only finitely many ways to add n non-negative numbers up to a certain total degree, so there are finitely many n-tuples $(k_1, k_2, \ldots, k_n)$ that we need to eliminate. This proves the existence of a $R[p_1, p_2, \ldots, p_n]$ representation.

Now it suffices to prove uniqueness of such a representation. By way of contradiction, if there exists an f with two different representations, then we can subtract the two different representations, and say that there exists some $\sum_i a_i \prod_{j=1}^{n} p_j^{d_{ij}} = 0$. In other words, we are proving algebraic independence.

But the second lemma above allows us to see that there is a bijection between product of p_j and the leading terms in x_j. Since the x_j are algebraically independent by definition, it is impossible to cancel out the leading term of two different products of p_j, which imply that a_i must all be 0.

Remark 2.7.43. It is a good exercise to program yourself a symmetric polynomial decomposition calculator, simply by following the algorithm as described in the theorem.

Corollary 2.7.44. $R[x_1, x_2, \ldots, x_n]^{S_n} \cong R[x_1, x_2, \ldots, x_n]$.

Proof. The theorem above essentially proves $R[x_1, x_2, \ldots, x_n]^{S_n} \cong R[p_1, p_2, \ldots, p_n]$. But Proposition 2.7.7 tells us that $R[p_1, p_2, \ldots, p_n] \cong R[x_1, x_2, \ldots, x_n]$.

2.8 Factorial Rings

Unique Factorization Domains

Definition 2.8.1. Suppose R is a commutative integral domain. For some $\alpha \in R^\star$, if there exists some $\{\beta, \gamma\} \subset R$ not units such that $\alpha = \beta\gamma$, we say α factors in R. Notice the definition excludes units u since it is always possible to write $\alpha = u(u^{-1}\alpha)$, which we do not consider factorization. We say in this case that β and γ properly divides α.

Definition 2.8.2. We call α irreducible if α is not factorable.

Proposition 2.8.3. Suppose we can factor $\alpha = \beta\gamma$. Then $(\alpha) \subsetneq (\beta)$ and $(\alpha) \subsetneq (\gamma)$.

Proof. It is sufficient to prove only the case of β. Clearly $\alpha \in (\beta)$, so $(\alpha) \subseteq (\beta)$. On the other hand, if $(\alpha) = (\beta)$, then there exists some unit u where $\alpha = \beta u$, which tells us in our case, $(\alpha) \subsetneq (\beta)$.

Remark 2.8.4. Because of this relationship between divisibility and ideals, every single statement below can be translated between these two languages. Sometimes it is easy to think of statements in one language or another.

Definition 2.8.5. Suppose R is a commutative integral domain. R is a unique factorization domain (UFD) if all $\alpha \in R^\star$ can be factorized into $\alpha = \prod_{i=1}^{n} p_i$ where p_i are irreducible elements, and this factorization is unique up to reordering of elements, and multiplication by units.

Theorem 2.8.6. R is a UFD if the following two conditions hold:

(i) *Divisor chain.* Given any $a_1 \in R^\star$, there exists no infinite proper divisor chain such that a_{i+1} properly divides a_i; and

(ii) *Primeness.* If p is irreducible, and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof. Factorization exists simply based on condition (i), since that allows our recursive factorization to terminate.

Now we prove uniqueness. Suppose that we have two factorizations $\alpha = p_1 \ldots p_r = p_1' \ldots p_s'$. Since $p_1 \mid p_1 \ldots p_r$, it should also divide $p_1 \mid p_1' \ldots p_s'$, which by condition (ii) it should divide one of p_i'. Without loss of generality, let this be p_1'. But as p_1' is irreducible, we conclude that $p_1' = up_1$ for some unit u. As we only require factorization up to multiplication by units, we can ignore u in this case, and look at the rest of the expression $p_2 \ldots p_r = p_2' \ldots p_s'$. But this is no different from the case of p_1 and p_1', so we recursively repeat that process, and see that all terms match up to unit multiplication.

Remark 2.8.7. It is also possible to rephrase condition (i) as having no infinite chain of proper ideals.

Definition 2.8.8. Suppose R is a commutative domain, and $p \in R^\star$. We call p prime if $p \mid ab$ implies either $p \mid a$ or $p \mid b$. In a similar vein, suppose $P \subsetneq R$ is an ideal, we call P a prime ideal if the product of ideals $IJ \subseteq P$ implies either $I \subseteq P$ or $J \subseteq P$.

Proposition 2.8.9. Suppose R is a commutative ring, and I an ideal. I is a prime ideal if and only if R/I is an integral domain.

Proof. For the foward direction, suppose I is a prime ideal. By way of contradiction, let R/I not be a domain, so there exists nonzero $x+I, y+I$ such that $(x+I)(y+I) = xy+I = I$. But since $xy \in I$, the product of the two generated ideals $(x)(y) \subseteq I$, so either $(x) \subseteq I$, which implies $x \in I$, or $(y) \subseteq I$, which implies $y \in I$, contradicting our assumption of nonzero x, y.

For the reverse direction, suppose R/I is an integral domain. Then for all $\{x, y\} \subset R$, $(x+I)(y+I) = xy+I = I$, $xy \in I$ implies either $x \in I$ or $y \in I$. For any two ideals $JK \subseteq I$, every $jk \in I$ for $j \in J$ and $k \in K$. Without loss of generality, suppose J not a subideal of I, so there exists some $j_0 \in J$ such that $j \notin I$. Then clearly since $j_0 k \in I$ for all $k \in K$, $k \in I$, so $K \subseteq I$. Hence I is prime.

Lemma 2.8.10. In a UFD, elements are prime if and only if they are irreducible.

Proof. The reverse direction is given by Theorem 2.8.6. For the forward direction, if $p = ab$ is prime, clearly $p \mid ab$, so $p \mid a$ or $p \mid b$. But $a \mid p$ and $b \mid p$, so either a or b must be a unit.

Definition 2.8.11. Suppose R is a commutative domain, and $\{a, b\} \subset R^\star$. $d \in R$ is a greatest common denominator of a and b, denoted $d = \gcd(a, b)$, if $d \mid a$ and $d \mid b$, and for all $c \in R$, $c \mid a$ and $c \mid b$ implies $c \mid d$. Similarly, $m \in R$ is a least common multiple of a and b, denoted $m = \operatorname{lcm}(a, b)$, if $a \mid m$ and $b \mid m$, and for all $n \in R$, $a \mid n$ and $b \mid n$ implies $m \mid n$.

Theorem 2.8.12. The primeness condition is equivalent to the following condition:

(ii) *GCD.* Any two elements have a GCD.

Proof. Primeness implies GCD is simple. Write $a = p_1^{i_1} \dots p_r^{i_r}$ and $b = p_1^{j_1} \dots p_r^{j_r}$. Then $\gcd(a, b) = p_1^{\min(i_1, j_1)} \dots p_r^{\min(i_r, j_r)}$.

GCD is commutative and associative as in $\gcd(a, b)$ is also a $\gcd(b, a)$ simply by definition; $d_n = \gcd(a_1, a_2, \dots, a_n)$ is defined recursively as $d_1 = a_1$, $d_{i+1} = \gcd(d_i, a_{i+1})$, and clearly that is by definition $d_n \mid a_i$ for all i, and $c \mid a_i$ implies $c \mid d_n$.

We claim that $c \gcd(a, b)$ is also a $\gcd(ca, cb)$. Suppose $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$, and hence $cd \mid ca$ and $cd \mid cb$, and $cd \mid \gcd(ca, cb)$. There exists some $x \in R$ such that $cdx = \gcd(ca, cb)$, and there exists some $y \in R$ with $cdxy = y \gcd(ca, cb) = ca$, which imply $cdx = ca$, and hence $dx \mid a$. Without loss of generality $dx \mid b$ too, so $dx \mid d$, and we know x is a unit, so cd is a GCD of ca and cb.

From the above we can now prove that if a coprime with b and a coprime with c, then a coprime with bc. We can show this with $1 = \gcd(a, c) = \gcd(a, c \gcd(a, b)) = \gcd(a, ca, cb) = \gcd(a, cb)$.

GCD implies primeness because if p is irreducible and $p \nmid a$ and $p \nmid b$, then p coprime a and p coprime b, so p coprime ab, and hence $p \nmid ab$.

Principal Ideal Domains

Remark 2.8.13. Recall from earlier that principal ideal domains (PID) are commutative domains with every ideal generated by a single element.

Proposition 2.8.14. Suppose R is a PID, $I \subseteq R$ is an ideal. Then I is maximal if and only if I is a nonzero prime ideal.

Proof. Suppose I is a maximal ideal. Then by Corollary 2.4.15 R/I is a field, which in particular it must be an integral domain. Hence by Proposition 2.8.9 I is a prime ideal.

Now suppose I is a nonzero prime ideal. We suppose there is an intermediate ideal $I \subseteq J \subseteq R$. But because R is a PID, $I = \langle x \rangle$, $J = \langle y \rangle$ for some $\{x, y\} \subset R$. But as $I \subseteq J$, $x = ay$ for some $a \in R$; but by primality of I, either $a \in I$ or $y \in I$. If $y \in I$ then $I = J$ so I is maximal. If $a \in I$ then $a = bx$ for some $b \in R$, so $x = bxy$, and therefore $by = 1$. y is a unit, so $J = R$, and I is maximal.

Theorem 2.8.15. If R is a PID, then R is a UFD.

Proof. We first prove that it satisfies the divisor chain condition via the ideal chain condition. Suppose we have an infinite ideal chain $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_r) \subseteq \cdots$. Then by Proposition 2.4.11, $I = \bigcup_{i=1}^{\infty}(a_i)$ is an ideal. Notice that $I = (b)$ must be generated by some element, and since $b \in I$, there exists some r that $b \in (a_r)$. However, by definition of the infinite union, $(b) \subseteq (a_r) \subseteq (a_{r_1}) \subseteq \cdots \subseteq I = (b)$. Hence we are forced to conclude that $(b) = (a_r) = (a_{r+1}) = \cdots = I$, and every infinite chain of ideals are only proper up to a finite r. There are no infinite chain of proper ideals.

Now we prove the primeness condition. Suppose p is irreducible, $p \mid ab$ and $p \nmid a$. p irreducible means (p) is maximal (similar to Theorem 2.7.26). As $p \nmid a$, then $a \notin (p)$, so the ideal generated by two elements $(p, a) \supsetneq (p)$, and hence $(p, a) = R = (1)$. By Bézout's Identity, there exists u, v such that $up + va = 1$, and hence $upb + vab = b$. As $p \mid upb$ and $p \mid v(ab)$, $p \mid b$.

Then by Theorem 2.8.6, R is a UFD.

Remark 2.8.16. In general it is difficult to determine whether any ring is a PID. The Krull dimension is one way to determine PIDs via the length of prime ideals.

Definition 2.8.17. Suppose R is a commutative domain. We call R a Euclidean domain if there exists a long division algorithm $\delta\colon R \to \mathbb{Z}$, such that for all $a, b \in R^\star$, we can find $q, r \in R$ with $a = qb + r$, where $\delta(r) < \delta(b)$, and $\delta(x) = 0$ if and only if $x = 0$.

Theorem 2.8.18. If R is a Euclidean domain, then R is a PID.

Proof. We first look at the ideal of a single element, $I = \{0\}$; clearly this is $I = (0)$.

Now suppose I has more than one element. Choose any nonzero element $x \in I$ such that $\delta(x) \leq \delta(y)$ for all nonzero $y \in I$; in other words, $\delta(x)$ is minimal. Now suppose we have some nonzero $y \in I$. We factor it with $y = qx + r$, which we know $r = y - qx \in I$; and according to the Euclidean function $\delta(r) < \delta(x)$, as $\delta(x)$ is minimal, $\delta(r) = 0$, so $r = 0$. Hence all $y \in I$ is a multiple of x, and $I = (x)$.

Corollary 2.8.19. If R is a Euclidean domain, then R is a UFD.

Proof. By the theorem above and Theorem 2.8.15.

Polynomials over UFDs

Definition 2.8.20. Suppose R is a UFD, and $f(x) \in R[x]$ a polynomial. We define the content of f, a function $c\colon R[x] \to R$ to be the GCD of all nonzero coefficients. We call f primitive if $c(f)$ is a unit. Hence we can write $f = c(f)f_1$, where f_1 is primitive.

Lemma 2.8.21. Suppose R is a UFD, and F its field of fractions. If $f(x) \in F[x]$, there exists a unique factorization up to multiplication of units in R for $f(x) = \gamma f_1(x)$ where f_1 is primitive in $R[x]$, and $\gamma \in F$.

Proof. Since all coefficients of f are fractions, it is sufficient to look at the product of all denominators, and multiply by that to obtain some $g(x) \in R[x]$. Hence there exists some $a \in R$ such that $af(x) = g(x) \in R[x]$. We can then decompose $g(x) = bg_1(x)$ where $b = c(g)$ and g_1 is primitive. Therefore $af(x) = bg_1(x)$, so $f(x) = \frac{b}{a}g_1(x)$, and there exists $\gamma = \frac{b}{a}$.

We now prove uniqueness. Suppose $f(x) = \gamma' g_1'(x)$ for another such combination. Then since $\gamma' \in F$, we write $\gamma' = b'/a'$, and we have $f(x) = \frac{b'}{a'}g_1'(x) = \frac{b}{a}g_1(x)$. So we have $aa'f(x) = ab'g_1'(x) = a'bg_1(x) \in R[x]$, but that tells us $c(aa'f) = ab' = a'b$ up to unit multiplication. Hence $ab' = ua'b$ for some unit u, and $ub/a = b'/a'$.

Corollary 2.8.22. Suppose $\{f(x), g(x)\} \subset R[x]$ are both primitive. If there exists some $\gamma \in F$ such that $\gamma f = g$, then γ is a unit in R.

Proof. By the proof of lemma above, $\gamma'/\gamma = u$ is a unit.

Lemma 2.8.23 (Gauss' Lemma for primitivity)**.** Suppose R is a UFD. If $\{f, g\} \subset R[x]$ are both primitive, then fg is also primitive.

Proof. We prove the contrapositive. Suppose fg is not primitive. Then there exists some prime p which divides every coefficient of fg. Considering $T = R/(p)$, since p prime, Proposition 2.8.9 shows that T is a domain. By Proposition 2.7.22, since T is a domain, $T[x]$ is also a domain. We can write a quotient map $\pi\colon R \to T,\ r \mapsto r + (p)$ the obvious way, and extend it to $\pi\colon R[x] \to T[x]$ by sending $x \mapsto x$. Hence $\pi(fg) = \pi(f)\pi(g) = (p)$, as all the coefficients, and hence all the terms are divisible by p. But as $T[x]$ is a domain, either $\pi(f) = (p)$ or $\pi(g) = (p)$, which says either f or g is not primitive.

Lemma 2.8.24 (Gauss' Lemma for irreducibility)**.** Suppose R is a UFD, and F its field of fractions. If $f(x) \in R[x]$ is primitive and irreducible, then $f(x) \in F[x]$ is irreducible.

Proof. By way of contradiction, suppose $f(x) = f_1(x)f_2(x)$ can be factored in $F[x]$. Then by Lemma 2.8.21, there exists $\gamma_i \in F$ and primitive $g_i \in R[x]$ such that $f(x) = f_1(x)f_2(x) = \gamma_1\gamma_2 g_1(x)g_2(x)$. But considering f, g_1, g_2 as primitive elements of $R[x]$, we know that $\gamma_1\gamma_2$ is a unit in R by Corollary 2.8.22. Then that implies f_1, f_2 are also elements of $R[x]$, so f factors in $R[x]$ too, which is a contradiction.

Theorem 2.8.25. Suppose R is a UFD. Then $R[x]$ is also a UFD.

Proof. We first prove that a factorization of polynomials exist. Suppose $f(x) \in R[x]$ is nonzero and not a unit. Then we can write $f = c(f)f_1$, where f_1 primitive. Clearly $c(f) \in R$ can factor into irreducible components. Now consider f_1. If f_1 is irreducible we are done. However, if f_1 can be factored such that $f_1 = g_1g_2$, then we see that $0 < \deg g_i < \deg f_1$, so the degree gets reduced, and hence if we perform factorization recursively, there are at most $\deg f_1$ recursions, and factorization terminates. Hence the factorization of f is the product of the factorization of $c(f)$ and the factorization of f_1.

We then prove the factorization is unique up to multiplication by units. We first consider $f(x) \in R[x]$ primitive. Then $f(x) = q_1(x)q_2(x)\dots q_n(x)$ factors into irreducibles, with $\deg q_i > 0$, since Corollary 2.8.22 tells us that if we have $q_i = 0$, then q_i is a unit, and by definition we only perform factorization up to units, so q_i should not be in the factorization.

Suppose we also have another factorization into irreducibles $f(x) = q_1'q_2'\dots q_m'$, $\deg q_i' > 0$. Since q_i and q_i' are all primitive, by Gauss' lemma they are also irreducible in $F[x]$. We have shown earlier in Corollary 2.7.19 that $F[x]$ is a PID, which by Theorem 2.8.15 $F[x]$ is a UFD. Then we know that the factorization is equal up to units in $F[x]$, and without loss of generality we pair up the factors $q_i = \gamma q_i'$ for some $\gamma \in F$. But Corollary 2.8.22 once again tells us that $\gamma \in R$ is a unit, which is exactly what we desire.

Lastly we consider $f(x)$ not primitive. Then $f(x) = c(f)f_1(x)$ where $f_1(x)$ is primitive. $c(f) = p_1\dots p_m$ uniquely factors up to unit multiplication in R, and the previous paragraph tells us $f_1(x)$ does so too. This completes the proof for uniqueness.

Theorem 2.8.26 (Eisenstein's criterion)**.** Suppose R is an integral domain, $P \subseteq R$ some prime ideal. Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in R[x]$ be a polynomial. If the coefficients

(a) $a_i \in P$ for all $0 \le i \le n-1$, all coefficients but the leading term in the ideal;

(b) $a_n \notin P$ leading term not in the ideal; and

(c) $a_0 \notin P^2$ constant term not in the square,

then $f(x)$ is irreducible in $R[x]$.

Proof. Suppose, by way of contradiction, that $f(x)$ is reducible in $R[x]$. Then we can write $f(x) = g(x)h(x)$, and we shall denote

$$g(x) = c_kx^k + c_{k-1}x^{k-1} + \dots + c_1x + c_0 \qquad h(x) = d_\ell x^\ell + d_{\ell-1}x^{\ell-1} + \dots + d_1x + d_0$$

By condition (a) & (c), only one of c_0 and d_0 is in P, so without loss of generality let $c_0 \in P$ and $d_0 \notin P$.

We claim that this implies $c_i \in P$ for all $0 \le i \le k$. We already have our base case $c_i \in P$ from above, so by way of strong induction, suppose $c_0, c_1, \dots, c_{i-1} \in P$. Since $a_i = \sum_{j+j'=i} c_jd_{j'} = c_id_0 + c_{i-1}d_1 + \dots + c_0d_i \in P$ by condition (a), and every term in the sum except for the first term is in P by assumption, as $d_0 \notin P$, we must have $c_i \in P$.

But $c_k \in P$ implies $a_n = c_kd_\ell \in P$, which contradicts condition (b). Hence $f(x)$ is irreducible in $R[x]$.

Corollary 2.8.27 (Eisenstein's criterion over integers)**.** Suppose we have a polynomial with integer coefficients $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime p such that

(a) $p \mid a_i$ for all $0 \leq i \leq n-1$, p dividing all coefficients but the leading term;

(b) $p \nmid a_n$ does not divide the leading term; and

(c) $p^2 \nmid a_0$ the square does not divide the constant term,

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. By the theorem above we get irreducibility in $\mathbb{Z}[x]$; by Gauss' lemma, we get irreducibility in $\mathbb{Q}[x]$.

Corollary 2.8.28 (Irreducibility of the cyclotomic)**.** Let p be prime. The cyclotomic polynomial $\Phi_p(x) = \sum_{i=0}^{p-1} x^i \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$.

Proof. It is sufficient to prove that $\Phi_p(y+1)$ as a polynomial of y is irreducible. By the binomial theorem

$$\Phi_p(y+1) = (y+1)^{p-1} + (y+1)^{p-2} + \cdots + 1 = \sum_{i=0}^{p-1} \binom{p}{i} y^{p-1-i}$$

Note that by definition of the binomial coefficient, only the leading term $\binom{p}{0} = 1$ is not divisible by p, and the constant term $\binom{p}{p-1} = p$ is not divisible by p^2, so by Eisenstein's criterion, it is irreducible.

3 Fields

Remark 3.0.1. We begin by recalling the definition of a field. Fields are quintuples $(F, +, \cdot, 0, 1)$ where $(F, +, 0)$ and $(F^\star, \cdot, 1)$ are both abelian groups, and multiplication distributes over addition.

Remark 3.0.2. Fields are commutative rings, so theorems in Section 2 will entirely hold, and we will be using those theorems throughout.

Remark 3.0.3. Much of our foundation will come from extending any integral domain R (in particular $\mathbb{Z}$) to its field of fractions F (in particular $\mathbb{Q}$).

3.1 Field Extensions

Definition 3.1.1. Suppose F is a field, and $F[x]$ its polynomial ring. Corollary 2.7.19 tells us that $F[x]$ is a domain, and hence we can construct its field of fractions, which we denote $F(X) = \{\frac{f(x)}{g(x)} : f, g \in F[x], g \neq 0\}$. This is often called the transcendental extension of F, or the univariate function field over F.

Remark 3.1.2. Recall that if R is a commutative ring, P a prime ideal, and M a maximal ideal, then R/P is an integral domain and R/M is a field. But when F a field, prime ideals and maximal ideals are the same thing.

Definition 3.1.3. Suppose F is a field. A field extension K/F is a field $K \supseteq F$. We say F is a subfield of K, where F is a base field, and K is an over field of F.

In commutative diagrams, we often denote this as

$$\begin{array}{c} K \\ | \\ F \end{array}$$

Proposition 3.1.4. Suppose K/F a field extension. K can be characterized as a vector space over F.

Proof. Let $k, \ell \in K$, and $\lambda \in F$. Trivially by field addition $k + \ell \in K$, and $\lambda \in F \subseteq K$, so by field multiplication we have $\lambda k \in K$. Moreover, distributivity holds because of $\lambda(k + \ell) = \lambda k + \lambda \ell$ due to distributivity in K.

Definition 3.1.5. Suppose K/F field extension. We call K/F finite or K is a finite extension of F if K is a finite-dimensional vector space over F. If K/F finite, the degree of K/F, denoted $[K : F] = \dim_F K$ is the dimension of K as an F-space.

Theorem 3.1.6. Suppose K/F and L/K are finite field extensions. Then L/F is a finite extension, and in particular, $[L : F] = [L : K][K : F]$.

Proof. Since K/F finite, let $\{a_i\}_{i=1}^m$ be a basis for K/F, so $[K : F] = m$. For every $a \in K$, we can write $a = \sum_{i=1}^m \lambda_i a_i$ for some $\lambda_i \in F$. Similarly since L/K finite, let $\{b_j\}_{j=1}^n$ be a basis for L/K, so $[L : K] = n$. For every $b \in L$, we can write $b = \sum_{j=1}^n \mu_j b_j$ for some $\mu_j \in K$. But then we have a linear combination of mn elements

$$b = \sum_{j=1}^n \mu_j b_j = \sum_{j=1}^n \left(\sum_{i=1}^m \lambda_{ij} a_i \right) b_j = \sum_{i,j=1}^{m,n} \lambda_{ij}(a_i b_j)$$

It suffices to check that $\{a_i b_j\}_{i=1}^m{}_{j=1}^n$ forms a basis. Suppose that

$$0 = \sum_{i,j=1}^{m,n} \lambda_{ij}(a_i b_j) = \sum_{j=1}^n \left(\sum_{i=1}^m \lambda_{ij} a_i \right) b_j$$

But by linear independence of b_j, for each individual j, $\sum_{i=1}^m \lambda_{ij} a_i = 0$, and by linear independence of a_i, for all i, $\lambda_{ij} = 0$. This proves linear independence.

Corollary 3.1.7. Finiteness is a property that is stackable, and degree of extension is multiplicative.

Proof. Merely proceed by induction on the tower of field extensions, applying the theorem above.

Theorem 3.1.8. Every field homomorphism is injective.

Proof. Suppose $\phi\colon F \to K$ is a field homomorphism. By way of contradiction, suppose ϕ is not injective. Then there exists $a, b \in F$ such that $\phi(a) = \phi(b)$ and $a \neq b$. But that tells us $f(a-b) = 0 = f(0)$, and in particular, since $a - b \neq 0$, $f(a-b)f((a-b)^{-1}) = f(1) = 1$. But that implies $0f((a-b)^{-1}) = 1$ which is a contradiction.

3.2 Algebraic Extensions

Definition 3.2.1. Suppose K/F is a field extension, and $a \in K$ some element. We call a algebraic over F if there exists a (monic) polynomial $f(x) \in F[x]$ such that $f(a) = 0$. If $a \in K$ is not algebraic over F, we call a transcendental over F.

Definition 3.2.2. Suppose $a \in K$ is algebraic over F. The minimal polynomial of a over F, either denoted $\min_F(a)$ or $\min(a; F)$ is the irreducible polynomial $f(x) \in F[x]$ with the lowest degree such that $f(a) = 0$.

Proposition 3.2.3. A monic minimal polynomial exists and is unique for every algebraic $a \in K$.

Proof. By definition there must be some polynomial that it satisfies. If it is reducible, reduce it into irreducible components, and a must satisfy one of those irreducible components. It is unique since if another monic polynomial $g(x)$ satisfies our conditions, $(g-f)(x)$ also satisfies our conditions, and since they are the same degree, $\deg(g-f) < \deg f$ violates minimality.

Definition 3.2.4. Suppose $a \in K$ is algebraic over F. We define the degree of a to be the degree of its minimal polynomial, $\deg a = \deg \min_F(a)$.

Definition 3.2.5. Suppose K/F is a field extension. If all elements $a \in K$ are algebraic over F, we call K/F an algebraic extension.

Definition 3.2.6. Suppose K/F is an extension, and $a \in K$ some element. $F(a) \subseteq K$ is the smallest subfield that contains F and all elements $\lambda = \sum_i \ell_i a^i$ for some $\ell_i \in F$.

Proposition 3.2.7. $F(a)$ is the field of fractions of $F[a]$.

Proof. By definition of a field of fractions, $F(a)$ is the smallest field that contains $F[a]$.

Theorem 3.2.8. Suppose K/F is a field extension, and $a \in K$ some element. The following are equivalent:

(a) a is algebraic over F;

(b) $F(a)$ is a finite extension of F; and

(c) $F[a] = F(a)$.

Proof. We first prove that (a) implies (c). Since a is algebraic, there is some minimal polynomial $a^n + \lambda_1 a^{n-1} + \cdots + \lambda_n = 0$ for $\lambda_i \in F$. But we can rewrite the above as

$$-\lambda_n = a^n + \lambda_1 a^{n-1} + \cdots + \lambda_{n-1} a = a(a^{n-1} + \lambda_1 a^{n-2} + \cdots + \lambda_{n-1})$$

and clearly $\lambda_n \neq 0$, since otherwise $a^{n-1} + \lambda_1 a^{n-2} + \cdots + \lambda_{n-1}$ would be a minimal polynomial of degree less than n, violating minimality of the original polynomial. Hence we have a polynomial expression for the inverse

$$a^{-1} = -\frac{1}{\lambda_n}(a^{n-1} + \lambda_1 a^{n-2} + \cdots + \lambda_{n-1})$$

so $F(a) \subseteq F[a]$. $F[a] \subseteq F(a)$ by definition and we have equality.

We now prove that (c) implies (b). For any $i \geq 0$, a^{n+i} is in the F-span of $\{a^j\}_{j=0}^{n-1}$. and since we write elements in $F(a) = F[a]$ as linear combinations of powers of a, the degree of those elements must be at most n, hence $[F(a) : F]$ is finite.

Lastly we prove that (b) implies (a). Suppose $F(a)$ is a finite extension. Then $\{a^i\}_{i=0}^{\infty} \subseteq F(a)$ is a linearly dependent set. We shall find the smallest *ell* such that $\{a^i\}_{i=0}^{\ell}$ is a linearly dependent set. By linear dependence we will have $\lambda_0 + \lambda_1 a + \cdots + \lambda_\ell a^\ell = 0$ for some $\lambda_i \in F$, $\lambda_\ell \neq 0$. Hence we have found a degree ℓ polynomial that a satisfies, and a must be algebraic.

Corollary 3.2.9. Suppose K/F is a finite extension. Then K is algebraic over F.

Proof. Suppose $a \in K$. Since we have $F \subseteq F(a) \subseteq K$, $F(a)/F$ must be finite, which by the theorem above must be algebraic.

Remark 3.2.10. We have shown that finite extensions are algebraic, but algebraic extensions are not necessarily finite.

Theorem 3.2.11. Suppose K/F is a field extension. The set of all F-algebraic elements in K form a subfield of K containing F.

Proof. Let $a, b \in K$ be algebraic over F. It is sufficient to prove that $a \pm b$, ab, and a/b when $b \neq 0$ are all algebraic. Observe that $[F(a) : F], [F(b) : F]$ are finite by the previous theorem. Let $F_1 = F(a) \subseteq K$. Then again, $[F_1(b) : F]$ is also finite by Theorem 3.1.6. This process is repeatable for finitely many elements. From this we can see that $F(a)(b) = F(a, b)$ by minimality of the extension by an element. But then this tells us that $a, b \in F(a, b)$ is a field, so $a \pm b$, ab, and a/b are all in $F(a, b)$. and finite implies algebraic by the theorem above.

Definition 3.2.12. Suppose K/F is an extension. Then the subfield of all F-algebraic elements in K is usually denoted $F^{\text{alg}} \subseteq K$. K/F^{alg} has no algebraic elements over F, while F^{alg}/F is an algebraic extension.

Definition 3.2.13. Suppose K/F is an extension. K/F is finitely generated if there exists a finite set $S \subseteq K$ such that $K = F(S)$.

Theorem 3.2.14. Suppose K/F is finitely generated by S. If all elements of S are algebraic, then K/F is algebraic.

Proof. If $S = \{s_i\}_{i=1}^{n}$, then merely apply Theorem 3.2.8 to see that $F(S)/F$ is finite, so Corollary 3.2.9 tells us that it is algebraic.

Corollary 3.2.15. Suppose K/F and L/K are algebraic extensions. Then L/F is algebraic.

Proof. Suppose $\lambda \in L$. Then there exists $f(x) \in K[x]$ such that $f(\lambda) = 0$. $f(x) = x^n + b_1 x^{n-1} + \cdots + b_0$ where $b_i \in K$. But notice that $b_i \in K$ are algebraic over F, so $F(b_1, \ldots, b_n)/F \subseteq K$ is a finite extension by the theorem above. We can see that $f(x)$ is also a polynomial in $F(b_1, \ldots, b_n)[x]$, which tells us that $F(b_1, \ldots, b_n)(\lambda)/F(b_1, \ldots, b_n)$ is finite. But these two finite extensions combined gives us that $F(b_1, \ldots, b_n)(\lambda)/F$ is finite by Theorem 3.1.6. Since $F(\lambda) \subseteq F(b_1, \ldots, b_n)$, $F(\lambda)/F$ must also be finite, which implies λ is algebraic over F by Theorem 3.2.8.

3.3 Splitting Fields and Algebraic Closures

Theorem 3.3.1. Suppose $f(x) \in F[x]$ is an irreducible polynomial of degree at least 2, There exists an extension K/F such that $f(x)$ has roots in K.

Proof. Let $I = (f(x)) \subseteq F[x]$ be a maximal ideal, since $f(x)$ is irreducible by Theorem 2.7.26. Then we have a field $K = F[x]/I \supseteq F$ by Corollary 2.4.15, with degree $[K : F] = \deg f$ which we will say is n. This induces a homomorphism $\pi \circ \iota \colon F \to K$ where $\iota \colon F \to F[x]$ is the inclusion of F into its polynomial ring, and $\pi \colon F[x] \to K$ is the quotient by I, both of them ring homomorphisms. We can see that $\pi \circ \iota$ is a field homomorphism, since elements in F within $F[x]$ will not get collapsed by I as their degrees are always 1. Now see that $\pi(f(x)) = \overline{f(x)} = 0$ in K, so $f(\bar{x}) = 0$, and π maps $x \mapsto \bar{x}$, so $\bar{x}$ is a root in K, and $K = \langle 1, x, \ldots, x^{n-1} \rangle$.

Corollary 3.3.2. If $f(x) \in F[x]$ has degree n, then there exists a field extension K/F with $[K : F] \leq n$ such that $f(x)$ acquires a root.

Proof. Split $f(x)$ into irreducible components and then apply the theorem above.

Definition 3.3.3. Suppose L_1/F and L_2/F are field extensions, where $L_1, L_2 \subseteq L$. The composite extension or the compositum, denoted $L_1 \cdot L_2$ or L_1L_2, is the smallest field extension of F in L that contains both L_1 and L_2.

Definition 3.3.4. A polynomial $f(x) \in F[x]$ splits over an extension K/F if $f(x) \in K[x]$ can be written as a product of linear polynomials, i.e. all roots exist in K.

Definition 3.3.5. Suppose K/F is an extension. An automorphism of K is a field automorphism $\sigma \in \mathrm{Aut}(L)$ that is bijective; an F-automorphism is a field automorphism $\sigma \in \mathrm{Aut}_F(L)$, with the additional condition that it is the identity when restricted to F, $\sigma|_F = \mathrm{id}_F$.

Lemma 3.3.6. Suppose K/F is an extension, and $\sigma \in \mathrm{Aut}_F(K)$ an F-automorphism. If $a \in K$ is an element with a minimal polynomial $\min_F(a) = f(x)$, then $\sigma(a)$ is also a root of $f(x)$.

Proof. By definition a is a root of $f(x)$, so $f(a) = 0$. But $\sigma(f(a)) = \sigma(0) = 0$, and notice that $\sigma(f(x)) = f(x)$, since the coefficients are in F so they remain unchanged under σ, so $f(\sigma(a)) = 0$.

Definition 3.3.7. The splitting field of a polynomial $f(x) \in F[X]$ over F is a field K such that

(i) $f(x)$ splits completely over K;

(ii) $K \supseteq F$; and

(iii) if K' satisfies the previous two conditions, then $K' \supseteq K$.

Proposition 3.3.8 (Existence of Splitting Fields)**.** For any $f(x) \in F[x]$, its splitting field exists.

Proof. Without loss of generality suppose $f(x)$ irreducible and monic. By Theorem 3.3.1, we can find a field extension F_1/F such that $f(x) = (x - a_1)f_1(x) \in F_1[x]$. Iterate on $f_i(x)$ until $f(x)$ is comprised of linear factors.

Corollary 3.3.9. Let $f(x) \in F[x]$ be a polynomial of degree n. Then there exists an extension K/F with degree $[K : F] \leq n!$ such that F splits completely over K.

Proof. Same proof as proposition above, but notice that $[F_1 : F] \leq n$, and then induct on n, since $\deg f_1(x) \leq n - 1$.

Lemma 3.3.10. Suppose F is a field. Then the following are equivalent:

(a) The only algebraic extension of F is itself;

(b) The only finite extension of F is itself;

(c) If K/F is an extension, then F is the set of F-algebraic elements in K;

(d) Every $f(x) \in F[x]$ splits over F; and

(e) Every $f(x) \in F[x]$ has a root in F.

Proof. (a) implies (b) is the contrapositive of Corollary 3.2.9.

(b) implies (c) because if there exists another F-algebraic element $a \in K - F$, then there is a finite extension $F(a)/F$.

(c) implies (d) since if $f(x) \in F[x]$ and a is a root, then a is algebraic over F, and must be in F. Induct on order of f.

(d) implies (e) trivially true.

(e) implies (d) simply by induction on degree of f.

(d) implies (a) since if there are other algebraic extensions, then that means there is some polynomial that does not have a root in F.

Definition 3.3.11. F is algebraically closed if it satisfies any of the conditions above.

Definition 3.3.12. If K is an algebraic extension of F and is algebraically closed, then K is an algebraic closure of F.

Theorem 3.3.13 (Existence of Algebraic Closures)**.** Suppose F is a field. Then there exists an algebraically closed field $K \supseteq F$.

Proof. We first attempt to construct an extension F_1/F such that every polynomial $f(x) \in F[x]$ of degree at least 1 has at least one root. For every $f(x) \in F[x]$ let us assign an arbitrary letter (some unique indeterminate) X_f, and let S be the set of all X_f. We can get a bijection between S and $F[x] - F$. We now get a multivariate polynomial ring $F[S]$.

We now wish to show that the ideal I generated by all $f(X_f)$ is not the unit ideal $(1) = F[S]$. Suppose, by way of contradiction, that $I = (1) = F[S]$.

Corollary 3.3.14. Suppose F is a field, then there exists an algebraic extension F^{alg}/F that is algebraically closed.

Proof.

Proposition 3.3.15. Suppose $\sigma\colon F \to L$ is a field homomorphism, where $L = \overline{L}$ iss algebraically closed. Let α be algebraic over F, $p(x) = \min_F(a) = \sum_{i=0}^n a_i x^i$ a monic minimal polynomial, and $\sigma(p)(x) = \sum_{i=0}^n \sigma(a_i)x^i$ its image. Then given a homomorphism $\tau\colon F(\alpha) \to L$ that is an extension of σ ($\tau|_F = \sigma$), the evaluation map $\tau \mapsto \tau(\alpha)$ is a bijection between homomorphisms extending σ ($\{\tau \in \text{Hom}(F(\alpha), L) : \tau|_F = \sigma\}$) and the roots of the image polynomial in L ($\{\beta \in L : \sigma(p)(\beta) = 0\}$).

Proof. Let $\tau\colon F(\alpha) \to L$ extending σ. Then $\tau(p(\alpha)) = \sigma(p)(\tau(\alpha)) = 0$ since $p(\alpha) = 0$.

Theorem 3.3.16 (Uniqueness of Splitting Fields)**.** Suppose $p(x) \in E[x]$ an irreducible polynomial, and K is a splitting field of $p(x) \in E[x]$. Suppose $\phi\colon E \to F$ is a field isomorphism, and L is a splitting field of $\phi(p)(x) \in F[x]$. Then ϕ extends to an isomorphism $\sigma\colon K \to L$ where $\sigma|_E = \phi$. In particular, splitting fields of $p(x) \in F[x]$ over F are F-isomorphic.

3.4 Separability

Definition 3.4.1. An (irreducible) polynomial $f(x) \in F[x]$ of degree n is separable if $f(x)$ has n distinct roots in its splitting field, or equivalently, if its irreducible factors are distinct and separable.

Proposition 3.4.2. $f(x) \in F[x]$ is inseparable if and only if f and f' share a root.

Proof. Suppose $f(x)$ is separable. Then we can write, in its splitting field, that $f(x) = \prod_i (x - r_i)$ for all distinct r_i. By the product rule, $f'(x)$ has one term that is missing $x - r_i$, and all other terms contain $x - r_i$, Let us inspect $f'(r_i)$. All the terms that contain r_i will evaluate to 0, while the term that has r_i missing will evaluate to nonzero. Hence $0 = f(r_i) \neq f'(r_i)$.

Now suppose $f(x)$ is inseparable. Then there is some root r that has multiplicity $m > 1$, so we write in a splitting field $f(x) = (x - r)^m g(x)$. The formal derivative is then $f'(x) = m(x - r)^{m-1} g(x) + (x - r)^m g'(x)$. Hence $f(r) = f'(r) = 0$.

Definition 3.4.3. Suppose $f(x) \in F[x]$ is a (monic) polynomial, and over a splitting field is written as $f(x) = \prod_{i=1}^k (x - r_i)^{m_i}$ where r_i are all distinct and $m_i \geq 1$. The multiplicity of a root r_i is m_i. We call r_i a simple root if $m_i = 1$, and we say $f(x)$ has repeated roots if there exists i such that $m_i > 1$.

Resultant and Determinant

Remark 3.4.4. Historically the resultant is very important in determining separability, but in modern times the discriminant is more often used. Nevertheless, we shall include it here for sake of completeness.

Definition 3.4.5. Suppose $f(x), g(x) \in F[x]$ are polynomials; $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$ and $g(x) = \sum_{j=0}^{m} b_j x^{m-j}$, and the leading terms are nonzero. The resultant of f and g is

$$\mathcal{R}(f,g) = a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j)$$

where α_i are the roots of f, and β_j are the roots of g.

Lemma 3.4.6. $\mathcal{R}(f,g) = 0$ if and only if f and g share a root.

Proof. If they share a root then one of the terms in the product is 0.

Corollary 3.4.7. f is inseparable if and only if $\mathcal{R}(f,f') = 0$.

Proof. f and f' sharing a root is equivalent to the resultant being zero by the lemma above. Then apply Proposition 3.4.2.

Remark 3.4.8. If $f(x) = \prod_i (x - \alpha_i)$ and $g(x) = \prod_j (x - \beta_j)$ are monic, then $\prod_i g(\alpha_i) = (-1)^{mn} f(\beta) = \mathcal{R}(f,g)$. Also notice that the resultant is closely related to the Vandermonde determinant.

$$\mathcal{R}(f,g) = \det \begin{bmatrix} a_0 & a_1 & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & a_n & & \\ & & \ddots & & & \ddots & \\ & & & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & & & \\ & b_0 & b_1 & \cdots & b_m & & \\ & & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \cdots & b_m \end{bmatrix}$$

where you have m rows of a_i and n rows of b_i, resulting in a $(m+n) \times (m+n)$ matrix.

Definition 3.4.9. Suppose $f(x) \in F[x]$ is a polynomial. The discriminant is

$$\mathcal{D}(f) = a_0^{2n-2} (-1)^{n(n-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j) = a_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

where α_i are roots.

Proposition 3.4.10. $\mathcal{R}(f,f') = (-1)^{n(n-1)/2} a_0 \mathcal{D}(f)$.

Proof.

Separable Extensions

Definition 3.4.11. Suppose F is a field, and a algebraic over F. a is a separable element if $\min_F(a)$ is separable.

Definition 3.4.12. Suppose E/F is an algebraic extension. E/F is a separable extension if every $a \in E$ is separable.

Lemma 3.4.13. Let $f(x) = \min_F(a) \in F[x]$. $f(x)$ is separable if and only if $(f, f') = 1$ are coprime.

Proof. Let $f(x)$ is separable. By way of contradiction, suppose $g(x) \in F[x]$ is a monic irreducible polynomial of degree d, where $g \mid f$ and $g \mid f'$. Let us write $f(x) = g(x)h(x)$ Without loss of generality we may assume $(g, h) = 1$ are also coprime, since if they share factors, then send all those factors to g, and that does not change irreducibility. But then $f'(x) = g'(x)h(x) + h'(x)g(x)$, which implies that $g(x) \mid g'(x)$ since $g \mid h'g$, $g \mid g'h$, and $g \nmid h$. But that is not possible, since g' must have a lower degree that g. Hence $(f, f') = 1$ are coprime.

Now suppose $(f, f') = 1$. Notice they cannot share a root in the splitting field in this case, which by Proposition 3.4.2 means $f(x)$ is separable.

Definition 3.4.14. Suppose E/F is an extension, and $\sigma\colon F \to L$ an embedding of fields. We denote the set of all homomorphisms $\sigma^*\colon E \to L$ extending σ, that is, $\sigma^*|_F = \sigma$ as $S_\sigma = \{\sigma^* \in \mathrm{Hom}(E, L) : \sigma^*|_F = \sigma\}$.

Theorem 3.4.15. Suppose $E = F(\alpha)$ is an algebraic extension of F, $L = \overline{L}$ is an algebraically closed field extension of F, and $p(x) = \min_F(\alpha) \in F[x]$ is the minimal polynomial. If $\sigma\colon F \to L$ is an embedding, then $|S_\sigma|$, the number of embeddings of E into L extending σ is the number of distinct roots of $\sigma(p)(x)$. In particular, $|S_\sigma| = [E : F]$ if and only if E/F is separable.

Proof.

Proposition 3.4.16. Suppose E/F is an algebraic extension, $L = \overline{L}$ algebraically closed, and $\sigma\colon F \to L$ an embedding of fields, Then there exists an embedding $\tau\colon E \to L$ that extends σ, i.e. $\tau|_F = \sigma$. If E is an algebraic closure of F, and L is the algebraic closure of $\sigma(F)$, then τ is an isomorphism.

Proof.

Proposition 3.4.17. Suppose E/F is a finite extension, $L = \overline{L}$ is algebraically closed, and $\sigma\colon F \to L$ an embedding of fields. There are at most $[E : F]$ different embeddings extending σ, that is, $|S_\sigma| \leq [E : F]$.

Proof.

Proposition 3.4.18. Suppose $F \subseteq E \subseteq L$ is a tower of field extensions. If L/F is separable, then L/E and E/F are separable.

Proof.

Theorem 3.4.19. Suppose E/F is a finite extension, $L = \overline{L}$ algebraically closed, and $\sigma\colon F \to L$ an embedding of fields. Then $|S_\sigma|$, the number of distinct embeddings of E into L extending σ is exactly $[E : F]$ if and only if E/F is separable.

Proof.

Theorem 3.4.20 (Transitivity of Separable Extensions)**.** Suppose $F \subseteq E \subseteq L$ is a tower of field extensions. If E/F and L/E are both separable, then L/F is separable.

Proof.

Separable Degree

Definition 3.4.21. Suppose E/F is a finite extension, $L = \overline{L}$ algebraically closed, and $\sigma\colon F \to L$ an embedding of fields. We call the number of embeddings of E to L extending σ the separable degree of E/F, denoted $[E : F]_s = |S_\sigma|$.

Corollary 3.4.22. Suppose E/F is a finite extension. Then $[E : F]_s \leq [E : F]$.

Proof. Restatement of Proposition 3.4.19.

Definition 3.4.23. Suppose E/F an extension. The separable closure of F in E is F_s, the field of all elements in E that are separable over F.

Proposition 3.4.24. Suppose E/F an extension. The separable degree is $[F_s : F] = [E : F]_s$.

Proof.

Corollary 3.4.25. Suppose E/F a finite extension. Then $[E : F]_s \mid [E : F]$.

Proof. Since $F \subseteq F_s \subseteq E$ a tower of field extensions, $[E : F] = [E : F_s][F_s : F]$ by Theorem 3.1.6. By proposition above $[F_s : F] = [E : F]_s$, which divides $[E : F]$.

Definition 3.4.26. Suppose E/F a finite extension, and F_s the separable closure. Then the degree of inseparability is $[E : F]_{pi} = [E : F_s]$. Hence by definition $[E : F] = [E : F]_{pi}[E : F]_s$.

Proposition 3.4.27. Suppose $F \subseteq L \subseteq E$ is a tower of finite extensions. Then $[E : F]_{pi} = [E : L]_{pi}[L : F]_{pi}$ and $[E : F]_s = [E : L]_s[L : F]_s$.

Proof.

Simple Extensions

Definition 3.4.28. Suppose E/F is an extension. E/F is simple (algebraic) if $E = F(\alpha)$ (for α algebraic over F). We call α a primitive element of E/F.

Theorem 3.4.29 (Primitive Element Theorem)**.** Suppose E/F is a finite separable extension. Then E/F is simple.

Proof.

3.5 Inseparability

Remark 3.5.1. Recall from Theorem 2.6.6 that fields come in 2 flavours, either characteristic 0 or prime p.

Proposition 3.5.2. Let $F = \mathbb{F}_p$. Suppose E/F is a finite extension where $[E : F] = n$. Then $|E| = p^n$.

Proof. Conclusion is obvious when we view E as an F-space.

Definition 3.5.3. Suppose F is a field with characteristic p. The Frobenius homomorphism is the map $\Phi\colon F \to F,\ x \mapsto x^p$.

Proposition 3.5.4. The Frobenius homomorphism is an endomorphism, and is an automorphism if the field is finite.

Proof.

$$\Phi(x+y) = (x+y)^p = x^p + y^p = \Phi(x) + \Phi(y)\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y)$$

This proves endomorphism. But field homomorphisms are always injective by Theorem 3.1.8, and so by the pigeonhole principle it is also surjective, which proves automorphism.

Corollary 3.5.5. Any nonzero element $a \in \mathbb{F}_p^\star$ is a pth power.

Proof. Simple restatement of the proposition above.

Proposition 3.5.6. Suppose F is a field of characteristic p, and $f(x) \in F[x]$ an irreducible polynomial. Then there exists some $g(x) \in F[x]$ irreducible and separable such that $f(x) = g(x^{p^m})$ for some unique $m \geq 0$.

Proof.

Definition 3.5.7. We call the degree of g the inseparable degree of $f(x)$, and p^m the separable degree of $f(x)$.

Proposition 3.5.8. Suppose $E = F(\alpha)$ is an extension of F, and $f(x) = \min_F(\alpha)$. Then the definitions of separable and inseparable degrees for the polynomial and the field coincide, that is, $[E : F]_s$ is the separable degree of $f(x)$, and $[E : F]_{pi}$ is the inseparable degree of $f(x)$.

Proof.

Proposition 3.5.9. Suppose F is a field. Then all roots of $f(x)$ have the same multiplicity. In particular,

(a) if F has characteristic 0, the multiplicity is 1; and

(b) if F has characteristic p, the multiplicity is p^n for some $n \in \mathbb{N}$

Proof. If F has characteristic 0, we know that the only irreducible polynomials are linear ones. They clearly have one root of multiplicity 1.

Now consider the case of characteristic p. Let $\{\alpha, \beta\} \subset \overline{F}$ be roots of $f(x)$. Consider the extensions $F(\alpha)$ and $F(\beta)$, and the homomorphism $\sigma\colon F(\alpha) \to F(\beta)$, $\alpha \mapsto \beta$ where $\sigma|_F = \mathrm{id}$. By Proposition 3.4.16, we can extend σ to $\tau \in \mathrm{Aut}(\overline{F})$. Let $f(x) = (x-\alpha)^m h(x) \in \overline{F}[x]$, $h(\alpha) \neq 0$. Then $f(x) = \tau(f)(x) = (x-\beta)^m \tau(h)(x)$. Therefore multiplicity of α at most the multiplicity of β. But this argument is symmetric, so the multiplicity of α is also at least multiplicity of β. Hence the multiplicities are equal.

Now suppose $f(x)$ irreducible. Note that from Proposition 3.5.6 we can find $g(x) \in F[x]$ such that $f(x) = g(x^{p^m})$. If a is a root of $f(x)$, then a^{p^m} is a root of $g(x)$, and hence a has multiplicity p^m since $x^{p^m} - a^{p^m} = (x-a)^{p^m}$.

Definition 3.5.10. Suppose F is a field with characteristic p, and E/F an algebraic extension. An element $\alpha \in E$ is purely inseparable if $\min_F(\alpha)$ has only one distinct root.

Definition 3.5.11. Suppose E/F an algebraic extension. E/F is purely inseparable if all elements in E are purely inseparable over F.

Lemma 3.5.12. Suppose F is a field with characteristic p. If α is algebraic over F, then α is purely inseparable over F if and only if $\alpha^{p^n} \in F$ for some n. In this case, $\min_F(\alpha) = (x-\alpha)^{p^n}$.

Proof.

Theorem 3.5.13. Suppose K/F is an algebraic extension. If $\alpha \in K$ is both separable and purely inseparable, then $\alpha = F$.

Proof.

Theorem 3.5.14. If K/F is purely inseparable, then K/F is normal. If K/F is purely inseparable, finite, and F has characteristic p, then $[K : F] = p^n$ for some n.

Proof.

Theorem 3.5.15. Suppose X a set, and $K = F(X)$, with alll $\alpha \in X$ purely inseparable. Then K is purely inseparable.

Proof.

Theorem 3.5.16. Suppose $F \subseteq L \subseteq K$ are a tower of extensions. K/F is purely inseparable if and only if K/L and L/F are purely inseparable.

Proof.

3.6 Perfect Fields and Normal Extensions

Perfect Fields

Definition 3.6.1. Suppose F is a field. F is perfect if every algebraic extension of F is separable.

Proposition 3.6.2. Suppose F is a field with characteristic p. F is perfect if and only if $F^p = F$, i.e. the Frobenius endomorphism $\Phi_p \colon F \to F,\ x \mapsto x^p$ is bijective.

Proof.

Proposition 3.6.3. Algebraically closed fields are perfect.

Proof.

Theorem 3.6.4. Finite fields are perfect.

Proof.

Lemma 3.6.5. Suppose F is a field with characteristic p. If $a \in F - F^p$, then $x^p - a$ is irreducible and inseparable.

Proof.

Lemma 3.6.6. Suppose F is a field with characteristic p. If $a \in F^p$, then $x^p - a$ is reducible.

Proof.

Proposition 3.6.7. Suppose p is a prime, and $x^p - 1$ splits completely over a field K. Let L/K be an extension, with $a \in L$ an algebraic element over K, and the prime $p \nmid [K(a) : K]$ does not divide the degree of the extension. Then $K(a) = K(a^p)$.

Proof.

Theorem 3.6.8. A field K is perfect if and only if its characteristic is 0, or if its characteristic is p and $K^p = K$.

Proof.

Normal Extensions

Definition 3.6.9. Suppose K/F is an algebraic extension. K/F is normal if $f(x) \in F[x]$ irreducible over F and has a root in K implies $f(x)$ splits completely in K.

Remark 3.6.10. In general, normality is not a transitive property, meaning that it does not stack.

Theorem 3.6.11. Suppose $F \subseteq K \subseteq L$ is a tower of extensions. If L/F is normal, then L/K is normal.

Proof.

Lemma 3.6.12. Suppose $F \subseteq E_i \subseteq E$ are two towers of extensions with $i \in \{1, 2\}$. If E_1/F and E_2/F are normal, then $(E_1 \cdot E_2)/F$ and $(E_1 \cap E_2)/F$ are normal.

Proof.

Lemma 3.6.13. Suppose F is a field, and K/F is an algebraic extension. Let I be some index set, and $i \in I$, with $F \subseteq E_i \subseteq K$ are intermediate extensions such that E_i/F is normal. Then $\bigcap_{i \in I} E_i$ is a normal extension of F.

Proof.

Lemma 3.6.14. Suppose K/F is a normal extension, and K_{sep} denotes the separable closure of F in K. Then $F \subseteq K_{\text{sep}} \subseteq K$ is a tower of normal extensions.

Proof.

Proposition 3.6.15. Let $F \subseteq K \subseteq L$ be a tower of field extensions.

(a) If K/F is normal, and $\tau \in \text{Aut}_F(L)$ is an F-automorphism, then $\tau|_K \in \text{Aut}_F(K)$.

(b) If L/F is normal, then any $\sigma \in \text{Hom}_F(K, L)$ extends to and F-automorphism over L.

Proof.

Theorem 3.6.16. Suppose E/F is an algebraic extension, with $E \subseteq \overline{F}$. The following are equivalent:

(a) Every $\sigma \in \text{Hom}_F(E, \overline{F})$ is also $\sigma \in \text{Aut}_F(E)$;

(b) E is a splitting field of a family of polynomials in $F[x]$; and

(c) E/F is normal.

Proof.

3.7 Finite Fields

Proposition 3.7.1 (Existence of Finite Fields)**.** Any finite field must be of order p^n for some prime p, and such fields exists for all $n \in \mathbb{N}$.

Proof. Suppose F is a finite field of characteristic p. Treating F as an additive group, $1 \in F$, $p \mid |F|$. Suppose, by way of contradiction, that there exists another prime $q \neq p$ such that $q \mid |F|$. Then by Cauchy's theorem, there exists $x \in F$ with order q so $qx = 0$. By Bézout's identity, there exists some a, b such that $ap + bq = 1$. Hence $x = (ap + bq)x = a(px) + b(qx) = 0$, which is contradiction as 0 does not have order q.

We can then apply Proposition 3.5.2 and simply have $\mathbb{F}_p(x)$, with $x^n \in 1$ to be our finite field.

Lemma 3.7.2. Suppose K is a field, and $G \subseteq K^*$ a finite subgroup of the multiplicative group. Then G is cyclic.

Proof. Let $|G| = n$, and $m = \exp(G)$. By Lagrange's theorem, $m \mid n$. If $g \in G$, then $g^m = 1$, so each element of G is a root of $x^m - 1$. This polynomial has at most m roots on K, which implies all the elements of G are roots of $x^m - 1$, so $n \leq m$. Hence we have $\exp(G) = |G|$ so G is cyclic.

Corollary 3.7.3. If K/F is an extension of finite fields, then K is a simple extension of F.

Proof. Consider $|K| = p^n$, so $|K^*| = p^n - 1$. If $a \in K^*$, then $a^{p^n - 1} = 1$. Hence $a^{p^n} = a$ for all $a \in K$. K is then the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, and is normal over $\mathbb{F}_p$ by Theorem 3.6.16. The derivative test yields separability.

Conlcude from the primitive element theorem and the lemma above, since cyclic groups have a single generator.

Remark 3.7.4. In fact the primitive element does not have to be a generator of the multiplicative group.

Corollary 3.7.5 (Uniqueness of Finite Fields)**.** Finite fields of the same cardinality are unique up to isomorphism.

Proof. Any two fields of order p^n are splitting fields over $\mathbb{F}_p$ of $x^{p^n} - x$. Conclude by uniqueness of splitting fields.

Lemma 3.7.6. The finite field $\mathbb{F}_{p^n}$ is expressible as $\mathbb{F}_p[x]/(f)$ for some $f(x) \in \mathbb{F}_p[x]$ of degree n.

Proof. Since Lemma 3.7.2 tells us that $\mathbb{F}_{p^n}^*$ is cyclic, we pick $\theta \in \mathbb{F}_{p^n}$ to generate it. Hence θ generates $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, and it will satisfy some irreducible polynomial $f \in \mathbb{F}_p[x]$. Then the evaluation map $\phi\colon \mathbb{F}_p[x] \to \mathbb{F}_{p^n},\ x \mapsto \theta$ induces an isomorphism $\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n}$, since $\deg f = n$.

Corollary 3.7.7. Suppose F is a finite field, and $f(x) \in F[x]$ is a monic irreducible polynomial of degree n. Then if a is a root of f in an extension of F, then $F(a)$ is the splitting field of f. Consequently, if K is a splitting field of f, then $[K : F] = n$. If $|F| = q$, then the roots are a^{q^r} for $r \geq 1$.

Proof. Let K be a splitting field of f. If $a \in K$ is a root, then $F(a)$ is an extension of F of degree n. By irreducibility $f(x) = \min_F(a)$, and the minimal polynomial splits in $F(a)$. Hence $K = F(a)$ is degree n.

Lastly, we see that $\min_F(a) = (x-a)^{p^n}$ by Lemma 3.5.12, and clearly $a^q - a = 0$.

Proposition 3.7.8. For some prime p and $n, m \in \mathbb{N}$, $m \mid n \iff \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

Proof. $\mathbb{F}_{p^m}$ is the set of roots of $x^{p^m} - x$ by the uniqueness of finite fields in some algebraic closure $\overline{\mathbb{F}}_p$. Note that if $m \mid n$, then $n = dm$, so

$$x^{p^n} = x^{p^{dm}} = \left(x^{p^{(d-1)m}}\right)^{p^m} = x^{p^{(d-1)m}} = \cdots = x^{p^m} = x$$

so x is a root of $x^{p^n} - x$, and $x \in \mathbb{F}_{p^n}$.

Conversely, suppose $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Then $\mathbb{F}_{p^n}$ can be treated as a $\mathbb{F}_{p^m}$-vector space of dimension d, by Proposition 3.1.4. Hence $p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d = (p^m)^d = p^{md}$, and $m \mid n$.

Proposition 3.7.9. Let $n \in \mathbb{N}$. Then $x^{p^n} - x$ factors over $\mathbb{F}_p$ into the product of all monic irreducible polynomials over $\mathbb{F}_p$ of degree m, where $m \mid n$.

Proof.

Lemma 3.7.10. Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over some finite field $\mathbb{F}_q$, and let α be a root of f in some extension. Then, for a polynomial $h \in \mathbb{F}_q[x]$, $h(\alpha) = 0$ if and only if $f \mid h$.

Proof.

Lemma 3.7.11. Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m. Then $f \mid x^{q^n} - x$ if and only if $m \mid n$.

Proof.

Corollary 3.7.12. If $N_q(d)$ is the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d, then

$$q^n = \sum_{d \mid n} d N_q(d) \qquad \forall n \in \mathbb{N}$$

where we are summing over all positive $d \mid n$.

Proof.