Algebra Comp Notes

Jay Havaldar

Contents

1 Group Theory, Part 1: Definitions and Basics **4**
- 1.1 Introduction . . . 4
- 1.2 The General Linear Group . . . 4
- 1.3 Subgroups . . . 5
- 1.4 Homomorphisms . . . 7
  - 1.4.1 Cayley's Theorem . . . 7
- 1.5 Normal Subgroups . . . 7
- 1.6 The Isomorphism Theorems . . . 9
  - 1.6.1 Endomorphisms of Abelian Groups . . . 10

2 Group Theory, Part 2: The Sylow Theorems **11**
- 2.1 Group Actions . . . 11
- 2.2 Sylow Subgroups . . . 12
  - 2.2.1 Theorem . . . 13
  - 2.2.2 Theorem: First Sylow Theorem . . . 13
  - 2.2.3 Theorem: Second Sylow Theorem . . . 14
  - 2.2.4 Sylow's Third Theorem . . . 15

3 Ring Theory, Part 1: Introduction to Rings **16**
- 3.1 Ideals and Homomorphisms . . . 16
  - 3.1.1 Isomorphism Theorems for Rings . . . 17
- 3.2 Properties of Ideals . . . 18
- 3.3 Quotient Fields . . . 20
- 3.4 The Chinese Remainder Theorem . . . 21

4 Ring Theory, Part 2: Classification of Integral Domains **23**
- 4.1 Euclidean Domains . . . 23
- 4.2 Principal Ideal Domains . . . 24
- 4.3 Unique Factorization Domains . . . 25

5 Module Theory, Part 1: Introduction, Module Homomorphisms **27**
- 5.1 Quotient Modules and Module Homomorphisms . . . 28

6 Module Theory, Part 2: Generation of Modules, Direct Sums, Free Modules **30**
  - 6.0.1 Theorem . . . 31

7 Representation Theory, Part 1: Introduction **33**
- 7.1 Duals and Tensor Products of Representations; Representation of $Hom(V, W)$ . . . 33
- 7.2 Complete Reducibility; Schur's Lemma . . . 35
- 7.3 Examples: Abelian Groups; S_3 . . . 37

8 Representation Theory, Part 2: Character Theory **40**
8.1 Properties of Characters 40
8.2 Character Tables 41
8.3 The First Projection Formula 41
8.4 Character of the Regular Representation 43
8.5 Abelian Subgroups and Products of Groups 44

9 Field Theory, Part 1: Introduction, Algebraic Extensions **47**
9.1 Introduction 47
9.2 Algebraic Extensions 50

10 Field Theory, Part 2: Splitting Fields, Algebraic Closure **54**
10.1 Splitting Fields 54
10.2 Separable Extensions 59
10.3 Cyclotomic Polynomials and Extensions 63

11 The Fundamental Theorem of Galois Theory **65**
11.1 Introduction 65
11.2 The Fundamental Theorem of Galois Theory 68

1 Group Theory, Part 1: Definitions and Basics

1.1 Introduction

A **group** is a set together with a binary operation (multiplication) so that:

- Multiplication is associative.
- There is an identity e so that $eg = ge = g$.
- For each g there is an inverse g^{-1} so that $gg^{-1} = g^{-1}g = e$.
- The group is closed under multiplication.

The **order** of an element a is the minimum integer n so that $a^n = e$. The subgroup consisting of all elements of the group of finite order is called the **torsion subgroup**.

Example An important example of a group is the dihedral group D_n. It is generated by two kinds of elements: rotations, and reflections. It describes the symmetries of an n-gon with composition. The two kinds of elements are respectively described as:

$$r^n = es^2 = esrs = r^{-1}$$

D_1 is for example defined as
$1, r$ so it is simply $\mathbb{Z}/2\mathbb{Z}$. On the other hand, $D_2 =$
$1, r, s, rs$ is not cyclic; it is called the **Klein** group or the 4-group, which is distinct from $\mathbb{Z}/4\mathbb{Z}$.

1.2 The General Linear Group

An important group is the general group $GL(V)$. For an n-dimensional vector space V over a field, we can think of $GL(V)$ as the set of $n \times n$ matrices over a field with nonzero determinant -- with multiplication defined in the usual way (once we fix a basis).

A **bilinear form** $\phi : V \times V \to F$ that is linear in each variable. An **automorphism** of ϕ is is an isomorphism $\alpha : V \to V$ so that:

$$\phi(\alpha v, \alpha w) = \phi(v, w)$$

With a choice of a basis, we can restate this condition in terms of the matrix for α and the matrix P for ϕ:

$$(Av)^T \cdot PAw = v^T Pw$$
$$v^T A^T PAw = v^T Pw$$

So:

$$A^T PA = P$$

In particular, if ϕ is **symmetric**, i.e.:

$$\phi(v, w) = \phi(w, v)$$

Then we have the following definition.

Definition: For a symmetric non-degenerate bilinear form ϕ, define its automorphism group $Aut(\phi)$ to be the isomorphisms α so that $\phi(\alpha v, \alpha w) = \phi(v, w)$. This is called the **orthogonal group** of ϕ.

Definition: For a skew-symmetric non-degenerate bilinear form ϕ, define its automorphism group $Aut(\phi)$ to be the isomorphisms α so that $\phi(\alpha v, \alpha w) = \phi(v, w)$. This is called the **symplectic group** of ϕ.

In this case, we can write ϕ in some basis as the matrix:

$$J_{2m} = \begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix}$$

Where $2m = n$. Therefore, the symplectic group condition simply means a matrix has the property:

$$A^T J_{2m} A = J_{2m}$$

1.3 Subgroups

A subgroup is a subset of a group which is closed under multiplication and inverses, and which contains the identity. A particularly important is called the center of a group.

Definition: The **center** of a group G, denoted $Z(G)$ consists of all the elements which commute with all of G, i.e.:

$$Z(G) = \{z \in G \ : \ zx = xz \ \forall x \in G\}$$

Proposition

An intersection of subgroups is a subgroup.

The proof here is fairly straightforward.

We can talk about the **cosets** of a subgroup H as elements of the form aH for some $a \in G$, where:

$$aH = \{ah \ : \ h \in H\}$$

Cosets are well-defined, and are either disjoint or equal. Suppose that $a \ inbH$, then we can say for some $h \in H$:

$$a = bhaH = bhH = bH$$

So that means we can write a coset as aH for any choice of representative a. By the above argument, if two cosets share a single element, they are the same set. Finally, we can map aH to bH via multiplication by ba^{-1} (and conversely, map from bH to aH via multiplication by ab^{-1}). Thus, all the cosets are the same size.

Definition: The **index** of a subgroup H of G is the number of left cosets of H in G, and is denoted $(G : H)$.

Proposition (Lagrange's Theorem)

The order of a subgroup divides the order of the group.

We have:

$$|G| = (G : H)|H|$$

Therefore, $|H|$ divides $|G|$.

As a corollary, we consider the group generated by a certain element a. It has size n, where n is the order of a, and forms a subgroup. Thus, the order of any element in a group divides the order of the group.

We also have the following ``cancellation'' theorem. If H is a subgroup of G and K is a subgroup of H, we have:

$$(G : K) = (G : H)(H : K)$$

1.4 Homomorphisms

Definition: A **homomorphism** between groups G, G' is a map $\varphi : G \to G'$ so that $\varphi(ab) = \varphi(a)\varphi(b)$. In a sense, a homomorphism preserves the structure of the group. If a homomorphism is bijective, we say that it is an **isomorphism**.

1.4.1 Cayley's Theorem

An important theorem is Cayley's Theorem, which says we can think of each group as a subgroup of a permutation group. For $a \in G$, define the map:

$$\phi_a : G \to G \phi_a(b) = ab$$

Thus, the map ϕ_a is just multiplication by A. We can also show that it is a bijection, since we have:

$$\phi_a \circ \phi_{a^{-1}}(b) = \phi_a(a^{-1}b) = aa^{-1}b = b$$

And in fact we can say that: - Each ϕ_a is a bijection from G to G, hence $\phi_a \in S_{\|G\|}$, the symmetric group or group of permutations of G. - The map $\Phi : a \mapsto \phi_a$ is an injective map from G to $S_{\|G\|}$.

So this brings us to Cayley's Theorem:

Any finite group is a subgroup of a symmetric group.

1.5 Normal Subgroups

Definition: A subgroup N of a group G is normal if $gNg^{-1} = N$ for all $g \in G$. A normal subgroup is denoted $N \trianglelefteq G$.

It is sufficient to check that $gNg^{-1} \subset N$ for each g, since multiplying gives us $Ng^{-1} = g^{-1}N \implies N \subseteq g^{-1}Ng$, and substituting $g = g^{-1}$ we get the reverse inclusion.

Note however, that we can find a subgroup N and an element g so that $gNg^{-1} \subset N$ with strict inequality; however, if this holds for all g, then we indeed have a normal subgroup.

Proposition

Every subgroup of index two is normal.

Suppose H is a subgroup of index two. Pick $g \in G$ which is not in H. then gH is the complement of H. Similarly, Hg is the complement of H. So we have $gH = Hg$. Then $gHg^{-1} = H$.

Definition: A group is **simple** if it has no normal subgroups other than itself and the trivial subgroup.

Proposition

Suppose H, N are subgroups of G and N is a normal subgroup. Then $HN = \{hn \ : \ h \in H, n \in N\}$ is a subgroup of G. If H is also a normal subgroup, then HN is a normal subgroup of G.

Note that $gNg^{-1} = N$, so that we can write $gN = Ng$. For any $n \in N$, we can write $gn = n'g$ where $n' \in N$.

Taking $h_1n_1, h_2n_2 \in HN$, we have:

$$(h_1n_1)(h_2n_2) = h_1h_2n_1'n_2 \in HN$$

So indeed HN is closed under multiplication. It contains the identity automatically, and we can check inverses:

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}n'^{-1} \in HN$$

So indeed HN is a subgroup.

If H, N are both normal, we can write:

$$gHNg^{-1} = gHg^{-1}gNg^{-1} = HN$$

And we are done. We can also define the normal subgroup generated by any set in G.

Definition: For any set $X \subset G$, the smallest normal subgroup generated by X is exactly:

$$\bigcup_{g \in G} gXg^{-1}$$

Theorem

A subgroup N of G is normal iff it is the kernel of some homomorphism.

Evidently, the kernel of a homomorphism is a normal subgroup since for any $x \in \ker \varphi$:

$$\varphi(gxg^{-1}) = \varphi(g)e\varphi(g)^{-1} = e$$

Conversely, we map $g \mapsto gN$, i.e. map to cosets. We just need to show that G/N has a group structure which is preserved by this map. Define $(aN)(bN) = (ab)N$. We need to show that this multiplication is well defined.

Suppose that $aN = a'N$ and $bN = b'N$. Then we can show:

$$abN = a(bN) = ab'N = aNb' = a'Nb' = a'b'N$$

Where we use freely here that $aN = Na$ by the fact that N is a normal subgroup. So indeed this map is well defined, and preserves the group structure, and its kernel is evidently N. We call G/N the **quotient** of G by N.

1.6 The Isomorphism Theorems

As per usual, we have the isomorphism theorems.

First Isomorphism Theorem

Let $\varphi : G \to G'$ be a homomorphism of groups. Then:

$$\frac{G}{\ker \varphi} \cong \varphi(G)$$

And since $\ker \varphi$ is a normal subgroup by the above discussion, we have that $\varphi(G)$ is a subgroup of G'.

Second Isomorphism Theorem

Let S be a subgroup of G, and N a normal subgroup of G. Then: - SN is a subgroup of G. - $S \cap N$ is a normal subgroup of S. - $\frac{SN}{N} \cong \frac{S}{S \cap N}$.

Third Isomorphism Theorem

Suppose K, N are normal subgroups of G with $N \subseteq K \subseteq G$. Then:

$$\frac{G/N}{K/N} \cong \frac{G}{K}$$

Furthermore, we have the following correspondences from the third isomorphism theorem:

"Fourth" Isomorphism Theorem

Suppose N is a normal subgroup of G. Then there is a correspondence between subgroups K of G which contain N and subgroups of G/N, given by:

$$K \leftrightarrow kN$$

Where $k \in K$ is a representative. Similarly, the same bijection gives a correspondence between normal subgroups K of G which contain N and normal subgroups of G/N.

1.6.1 Endomorphisms of Abelian Groups

Definition: An **endomorphism** is a homomorphism from a group to itself.

Definition: An **automorphism** is an isomorphism from a group to itself, i.e. a bijective endomorphism.

For any group, there is at least one endomorphism: the so-called trivial endomorphism, which sends every element to 0.

In particular, suppose that we have an abelian group, and two endomorphisms $f, g \in End(G)$. Then we have for fixed $a \in G$:

$$(f+g)(a+b) = f(a+b) + g(a+b) = f(a) + f(b) + g(a) + g(b)$$

Now, as a consequence of the fact that G is abelian, we then can write:

$$(f+g)(a+b) = f(a) + g(a) + f(b) + g(b) = (f+g)(a) + (f+g)(b)$$

And so $f + g \in End(G)$. Thus, $End(G)$ is in particular a group (since it is closed under addition). Indeed it is a ring as well, with multiplication as composition. With some work, in some cases we can think of an endomorphism ring as a ring of matrices. In all cases, we can think of rings as subrings of the endomorphism ring of some underlying abelian group (in fact, itself considered as a group).

2 Group Theory, Part 2: The Sylow Theorems

The Sylow theorems tell us quite a lot of information in general about the subgroups of a group of finite order. In this post, I'll be covering the basic ideas behind and finally the proofs of the Sylow theorems.

2.1 Group Actions

First, we describe group actions. For any group G and a set S, we can define a group action $\rho : G \to Perm(S)$ which is a homomorphism from the group to the symmetric group (the set's permutations group). Alternatively, we could define the group action as operating on pairs in the product $G \times S$, i.e.:

$$\rho : G \times S \to S$$

With this definition, we also require associativity and also the action of the identity ($\rho(e, s) = s$).

Example For example, we look at conjugation. Let $C_x : G \to G$ be the map so that $C_x : y \mapsto xyx^{-1}$.

We can indeed think of $C : x \mapsto C_x$ as a homomorphism, from G to $Aut(G)$. The kernel of this homomomorphism is all the elements x so that:

$$C_x(y) = xyx^{-1} = yxy = yx$$

We denote the kernel of this homomorphism as the **center** of G, denoted $Z(G)$, and it consists of all elements $x \in G$ which commute with the group.

Definition: For a defined group action $\rho : G \to S$, the **stabilizer** of $s \in S$ consists of all the elements $x \in G$ so that $\rho(x, s) = s$. In other words, the stabilizer of s is all the group elements which send s to itself. Often it is denoted G_s.

Definition: In the case where ρ is the conjugation group action, we define the **centralizer** of a. These are all the elements $x \in G$ which commute with a. The group of all elements which fix a subgroup $H \subseteq G$ is called the **normalizer** of H.

Definition: We define the **orbit** of $s \in S$ under G to be the set $xs|x \in G$. In the case of the conjugation action, we refer to the orbits as **conjugacy classes** and it is clear that they form an equivalence class for the set.

There is a natural bijection between G/G_s and Gs, with the explicit bijection given by $hG_s \to hs$. Furthermore, the order of the orbit Gs is equal to the index $(G : G_s)$.

In particular, the number of conjugate subgroups to H is equal to the index of the normalizer of H. Also, the number of elements in the conjugacy class of x is equal to the index of the centralizer, i.e. G/G_s.

Example We will prove that every subgroup of index 2 is normal. Let S be the set of cosets of H defined in the usual way (there should be two). Then, the group action is defined as a homomorphism from G to $S_2 = Z_2$. Consider the kernel K of this homomorphism; this is all group elements $g \in G$ so that $gH = H$. So, the kernel of this homomorphism is a subgroup of H. But then that means G/K is a subgroup of Z_2. So $(G : K)$ is either 1 or 2. But we know that:

$$(G : K) = (G : H)(H : K)$$

And $(G : H) = 2$, so we must have $(H : K) = 1$ so this tells us that $(H : K) = 1$ and indeed $H = K$. So that means H is the kernel of the given homomorphism.

But for any homomorphism ϕ, if we pick an arbitrary $g \in G$ and k in the kernel, we have $\phi(gkg^{-1}) = \phi(g)\,\phi(k)\,\phi(g)^{-1} = e$. So indeed, the kernel is a normal subgroup. Therefore, H from the previous example is a normal subgroup.

We also can write the obvious fact that the order of a set S is the sum of all the orbits in this new notation, in the **decomposition formula:**

$$|S| = \sum_{G_s} (G : G_s)$$

We have a special case where the group action is conjugation. In this case, we take Y to be a set of representatives from each conjugation class and write the **class formula**:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$

2.2 Sylow Subgroups

Definition Let p be a prime number. Then a Sylow p-group is a finite group of order p^n for some n.

With this definition, we prove an intermediate theorem:

2.2.1 Theorem

Let G be a non-trivial p-group. Then G has a non-trivial center. Furthermore, G is solvable.

Proof From the class formula, we have:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$

If the center is trivial, then the sum on the RHS of the equation adds up to $|G| - 1 $. Since G is a p-group, the prime p divides both sides of the equation. However, this is clearly impossible since p does not divide $\|G\| - 1$. So the center is non-trivial.

We also know that $G/Z(G)$ is a p-group as well, and it is strictly smaller than G. The rest of the proof proceeds by induction on n.

We know for a fact that cyclic groups are solvable (with the shortest normal series which is abelian). Suppose the theorem holds for all p-groups with $n \leq k - 1$. Then, we have that $Z(G)$ and $G/Z(G)$ are both solvable since they are p-groups as well. So, we have proved the $n = k$ case.

2.2.2 Theorem: First Sylow Theorem

Suppose that we have $p^n \mid G$ and $p^{n-1} \nmid G$ for some prime p. Then, define a Sylow p-subgroup of G to be a subgroup of order p^n. We will prove that for every $p \mid G$, there exists a p-Sylow subgroup.

Lemma: Cauchy's Theorem We start with the brief lemma that for any finite abelian group G, for any prime $p \mid \ |G|$, there is a subgroup in G of order p. This is known as Cauchy's lemma and is a special case of Sylow's First Theorem.

By the fundamental theorem of finite abelian groups, G can be written as the direct product:

$$G = G(p) \times G'$$

Where $|G'|$ is prime to p. Take an element $a \in G(p)$ with order p^k. Then take:

$$b = a^{p^{k-1}}$$

We know that b is not the identity. However, $b^p = a^p = e$. So, b generates a cyclic group of order p, and we are done.

In fact, we can generalize Cauchy's theorem to arbitrary finite groups using the class equation:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$

Suppose that $p \mid |Z(G)|$. Then we can apply the earlier proof to $Z(G)$ to find an element of order p in $Z(G) \subseteq G$; so we are done.

Suppose instead that $p \nmid \|Z(G)\|$. Then, the sum on the right hand side cannot divide p either, and in particular there is at least one conjugacy class G_y with order prime to p. Therefore, $p \nmid |\frac{G}{G_y}|$. But this means that G_y divides p! Applying Cauchy's lemma to this group, we find an element of order p in G_y and therefore in G, and we are done.

Proof of Sylow's First Theorem Cauchy's lemma proves that G certainly has a subgroup of size p. With Sylow's first theorem, we prove that G has a subgroup of size p^n, where p^n is the largest power of p dividing the order of G. We proceed by induction on the size of G.

Suppose that there is a proper subgroup $H \subset G$ so that $(G : H)$ does not divide p. Then $p^n \mid \|H\|$, and so by induction H has a p-Sylow subgroup which is also a p-Sylow subgroup of G. We assume then that every proper subgroup $H \subset G$ has the property that $p \mid (G : H)$. Now, we let G act on itself by conjugation and consider the class formula:

$$|G| = |Z(G)| + \sum_{y \in Y} (G : G_y)$$

The order of each of the orbits divides the order of the group (since a stabilizer or in this case a conjugacy class, is a subgroup), so p divides the order of $Z(G)$, and G has a non-trivial center; furthermore, by a similar proof to Cauchy's lemma, we have that G contains a subgroup H of size p. Furthermore, since H is a subgroup of the center in particular, it is a normal subgroup.

We consider the group G/H. By the inductive hypothesis, this group has a subgroup K' of order p^{n-1}. By the third isomorphism theorem, K' is really (isomorphic to) a subgroup of the form K/H, where $H \subset K \subset G$. Take this K; it has order p^n as desired.

2.2.3 Theorem: Second Sylow Theorem

The second Sylow Theorem states that all p-Sylow subgroups are conjugate to each other. Before we get to that, let's prove a related lemma:

Lemma: Every p-subgroup of G is contained in some p-Sylow subgroup. This isn't hard to prove using the class formula. Let S be the set of p-Sylow subgroups of G, and G operates on S by conjugation. Let's take P to be one of those Sylow subgroups. Then we have:

$$|Orb(P)| = \frac{|G|}{|G_P|}$$

Where G_P is the normalizer of P which sends P to itself under conjugation. Evidently, G_P contains P, so that means $\|Orb(P)\|$ is prime to p. Let's take a look at the action of a p-subgroup H on $Orb(P)$ using the class formula:

$$|Orb(P)| = |Z| + \frac{|Orb(P)|}{|H_{Orb(P)}|}$$

By Lagrange, each term in the right hand sum divides $ |H| $ so that means there is a non-trivial center P' within $\|Orb(P)\|$. This means that H is contained within the normalizer of P'. Since H is contained in the normalizer, by the second isomorphism theorem we know that HP' is a subgroup with $P' \trianglelefteq HP'$. The order of the quotient group $HP'/P \cong H/(H \cap P')$ is a power of p, so the order of HP' is also a power of p. But then $HP' = P'$ since P' is a maximal p-subgroup of G; and therefore $H \subseteq P'$. We have now found a Sylow subgroup which contains H.

Proof of Sylow's Second Theorem Let H be some p-Sylow subgroup of G. H is contained in some conjugate P' of P by the above argument. And again by the above construction, because H and P' have equal orders, $H = P'$.

This second theorem implies as a direct corollary that if there is only one p-Sylow subgroup, it is normal.

2.2.4 Sylow's Third Theorem

Sylow's Third Theorem is arguably the most useful. It says that the number of p-Sylow subgroups of G is equal to $1 \mod p$. That means by counting arguments, if $\|G\|/p^n < p$, then the Sylow subgroup is normal.

Proof of Sylow's Third Theorem Take the action of $H = P$ on the set S consisting of the Sylow p-subgroups. Any other orbit cannot have just one element P', or else H is contained in the normalizer of P', and by earlier arguments $H = P = P'$. Take an element s' of any other orbit. It has a stabilizer, which is a proper subgroup of H; the stabilizer is a subgroup, so it is divisible by p.

As a result, the number of elements in S' is divisible by p. So the size of S (the set of all p-Sylow subgroups) is equal to 1 (the size of the center of conjugation under P) plus the size of all the remaining orbits (all of which have orders which divide p). So we are done.

3 Ring Theory, Part 1: Introduction to Rings

Definition: A **ring** R is a set with an addition and a multiplication operation which satisfies the following properties: - R is an abelian group under addition. - Distributivity of addition and multiplication. - There is a multiplicative identity 1. Some authors do not include this property, in which case we have what is called a **rng**.

Note that I denote 0 to be the additive identity, i.e. $r + 0 = 0 + r = 0$ for $r \in R$.

A **commutative ring** has a commutative multiplication operation.

Definition: Suppose $xy = 0$, but $x \neq 0$ and $y \neq 0$. Then x, y are called **zero divisors**.

Definition: A commutative ring without zero divisors, where $1 \neq 0$ (in other words our ring is not the zero ring), is called an **integral domain**.

Definition: A **unit** element in a ring is one that has a multiplicative inverse. The set of all units in a ring is denoted $R^\times$, often called the multiplicative group of R.

Definition: A **field** is a commutative ring in which every nonzero element is a unit.

Examples of rings include: $\mathbb{Z}, End(R, R)$. Examples of integral domains include $\mathbb{Z}$ (hence the name), as well as the ring of complex polynomials. Examples of fields include $\mathbb{Q}, \mathbb{C}, \mathbb{R}$.

Note that not every integral domain is a field, but as we will later show, every field is an integral domain.

Now we can define a fundamental concept of ring theory: ideals, which can be thought of as the analogue of normal groups for rings, in the sense that they serve the same practical role in the isomorphism theorems.

3.1 Ideals and Homomorphisms

Let R be a ring. A **left ideal** J is a subset of R satisfying the following properties: - J is closed under addition. - For every $x \in J$, $r \in R$, we have $rx \in J$

We can change the second property to closure under right multiplication for a right ideal; in the case of commutative rings we just speak of ideals. Note that the second condition guarantees that $0x = 0$ is in every ideal.

Definition: A **ring homomorphism** is a map φ between rings so that: - $\varphi(x + y) = \varphi(x) + \varphi(y)$. - $\varphi(xy) = \varphi(x)\varphi(y)$. - $\varphi(1) = 1$.

In this way, a ring homomorphism preserves structure. Note that an ideal in a ring is automatically a normal subgroup since a ring is an additive abelian group. We can extend this analogy by generalizing fundamental theorems regarding normal groups. We now come to the isomorphism theorems for rings, which are analogues of the same theorems for groups.

3.1.1 Isomorphism Theorems for Rings

First Isomorphism Theorem Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker \varphi$ is an ideal of R, and $\varphi(R)$ is a subring of S. Furthermore:

$$S/\ker \varphi \cong \varphi(R)$$

We can also define a canonical homomorphism $\varphi : R \to R/I$ from R to the ring of representative cosets of I, such that $\varphi : r \mapsto r + I$.

It is not hard to prove that this is a well-defined homomorphism; indeed, this is a homomorphism whose kernel is I. In this way, we show that every ideal is the kernel of a homomorphism, and that every kernel of a homomorphism is an ideal.

Second Isomorphism Theorem Let A be a subring of and B an ideal of R. Then the following set is a subring of R:

$$A + B = \{a + b \mid a \in A, b \in B\}$$

Furthermore, $A \cap B$ is an ideal of A, and finally:

$$(A + B)/B \cong A/(A \cap B)$$

Third Isomorphism Theorem Let I, J be ideals of R, with $I \subseteq J$. Then J/I is an ideal of R/I and:

$$(R/I)/(J/I) \cong R/J$$

We also have an analogue for the correspondence theorem for groups:

Correspondence Theorem for Rings As before, we can construct a bijection from the set of all subrings of R which contain and ideal I, and the subrings of R/I. In particular, the bijection is the map $J \mapsto J/I$, where $I \subseteq J$ and J is a subring of R which contains I.

Example Let $R = C[0,1]$, the continuous functions defined on the interval $[0,1]$. Then:

$$I = \left\{ f \in R \mid f(\frac{1}{2}) = 0 \right\}$$

I is an ideal.

Example Let $R = \mathbb{Z}$, the ring of integers. Then, an ideal can be written:

$$I_a = \{na \mid n \in \mathbb{Z}\}$$

Pick any integer a. If an ideal contains a, by multiplicative closure it also contains all the integer multiples of a.

3.2 Properties of Ideals

Let R be a ring and $a \in R$. Then we denote (a) as the **ideal generated by** a. An ideal generated by one element is called **principal ideal**. An ideal generated by a finite set of generators is called a finitely generated ideal. A principal ideal is something like a cyclic group, and a finitely generated ideal is something like a finitely generated subgroup.

Definition: Let I, J be ideals of R. Then we can construct the following ideals:

$$I + J = \{a + b \mid a \in I, b \in J\}$$

$$IJ = \left\{ \sum_{i=1}^{k} ab \mid a \in I, b \in J, k \in \mathbb{Z} \right\}$$

$$I^n = I^{n-1} I$$

Since an ideal contains the additive identity, it is clear that $I + J$ contains both I and J, and indeed it is the smallest ideal which contains both. Also note that IJ must contain the finite sums of elements of the form ab, since without that condition we would not have closure under addition. These constructions will be useful for many later proofs.

Definition: Let R be a commutative ring. P is called a **prime ideal** if $P \neq R$ and whenever $ab \in P$, then $a \in P$ or $b \in P$ (possibly both).

The definition of a prime ideal should look something like the definition of a prime number. If an integer ab divides a prime, then one of the two factors divides the prime. Indeed, (p) is a prime ideal in the integers for any prime p (and 0 is the only other prime ideal).

Proposition Suppose R is a commutative ring. Then P is a prime ideal iff R/P is an integral domain.

Proof: Suppose P is prime. Then $ab = 0$ in R/P iff $ab \in P$ in R. Thus, if R/P is an integral domain, then $ab = 0$ iff $a = 0$ or $b = 0$, or equivalently, $ab \in P$ iff $a \in P$ or $b \in P$. The converse follows similarly.

We will now take a look at the ideal structure of fields.

Proposition Let I be an ideal of R. Then $I = R$ iff I contains a unit.

Proof: If I contains a unit u, then $(ru^{-1})u \in I \implies r \in I$ for any element $r \in R$.

Proposition Let R be a commutative ring. Then R is a field iff its only ideals are 0 and R.

Proof: Suppose R is a field, and thus every non-zero element is a unit. By the previous proposition, every non-zero ideal is R. Conversely, suppose R has no proper non-trivial ideals. Take an arbitrary non-zero element $u \in R$. By hypothesis, $(u) = R$, so in particular $1 = vu$ for some $v \in R$. Thus, R is a field because all its non-zero elements are units.

Corollary If R is a field, then any nonzero ring homomorphism from R into another ring is an injection.

The kernel of any homomorphism is an ideal by the isomorphism theorems; since 0 is the only proper ideal, the kernel of any homomorphism is 0 and we have an injection.

So the ideal structure of fields is fairly simple.

Definition: An ideal M is called a maximal ideal in a ring R if the only ideal properly containing M is R.

Not all rings have maximal ideals. However, we can guarantee their existence by assuming **Zorn's Lemma**, which is equivalent to the controversial axiom of choice. I won't go into the proof here, but note that we don't need to invoke the axiom of choice to guarantee maximal ideals most rings; sometimes the maximal ideals are fairly obvious.

Proposition In a ring with identity every proper ideal is contained in some maximal ideal.

Now, we draw the connection between maximal ideals and fields.

Proposition Suppose R is a commutative ring. Then M is a maximal ideal in R iff R/M is a field.

Proof: By the correspondence theorem, there is a canonical homomorphism between the ideals of R/M and the ideals of R containing M. It is immediately clear that M is maximal if and only if R/M has no nonzero proper ideals, and is thus a field.

This proposition is crucial, as it allows us to construct fields in rings with maximal ideals simply by taking a quotient with a maximal ideal.

Proposition Assume R is commutative. Every maximal ideal of R is a prime ideal.

Proof: If an ideal is maximal, then R/M is a field. A field is certainly an integral domain, since $xy = 0 \implies x^{-1}xy = 0 \implies y = 0$. Therefore, M is a prime ideal.

We have thus shown that fields are a proper subset of integral domains; and that maximal ideals are proper subsets of prime ideals.

3.3 Quotient Fields

A reasonable question to ask is: how can we turn a (commutative) ring into a field? The simple answer is that we add inverses.

We model our answer after the rational numbers. We define fractions of the form $\frac{a}{b}$, where $a, b \in R$, and say that $\frac{a}{b}$ is equivalent to $\frac{c}{d}$ if $ad = bc$. We define a new ring with the elements being the equivalence classes of such fractions, and it's easy to check that with addition and multiplication as in $\mathbb{Q}$, we nearly have a well-defined ring.

The one issue is that we can't have zero or zero divisors in the denominator, or else we will end up with nonsensical statements like $0 = 1$ To avoid this, we assume R is integral (no zero divisors). It is easy to see then that we have invented a field, called the **quotient field** of R, which we will call K.

Definition: Let R be an integral domain. Then we define Quot(R) to be the field constructed by identifying equivalence classes of pairs (a, b) in R ($b \neq 0$) under the equivalence relation (a, b) $(cd) \iff ad = bc$, with the ring structure defined above.

There is a natural map from R into K, so that $r \mapsto \frac{r}{1}$. It is not hard to see that this is an injective ring homomorphism.

Definition: An injective ring homomorphism is called an **embedding**.

Suppose that R is a subring of a field F. Then we can create a field of elements of the form ab^{-1}, where $a, b \in R$ and $b \neq 0$. This is called the quotient field of R in F. This construction is naturally isomorphic to the above quotient field of R, with the isomorphism:

$$a/b \mapsto ab^{-1}$$

An important property of a quotient field is that it is in a way, the smallest field in which we can embed a ring. This is illuminated in the following theorem.

Theorem Let R be an integral ring, and $f : R \to E$ be an embedding of R into some field E. Let K be the quotient field of R.

Then, there is a unique embedding f^* from K to E, such that $f = f$, when restricted to $R \subset K$.

Visually, K, f^* is the unique pair of field and embedding so that the following diagram works out:

In category theory terms, the field of fractions of R is universal with respect to the property of embedding R into a field F.

Where i is the natural embedding of R into its quotient field and f is an injective ring homomorphism into a field E.

Indeed, we can just define $f^*(a/b) = f(a)/f(b) = f(a)f(b)^{-1}$.

Examples of Quotient Fields When we pick the integral domain $\mathbb{Z}$, we obtain the quotient field $\mathbb{Q}$, as expected. When we pick the ring of polynomials (soon to be defined rigorously), we get the rational functions as the quotient field. Taking the quotient field of a quotient field returns itself.

3.4 The Chinese Remainder Theorem

The goal is to eventually look at direct product decompositions of groups and rings. To that end, we introduce the Chinese Remainder Theorem.

Definition: The **direct product** of a finite list of commutative rings is defined as their product as abelian groups, with multiplication defined componentwise.

We also need the following definition:

Definition: Two ideals A, B in a commutative ring R are comaximal if $A + B = R$.

For example, in the ring of integers, the principal ideals generated by any two two coprime integers are co-maximal, and this is the prototypical example. Finally, we are ready to state the theorem:

Theorem (Chinese Remainder Theorem) Let A_i be a finite set of ideals in a commutative ring R. Then the map $\phi : R \to R/A_1 \times R/A_2 \times ... \times R/A_k$ defined by $r \mapsto (r + A_1, r + A_2, ..., r + A_k)$ is a ring homomorphism with kernel $\cap_{i=1}^k A_i$.

Furthermore, if the ideals A_i are pairwise comaximal, then the map ϕ is surjective and $\cap_{i=1}^k A_i = \Pi_{i=1}^k A_i$.

Proof We will prove the case for $k = 2$, and the rest of the proof follows by induction. First, we note that ϕ is of course a ring homomorphism since each natural projection map is a homomorphism, and the kernel is evident.

Say we are working with only two ideals A, B which are comaximal. Since $A+B = R$, we can find $x + y = 1$ with $x \in A, y \in B$. Thus, $x = 1 - y$ mod $B = 1$ mod B, and similarly $y = 1$ mod A.

So our map has $\phi(x) = (0, 1)$, and $\phi(y) = (1, 0)$. Now, we know the map is surjective, since if we pick arbitrary $a, b \in R$, then $\phi(ax + by) = (a + A, b + B)$.

We already knew that $AB \subset A \cap B$, since ideals are closed under left multiplication by any element in R. Furthermore, if $c \in A \cap B$, then $c = cx + cy \in AB$, so indeed $A \cap B \subset AB$ and the two are equal.

We could continue this argument inductively by setting $A = A_1$ and $B = A_2...A_k$ (which, as we saw earlier, is an ideal).

In particular, this tells us that $\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ if m, n are relatively prime. We can therefore find a unique solution to a particular class of Diophantine equations.

As a corollary, considering the multiplicative groups of $\frac{\mathbb{Z}}{n\mathbb{Z}}$, we can prove that the totient of an integer is exactly the product of the totients of its prime power factors.

4 Ring Theory, Part 2: Classification of Integral Domains

In this chapter, we talk about Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains.

4.1 Euclidean Domains

We define a **norm** on an integral domain R. It is analogous to the idea of a norm on a vector space.

Definition: A function $f : R \to \mathbb{Z}$ so that $N(0) = 0$ is called a norm. If $N(a) > 0$ for $a \neq 0$, then it is called a positive norm.

Now, we can define the Euclidean algorithm (which finds a common divisor for two elements).

Definition: An integral domain R is a **Euclidean domain** if there exists a norm N so that for all nonzero $a, b \in R$, we can write:

$$a = qb + r$$

For some element q with $N(r) < N(b)$ or $r = 0$.

Proposition

> Every Euclidean domain is a principal ideal domain, i.e. each ideal can be generated by a single element. In particular, if we have a nonzero ideal I, then I is generated by d, any nonzero element of I with minimum norm.

This proof is fairly straightforward. Dividing any element by d leaves a remainder with a norm smaller than that of d. But this is impossible, so indeed d divides every element in the ring.

Definition: Let R be a commutative ring and let $a, b \neq 0$. A greatest common divisor d of a, b is an element such that $d \mid a, d \mid b$, and if any other element d' is a common divisor, then $d' \mid d$.

Indeed, the greatest common divisor (if it exists) is a generator for the unique principal ideal containing a, b. It is clear to see then, that if this divisor is a unit, then a, b generate a maximal ideal.

Proposition

> If a, b nonzero elements in a commutative ring R, and $(a, b) = (d)$ for some element d, then d is a greatest common divisor of a, b.

Furthermore, it is clear that greatest common divisors are unique up to units.

4.2 Principal Ideal Domains

Definition: A principal ideal domain is an integral domain in which every ideal is principal.

Note that by an earlier proposition, every Euclidean domain is a principal ideal domain. However, the converse is not true. The ideal $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a principal ideal domain but not a Euclidean domain.

Proposition

> Every nonzero prime ideal in a principal ideal domain is maximal.

This follows straightforwardly from the definitions.

Corollary

> If R is a commutative ring and $R[x]$ is a principal ideal domain, then R is a field.

Assume R is a PID. Then in particular, R is an integral domain. Therefore, since (x) is a nonzero prime ideal, (x) must be maximal. Therefore, R is a field. The converse is also true and is very important for field theory.

> If k is a field, the $k[x]$ is a PID.

This follows from the fact that $k[x]$ is a UFD, with the norm given by the degree of a given polynomial. The Euclidean algorithm works in $k[x]$.

4.3 Unique Factorization Domains

Definition: Let R be an integral domain. Suppose $r \in R$ and r is nonzero and not a unit. Then r is **irreducible** if whenever it is written as a product $r = ab$, then at least one of a or b must be a unit.

Definition: Suppose $p \in R$ is nonzero. Then p is **prime** if (p) is a prime ideal.

Definition: Two elements a, b are said to be associate in R if $a = ub$ for some unit u.

Proposition

In an integral domain, a prime element is irreducible.

Suppose we have a prime element $p = ab$. Then either $p \mid a$ or $p \mid b$. WLOG, let $p \mid a$. Then $a = px$ for some $x \in R$ and therefore $p = pxb$. But then we have $xb = 1$ and therefore b is a unit. Therefore p is irreducible.

However, the converse is not necessarily true! Look at the element 3 in $\mathbb{Z}[\sqrt{-5}]$, since 9 can be factored in the complex plane into terms not dividing 3.

Proposition

In a principal ideal domain, irreducible elements are prime.

Check that any ideal generated by an irreducible element is maximal. By an earlier theorem, a prime ideal is maximal in a PID (in general, a maximal ideal is always prime).

Definition: A unique factorization domain is an integral domain in which every nonzero element which is not a unit can be written as a finite product of irreducibles, and this decomposition is unique up to associates.

We also have the following useful fact:

Proposition

An element is irreducible iff the ideal it generates is maximal amongst the principal ideals.

So there is some correspondence between irreducible elements and maximal ideals, and between prime elements and prime ideals (far more obvious). It makes sense, then, that if all ideals are principal, then the two notions coincide.

Proposition

In a UFD, irreducible elements are prime.

So indeed, UFDs are also domains in which these two notions collapse. Finally, we get the following classification:

Proposition:

Every principal ideal domain is a unique factorization domain.

So finally, we have:

Fields $\subset$ Euclidean Domains $\subset$ Principal Ideal Domains $\subset$ UFDs $\subset$ Integral Domains

Each inclusion is proper.

- $\mathbb{Z}$ is a Euclidean domain but not a field.
- $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID but not a Euclidean domain.
- $\mathbb{Z}[x]$ is a UFD but not a PID.
- $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not a UFD.

5 Module Theory, Part 1: Introduction, Module Homomorphisms

Definition: Let R be a ring. A module M over a ring R is an abelian group (with operation $+$) and a map $R \times M \to M$ which satisfies distributivity and associativity. If R has a 1, then we require that $1m = m$ for each $m \in M$.

These axioms should look fairly familiar. if R is a field, then a module is exactly a vector space over R. A module is nothing more than a generalization of vector spaces.

Definition: A submodule is a closed subgroup N of an R-module M which is closed under the action of R.

Example A significant example is modules over $\mathbb{Z}$. The action of an integer on $m \in M$ is defined straightforwardly as:

$$nm = m + m + \cdots + m$$

Where we are adding m to itself n times. This is the only possible action of $\mathbb{Z}$ over M, because of associativity and distributivity. What we have from this is that:

$\mathbb{Z}$-modules are exactly abelian groups.

In particular, $\mathbb{Z}$-submodules are exactly submodules of subgroups.

Example By associativity, we can define a module over $F[x]$, where F is a field. We simply need to define how $1, x$ act on elements in the module. Let V be a vector space over F -- we will make V an $F[x]$ module, by identifying the action of x with a linear transformation $T : V \to V$.

Conversely, if we have any module V over $F[x]$, then in particular V is a module over F. But we know that:

$$x(v + w) = xv + xw$$
$$x(av) = ax(v)$$

So this means that indeed x is a linear transformation. So there is a natural isomorphism between vector spaces V over F equipped with a linear transformation T and modules V over $F[x]$.

Consequently, the $F[x]$-submodules of V are exactly vector subspaces of V which are invariant under T.

Proposition

A nonempty N of an R-module M is a submodule iff $x + ry \in N$ for each $x, y \in N$, $r \in R$.

Let $r = -1$ and we get the subgroup criterion. Let $x = 0$ and we get closure under elements of R. The converse case is fairly straightforward.

5.1 Quotient Modules and Module Homomorphisms

Definition: Let R be a ring and M, N are R-modules. Then an R-module homomorphism φ is a map from M to N so that:

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$
$$\varphi(rx) = r\varphi(x)$$

As expected, an isomorphism is surjective as well as injective. The kernel and images are respectively submodules of M, N as expected. Finally, we define $Hom_R(M, N)$ to be the set of all R-module homomorphisms from M to N.

For example, $\mathbb{Z}$-module homomorphisms are simply abelian group homomorphisms (since the second criterion is implied by the first above). Over a field, the F-module homomorphisms are simply linear transformations between vector spaces. Note, however, that R-module homomorphisms where R is a ring do not necessarily have any connection to ring homomorphisms -- specifically because there is no requirement that a module homomorphism send identity to identity.

Proposition

$Hom_R(M, N)$ is an R-module.

We can define addition and multiplication in the usual way:

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$
$$(r\varphi)(m) = r(\varphi(m))$$

Furthermore, if $M = N$ then we can have a well-defined ring structure; multiplication is just composition. Indeed, $Hom_R(M, M)$ is a ring with identity -- and indeed it has a special name.

Definition: The ring $Hom_R(M, M)$ is called the endomorphism ring of M and is denoted $End(M)$ or $End_R(M)$.

Proposition

Let R be a ring and let M, N be R-modules with N a submodule of M. Then M/N (an abelian quotient group) can be made into a module over R by defining:

$$r(x + N) = rx + N$$

And we have a natural projection map $\pi : M \to M/N$ with kernel N.

Finally, we define the sum of two modules:

$$A + B = \{a + b \ : \ a \in A, b \in B\}$$

So that we can once more define the isomorphism theorems.

Theorem (Isomorphism Theorems)

- Let M, N be R-modules and let $\varphi : M \to N$ be a module homomorphism. Then $M/(ker\varphi) \cong \varphi(M)$.
- Let A, B be submodules of R-module M. Then we have: $(A + B)/B \cong A/(A \cap B)$.
- Let M be an R-module and let A, B be submodules of M with $A \subset B$. Then $(M/A)/(B/A) \cong M/B$.
- Let N be a submodule of the R-module M. Then there is a bijection between submodules of M containing N and submodules of M/N given by $A \mapsto A/N$.

6 Module Theory, Part 2: Generation of Modules, Direct Sums, Free Modules

Definition: Let R be a ring with identity, and $N_1, \dots, N_n$ are modules over R. Then: - $N_1 + \cdots + N_n$ consists of all finite sums of elements $\{n_1 + \cdots + n_n\}$ so that $n_i \in N_i$. - For any subset A of M let $RA = \{r_1 a_1 + \cdots + r_n a_n\}$ so that $r_i \in R$, $a_i \in A$ and $m \in \mathbb{Z}$. By convention, if $A = \emptyset$ then we define $RA = \{0\}$. Indeed if $A = \{a_1, \dots, a_n\}$ then we can write $RA = Ra_1 + \cdots + Ra_n$ and say that RA is the **submodule generated by** A. - A submodule N of M is finitely generated if there is some finite subset A of M so that $N = RA$. - A submodule N is cyclic if $N = Ra$ for some element $a \in M$.

Note that if R has identity, then $RA = A$.

Examples

- For a $\mathbb{Z}$-module, modules generated by $A \subset M$ are just subgroups generated by A.
- A ring R with identity is a cyclic module generated by 1. Any submodule is an ideal. In particular, a submodule which is cyclic is exactly a principal ideal. In particular, a PID is just a (commutative) integral domain with identity so that every R-submodule of R is cyclic.
- Let F be a field and consider an $F[x]$ module V, which is identified with the action of x. Then to say that V is a cyclic $F[x]$-module is spanned by:

  $$\{v, T(v), T^2(v), \dots\}$$

  For some $v \in V$ as a vector space over F.

Definition: Let $M_1, \dots, M_k$ be a collection of R-modules. Then we define the direct product:

$$M_1 \times \cdots \times M_k$$

Which consists of all the k-tuples of the modules, and it is clearly also an R-module. With a finite number k, we say that the direct sum $M_1 \oplus \times \oplus M_k$ is their direct product.

Proposition

TFAE: - The map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ is defined by $\pi : (a_1, \ldots, a_k) \mapsto a_1 + \cdots + a_k$. π is an isomorphism. - $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \ldots N_k) = 0$ for any choice of j. - Every $x \in N_1 + \cdots + N_k$ can be written uniquely as $a_1 + \cdots + a_k$ for $a_i \in N_i$.

Definition: An R-module F is called free on the subset A of F if for every nonzero $x \in F$, there exist unique nonzero elements $r_1, \ldots, r_n \in R$ so that:

$$x = r_1 a_1 + \ldots r_n a_n$$

And in this case, we say that A is a **basis** or a set of generators for F. If R is a commutative ring, the size of A is called the rank of F.

An important distinction here is that r_i as well as a_i are unique, whereas in a direct sum only a_i are unique.

6.0.1 Theorem

For any set A there is a free R-module $F(A)$ on the set A. If M is *any* R-module and $\varphi : A \to M$ a set map, then there is a unique module homomorphism Φ so that the following diagram commutes (where j denotes the inclusion of A into $F(A)$).

When A is a finite set, we simply define $F(A) = Ra_1 \oplus \cdots \oplus Ra_n \cong R^n$ (if R has identity).

The proof is as follows. First, let $F(A) = \{0\}$ if $A = \emptyset$. Otherwise, let $F(A)$ be the set of all (set) functions $f : A \to R$ so that $f(a) = 0$ for all but finitely many a.

Indeed, we can see A as being included in $F(A)$ by constructing the function f_a such that $f_a(a) = 1$ and $f_a(b) = 0$ for all $b \neq a$. In this way, we can think of $F(A)$ as all (finite) linear combinations of elements of the form f_a which can be identified with the elements of A. And indeed $F(A)$ has a unique expression as such a formal sum. This is a module in the obvious way.

Now, suppose that $\varphi(A)$ is a map from the set A into an R-module M. Then we can define a map $\Phi : F(A) \to M$ by:

$$\varphi : \sum_{i=1}^{n} r_i a_i \mapsto \sum_{i=1}^{n} r_i \varphi(a_i)$$

Since elements of $F(A)$ have unique representations in this form, this map is well-defined. And by definition, restricting Φ to A yields exactly φ as a module homomorphism. And Φ is unique because it must respect the module homomorphism axioms.

When A is the finite set $\{a_1, \ldots, a_n\}$, then we have that $F(A) = Ra_1 \oplus \times \oplus Ra_n$. And indeed we can say that $R \cong Ra_i$ under the map $r \mapsto ra_i$. Therefore, the free R-module of a set of size n is simply R^n (in a sense, the ``simplest'' module).

Corollary

- If F_1, F_2 are free modules over A there is a unique isomorphism between them which is the identity on A.
- If F is any free R-module with basis A, then $F \cong F(A)$.

This is essentially the statement that universal objects are unique.

7 Representation Theory, Part 1: Introduction

Definition: A **representation** of a finite group G on a finite dimensional vector space V (WLOG the vector space is assumed to be over the complex numbers).

This map gives V the structure of a module over G, because for $g \in G$, we have:

$$g(v+w) = gv + gwg(hv) = (gh)v$$

Sometimes, V is itself called the representation of the group; thus, we identify a representation of a group as a vector space on which G acts linearly.

Definition: A map φ between two representations V, W of G (also called a G-linear map) is a vector space map $\varphi : V \to W$ such that for any $g \in G$ and $v \in V$:

$$g\varphi(v) = \varphi(gv)$$

Definition: A **subrepresentation** of a representation V is a vector subpace of W of V which is invariant under G.

Definition: A representation V is called **irreducible** if there is no proper nonzero invariant subspace W of V.

Given two represetnations, the direct sum $V \oplus W$ and the tensor product $V \otimes W$ are also representations. The latter is given by:

$$g(v \otimes w) = gv \otimes gw$$

Similarly, the nth tensor power can be constructed from a representation, and similarly the exterior powers and symmetric powers as subrepresentations.

7.1 Duals and Tensor Products of Representations; Representation of $Hom(V, W)$

The dual V^* of a vector space is a representation as well. We wish to respect the natural pairing between V^* and V, given by:

$$\langle v^*, v\rangle = v^*(v)$$

So we need to define the dual representation such that:

$$\langle \rho^*(g)v^*, \rho(g)v\rangle = \langle v^*, v\rangle$$

And this forces us to define the representation as follows. Note that by the definition of the transpose:

$$\rho(g^{-1})^T v^*(gv) = v^*(g^{-1}gv) = v^*(v)$$

So we define:

$$\rho^*(g) = \rho(g^{-1})^T : V^* \to V^*$$

Now that we have defined the dual and the tensor product of representations, we can show that $Hom(V, W)$ is a representation. Note that there is a natural identification:

$$V^* \otimes W \to Hom(V, W) a^* \otimes b \to (v \mapsto a^*(v)b)$$

It is not hard to show that this identification is surjective and injective, and hence an isomorphism of vector spaces. Now, we take an arbitrary element $a^* \otimes b \in V^* \otimes W$. We identify this element naturally with $\varphi \in Hom(V, W)$:

$$\varphi : v \mapsto a^*(v)b$$

Now we consider $g\varphi = g(a^* \otimes b)$. We have:

$$g(a^* \otimes b) = ga^* \otimes gb = (g^{-1})^T a^* \otimes gb$$

Where we have used the definition of the dual representation. By the natural identification again we have:

$$g\varphi : v \mapsto (g^{-1})^T a^*(v) gb = ga^*(g^{-1}v)b$$

But this is simply telling us that:

$$(g\varphi)(v) = g\varphi(g^{-1}v)$$

And this gives us the representation of the space $Hom(V, W)$.

Proposition 1

The vector space of G-linear maps between two representations V, W of G is the subspace of $Hom(V, W)$ which is fixed by G, often denoted $Hom_G(V, W)$

Note that if we have a G-linear map φ, then by definition:

$$g\varphi(v) = \varphi(gv)$$

Note that the representation of $Hom(V, W)$ however is given by:

$$(g\varphi)(v) = g\varphi(g^{-1}v) = \varphi(gg^{-1}v) = \varphi(v)$$

So indeed φ is fixed under the action of G. The converse holds evidently as well; if φ is fixed by G, then it follows that φ is G-linear.

Finally, if X is any finite set and G acts on X, then G naturally is embedded into the permutation group $Aut(X)$ of X. So we can construct a vector space with basis $e_x \ : \ x \in X$ and the action of G is then given by:

$$g \sum a_x e_x = \sum a_x e_{gx}$$

Definition: The **regular representation** R_G or R corresponds to the action of G on itself. We could alternatively define it as the space of complex-valued functions on G where:

$$(g\alpha)(h) = \alpha(g^{-1}h)$$

To prove that these are equivalent, we identify e_x with the function f_x which takes the value 1 on x and 0 elsewhere. Then we have:

$$(gf_x)(h) = f_x(g^{-1}h)$$

And evidently this function takes value 1 where $g^{-1}h = x$ or equivalently $h = gx$. Thus we can write:

$$(gf_x) = f_{gx}$$

7.2 Complete Reducibility; Schur's Lemma

Proposition 2 (Maschke's Theorem)

If W is a subrepresentation of a representation V of a finite group G, then there is a complementary invariant subspace W' of V, so that $V = W \oplus W'$

We define the complement as follows. Chose an arbitary subspace U which is complementary to W. Then we can write:

$$V \cong W \oplus U$$

So for any $v \in V$, we can identify it with some pair (w, u). Define the natural projection map $\pi_0 : V \mapsto W$ as:

$$\pi_0(w, u) = w$$

This map is G-linear. Then, we define a new map π:

$$\pi(v) = \sum_{g \in G} g\pi_0(g^{-1}v)$$

Since π_0 is G-linear, it follows that this map is G linear. In fact on W, we have:

$$\pi(w) = \sum_{g \in G} g\pi_0(g^{-1}w) = \sum_{g \in G} gg^{-1}\pi_0(w) = |G|w$$

So this map is nothing more than multiplication by $\|G\|$ on W. Therefore, its kernel is a subspace of V which is invariant under G and is complementary to W.

Corollary

Any representation is a direct sum of irreducible representations.

Now we move on to Schur's Lemma, one of the more useful theorems in basic representation theory.

Proposition 3 (Schur's Lemma)

If V, W are irreducible representations of G and $\varphi : V \to W$ is a G-module homomorphism, then: - Either φ is an isomorphism, of $\varphi = 0$. - If $V = W$, then $\varphi = \lambda I$ for some $\lambda \in \mathbb{C}$.

The first claim follows from the fact that if φ is a module homomorphism, then its kernel and image are subspaces of V, W respectively. Furthermore, for $v \in \ker \varphi$:

$$\varphi(gv) = g\varphi(v) = 0$$

So that the kernel is invariant under G. Similarly, for $\varphi(v)$ in the image we have:

$$g\varphi(v) = \varphi(gv)$$

And so $g\varphi(v)$ also lies in the image. Thus, we have shown the kernel and image of φ are subrepresentations of V and W respectively. The only possibilities are that the kernel is trivial and the image is W (yielding an isomorphism), or the kernel is V and the image is trivial (i.e. $\varphi = 0$).

To prove the second claim, φ must have an eigenvalue λ so that $\varphi - \lambda I$ has nonzero kernel. But if the kernel is nonzero, then by the above argument, the kernel is the V. So identically we indeed have:

$$\varphi - \lambda I = 0$$

Proposition 4

> For any representation V of a finite group G, there is a decomposition:
>
> $$V = V_1^{\oplus a_1} \oplus \cdots \oplus V_k^{\oplus a_k}$$
>
> Where V_i are distinct irreducible representations. The decomposition is furthermore unique.

This is a straightforward consequence of Schur's Lemma. Occasionally this decomposition is written:

$$V = a_1V_1 \oplus \cdots \oplus a_kV_k = a_1V_1 + \cdots + a_kV_k$$

Where the a_i denote multiplicities.

7.3 Examples: Abelian Groups; S_3

In general,if V is a repreentation of a finite group G, then each $g \in G$ gives a map $\rho(g) : V \to V$. However, in general, this map is not a G-module homomorphism (G-linear), i.e. in general we do not have:

$$g(h(v)) = h(g(v))$$

Indeed, $\rho(g)$ is G-linear for every ρ iff g is in $Z(G)$. Then g commutes with h and the above holds. In particular if G is abelian, the above holds. But if V is an irreducible

representation, by Schur's Lemma each $g \in G$ acts on V by a scalar multiple, so every subspace is invariant. Thus, V is one dimensional.

Therefore, the irreducible representations of an abelian group G correspond to homomorphisms:

$$\rho : G \to \mathbb{C}$$

Next, we look at S_3. There are two one dimensional representations, given by the trivial representation (U) and the alternating representation U' given by:

$$gv = \text{sgn}(g)v$$

Naturally, we ask if there are any others. Since G is a permutation group, it has a natural permutation representation, where it acts on $\mathbb{C}^3$ by permuting the basis vectors. The representation is not irreducible since it has the invariant subspace spanned by $(1, 1, 1)$. The complementary subspace is given by:

$$V = \{(z_1, z_2, z_3) \ : \ z_1 + z_2 + z_3 = 0\}$$

And this is irreducible since it has no invariant subspaces. It is called the standard representation.

In general, we take a representaiton W of S_3 and look at the action of the abelian subgroup $\mathbb{Z}/3$ on W. If τ is a generator of this subgroup (a 3-cycle), then the space W is spanned by eigenvectors for the action of τ. Furthermore, since $\tau^3 = 1$, the eigenvalues are all third roots of unity. We write $\tau(v) = \omega^i v$ where ω^i is one of the roots of unity.

Let σ be a transposition in S_3. Then we have the relation:

$$\sigma\tau\sigma = \tau^2$$

So therefore we can write:

$$\begin{aligned} \tau(\sigma(v)) &= \sigma(\tau^2(v)) \\ &= \sigma(\omega^{2i}v) \\ &= \omega^{2i}\sigma(v) \end{aligned}$$

So if v is an eigenvector for τ with eigenvalue ω^i, then $\sigma(v)$ is an eigenvector for τ with eigenvalue ω^{2i}.

If v is an eigenvector of τ with eigenvalue $\omega^i \neq 1$, then $\sigma(v)$ is an eigenvector with a different eigenvalue and hence independent. Thus, $v, \sigma(v)$ span a two dimensional subspace of W which is invariant under S_3.

On the other hand, if $w^i = 1$, then $\sigma(v)$ may or may not be linearly independent to v. If it is not, then v spans a one-dimensional subrepresentation, isomorphic to the trivial representation if $\sigma(v) = v$ and the alternating representation if $\sigma(v) = -v$. If $\sigma(v)$ and v are linearly independent, then $v+\sigma(v)$ and $v-\sigma(v)$ span one dimensional represnetations of W isomorphic to the trivial and alternating representations, respectively.

This is not the best approach to find the decomposition of any representation of S_3, but it is one way to do it.

8 Representation Theory, Part 2: Character Theory

Note that in S_3 the eigenvalues of the group elements completely determined the representation. If the eigenvalue was -1, it was the alternating representation; 1, the trivial representation; and finally ω, ω^2 correspond to the standard representation.

Note that if you know the eigenvalues λ_i of g, then you know the eigenvalues of $g^k = \lambda_i^k$ since the matrix is diagonal in some basis. Similarly, suppose that we know the sums $\sum \lambda_i^k$ for each k. Then this tells us everything about the eigenvalues.

For example, note that:

$$\left(\sum \lambda_i\right)^2 = \sum \lambda_i^2 + 2\sum_{i \leq j} \lambda_i \lambda_j$$

Now, suppose that the representation has dimension 2. Then the latter term on the right hand side is the middle term in the characteristic polynomial for g. The final term is the determinant of g. So with this information, we can solve for the eigenvalues of g.

Definition: The character of a representation is:

$$\chi_V(g) = \mathsf{tr}(g|_V)$$

This is a class function, i.e. χ_V is constant within a conjugacy class, since similar matrices have the same trace.

8.1 Properties of Characters

The following give us a useful way to compute combinations of representations.

$$\begin{aligned} \chi_{V \oplus W} &= \chi_V + \chi_W \\ \chi_{V \otimes W} &= \chi_V \cdot \chi_W \\ \chi_{V^*} &= \chi_V(g^{-1}) = \overline{\chi_V(g)} \end{aligned}$$

The last property follows from the fact that the eigenvalues of g are all roots of unity.

Proposition 1 (The Original Fixed Point Formula)

> If V is the permutation representation of G acting on a finite set X, then $\chi_V(g)$ is the number of elements fixed by g.

To prove this, consider that each orbit is a subspace of V which is fixed under G, hence a subrepresentation. And with respect to the natural basis, the matrix has trace 0, unless the matrix is simply 1×1, in which case it has trace 1. Therefore, the trace of g is the number of fixed points.

8.2 Character Tables

A character table has conjugacy classes (with sizes above them) labeling the columns. The rows are labelled by irreducible representations. In the appropriate box is the character of a conjugacy class representative in the given representation.

Character Table for S_3 So far, the table looks like:

| |1 | 3 | 2 | | S_3 |1 | (12) | (123) | |-------|--------|---------|---------| |U (trivial) | 1| 1 | 1 | |U' (alt.) | 1| -1 | 1 |

To find the remaining row, we first note that the permutation representation is given by $(3, 1, 0)$ by the fixed point formula. However, the permutation representation is the direct sum of $U \oplus V$, where V is the standard representation. So using this information, we solve for V to obtain:

| |1 | 3 | 2 | | S_3 |1 | (12) | (123) | |-------|--------|---------|---------| |U (trivial) | 1| 1 | 1 | |U' (alt.) | 1| -1 | 1 | |V (std.) | 2| 0 | -1 |

8.3 The First Projection Formula

Definition: The elements of a representation V which are fixed by each $g \in G$ is denoted V^G.

Proposition 2

> The following map projections V onto V^G:

$$\varphi(v) = \frac{1}{|G|} \sum_{g \in G} gv$$

Furthermore, this map is G-linear and projects onto V^G. In particular, each element of V^G spans a one-dimensional trivial representation. So with a given representation, we can find the multiplicity m of the trivial representation by noting that:

$$m = \dim V^G = \text{tr}(\varphi) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)$$

In particular, if V is irreducible and non-trivial, then this sum is zero.

Note also that:

$$Hom(V, W)^G = \{G\text{-module homomorphisms from } V \text{ to } W\}$$

So if V is irreducible, then by Schur's Lemma, each element of $Hom(V, W)$ is either a direct sum of isomorphisms or else 0. So in particular, dim $Hom(V, W)^G$ is the multiplicity of V in W.

If both V, W are irreducible, then:

$$\dim Hom_G(V, W) = \begin{cases} 1 & V \cong W \\ 0 & V \ncong W \end{cases}$$

Now, note that $Hom(V, W)) = V^* \otimes W$, so that:

$$\chi_{Hom(V,W)}(g) = \overline{\chi_V(g)} \cdot \chi_W(g)$$

Now now, note that by Proposition 2, we have:

$$\dim Hom(V, W)^G = \frac{1}{|G|} \sum \chi_{Hom(V,W)}(g) = \frac{1}{|G|} \sum = \overline{\chi_V(g)} \cdot \chi_W(g)$$

This naturally lets us define the following inner product on class functions on G.

$$(\alpha, \beta) = \frac{1}{|G|} \sum \overline{\alpha(g)} \beta(g)$$

And according to this basis, we have just proved the following theorem.

Theorem (Schur Orthogonality 1)

The characters of irreducible representations of G are orthonormal.

Corollary

The number of irreducible representations is at most the number of conjugacy classes.

To see this, note that the dimension of the space of class functions is at most the number of conjugacy classes, and that irreducible representations correspond to irreducible characters, which are orthonormal.

Note also that if we have as a decomposition into irreducible representations:

$$V = a_1 V_1 \oplus \cdots \oplus a_n V_n$$

Then the character is given by:

$$\chi_V = a_1 \chi(V_1) + \cdots + a_n \chi(V_n)$$

Proposition 3 (Projection Formula) And in particular, since irreducible characters are orthonormal the inner product is given by:

$$(\chi_V, \chi_V) = \sum a_i^2$$

And finally, $(\chi_V, \chi_V) = 1$ iff V is irreducible. Similarly, we can write:

$$a_i = (\chi_V, \chi_{V_i})$$

8.4 Character of the Regular Representation

Let the regular representation be R. Really G is acting on itself by left multiplication, so the fixed point formula gives us:

$$\chi_R(g) = \begin{cases} 0 & g \neq e \\ |G| & g = e \end{cases}$$

So R is not irreducible so long as $G \neq \{e\}$. In particular, to get the ith coefficient of the regular representation, we can write:

$$a_i = (\chi_{V_i}, \chi_R) = \frac{1}{|G|} \chi_{V_i}(e) \chi_R(e) = \dim V_i$$

Corollary

Each irreducible representation V_i of G appears in the regular representation $\dim V_i$ times.

Note however that:

$$\chi_R(e) = |G| = \sum a_i \dim(V_i) = \sum \dim(V_i)^2$$

And taking the character of any other element g

$$0 = \sum a_i \chi_{V_i}(g) = \sum \dim V_i \cdot \chi_{V_i}(g)$$

Theorem (Schur Orthogonality 2)

The columns of a character table are also orthogonal.

This follows from matrix multiplication. In particular, for $g \in G$:

$$\sum_{\chi} \overline{\chi(g)}\chi(g) = \frac{|G|}{c(g)}$$

Where $c(g)$ is the size of the conjugacy class of g.

8.5 Abelian Subgroups and Products of Groups

Proposition 4

Let $A \leq G$ be an abelian subgroup. Then each irreducible representation of G has degree at most $[G : A]$.

Suppose that we have an irreducible representation V of G. Then we can restrict the representation to A to obtain a representation of A.

Let $W \subseteq V$ be an irreducible subrepresentation of A. Since A is abelian, $\dim W = 1$ and it is spanned by some vector w. So we define:

$$V' = \{gw \ : \ g \in G\}$$

More precisely, we take the span of the orbit of w under G. Evidently, V' is stable under the action of G, and therefore is a subrepresentation of V. But V is irreducible, so $V' = V$. In particular we have for any $g \in G$, and $a \in A$:

$$ga(w) = g(\lambda w) = \lambda g w$$

For some $\lambda \in \mathbb{C}$. So the number of linearly independent elements gw is at most $[G : A]$, and the span of the orbit of w is exactly $V' = V$.

Proposition 5

> Suppose we have a product of groups $G_1 \times G_2$. Then if we have two irreducible representations V, W of G_1, G_2 respectively, then $V \otimes W$ is an irreducible representation of $G_1 \times G_2$.

We can prove this by simply noting that:

$$\frac{1}{|G_1|}\sum |\chi_V(a)|^2 = \frac{1}{|G_2|}\sum |\chi_W(b)|^2 = 1$$

And since the character of a tensor product is the product of characters we get:

$$\frac{1}{|G_1||G_2|}\sum\sum |\chi_V(a)|^2|\chi_W(b)|^2 = 1 \cdot 1 = 1$$

And so indeed the tensor product representation is irreducible.

Proposition 6

> Each irreducible representation of $G_1 \times G_2$ is of the form $V \otimes W$ for some V irreducible representation of G_1 and W irreducible representation of G_2.

Let f be a class function on $G_1 \times G_2$ which is orthogonal to each $V \otimes W$, where V, W irreducible in G_1, G_2 respectively. Note that since multiplication is defined componentwise we have:

$$(g, h)(a, b)(g^{-1}, h^{-}1) = (gag^{-1}, hah^{-1})$$

We consider the inner product of f with χ_V and χ_W. We have:

$$\sum_{a,b} f(a, b)\chi_V(a)^*\chi_W(b)^* = 0$$

Now fix:

$$g(a) = \sum_b f(a, b)\chi_V(a)^*$$

Let $h \in G_1$. Then we have:

$$g(hah^{-1}) = \sum_b f(hah^{-1}, b)\chi_W(b)^*$$

But:

$$(hah^{-1}, b) = (h, 1)(a, b)(h, 1)^{-1}$$

And f is a class function, so indeed we get:

$$g(hah^{-1}) = g(a)$$

So g is a class function on G_1. However we have for irreducible character χ_V on G_1:

$$\sum_a g(a)\chi_V(a)^*$$

And so $g = 0$ identically. We can argue similarly to complete the proof and say that $f(a, b)$ is identically zero.

9 Field Theory, Part 1: Introduction, Algebraic Extensions

9.1 Introduction

Recall that a field is a commutative ring in which every nonzero element has a multiplicative inverse.

Definition: The **characteristic** of a field is the additive order of 1. For example, if $1+1+1=0$, then we say the field has characteristic 3. If $1+1+\ldots$ is never equal to 0, we say the field has characteristic 0. The characteristic of a field is either 0 or a prime.

Denote $1+1+\cdots+1$, added n times, we denote this element $n \cdot 1$. For each field F, we have a natural homomorphism $\mathbb{Z} \to F$, which maps n to $n \cdot 1$. Note that a homomomorphism into a field is either zero identically or an isomorphism; thus the image of this map can be realized as a subfield of F.

The kernel of this homomorphism is exactly $(\text{char}F)\mathbb{Z}$. By the isomorphism theorems, then, F contains either a subring isomorphic to $\mathbb{Z}$ (in which case F contains $\mathbb{Q}$) or else F contains a subring isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (in which case $\mathbb{F}_p$, the finite field of p elements, is a subfield).

Definition: The prime subfield of a field F is the subfield generated by 1 additively. It is either $\mathbb{Q}$ or $\mathbb{F}_p$, the finite field of p elements.

Definition: If K is a field containing a subfield F, then K is an extension of F. The prime subfield is called the base field of an extension.

Definition: The degree of K/F, the extension K over F, is the dimension of K as a vector space over F.

Definition: Let K be an extension of F. Then for $\alpha \in K$, $F(\alpha)$ denotes the smallest subfield of K which contains F and α. This is called a simple extension of F; a simple extension is not, in general, simply an extension of degree 2 over F.

Theorem 1

> Let F be a field and $p(x) \in F[x]$ an irreducible polynomial. Then there exists a field K containing F such that $p(x)$ has a root.

We can prove this by considering the field:

$$K = \frac{F[x]}{(p(x))}$$

Since p is irreducible, and $F[x]$ is a PID, p spans a maximal ideal, and thus K is indeed a field. Furthermore, we have the canonical projection:

$$\pi : F[x] \to K$$

When restricted to F, this map is an isomorphism. Since it sends 1 to 1, it is an isomorphism and therefore an image of F lies in K. Thus, since π is a homomorphism, denoting the image in the quotient with a bar, we have:

$$\overline{p(x)} = p(\overline{x}) = 0$$

And thus, $\bar{x}$ is a root of p. In particular, let:

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

Then if $\theta = \bar{x}$, then the above proof gives us a basis for K:

$$1, \theta, \ldots, \theta^{n-1}$$

And thus, $[K : F] = n$, i.e. K is a vector space over F of dimension n. It remains to check that this is indeed a basis, i.e. that it is linearly independent; this follows from the fact that p is irreducible.

Theorem 2

> Let F be a field and $p(x) \in F[x]$ an irreducible polynomial. Suppose that K is an extension of F containing a root α of $p(x)$ such that $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then:
>
> $$F(\alpha) \cong \frac{F[x]}{(p(x))}$$
>
> This theorem tells us that any field over F in which $p(x)$ contains a root contains a subfield isomorphic to the extension we considered in Theorem 1. The natural homomorphism that allows us to prove this identity is:
>
> $$\varphi : F[x] \to F(\alpha) \subseteq K f(x) \mapsto f(\alpha)$$

This homomorphism is exactly evaluation. With some work, we can prove that this is a nontrivial ring homomorphism; thus the quotient ring is indeed a field.

Indeed, we can totally describe $F(\alpha)$ using this theorem:

Corollary

Suppose that $p(x)$ has degree n. Then:

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\} \subseteq K$$

Where $a_i \in F$.

Describing the fields which are generated by more than element is a little more complicated.

Note that Theorem 2 tells us that the roots of an irreducible polynomial are, in a sense, indistinguishable; adjoining any root of an irreducible polynomial yields an isomorphic field. We extend this result.

Theorem 3

Let $\varphi : F \to \tilde{F}$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) = \varphi(p(x))$ (we simply map each coefficient under φ). Then $p'(x)$ is irreducible.

Let α be a root of $p(x)$ and β be a root of $p'(x)$ in some extension of F'. Then there is an isomorphism:

$$\sigma : F(\alpha) \to F'(\beta)$$

$$\sigma : a \mapsto \beta$$

And such that σ restricted to F is exactly φ.

Thus, we can extend any isomorphism of fields to an isomorphism of simple extensions which maps roots to roots. In particular, if $F = F'$ and φ is the identity, then this tells us that $F(\alpha) \cong F(\beta)$, where β is another root of $p(x)$. This will be vital to understanding Galois theory.

Theorem 4 (Eisenstein's Criterion)

Suppose that we have a polymial in $\mathbb{Q}[x]$ given by:

$$a_n x^n + \cdots + a_1 x + a_0$$

Then if there exists a prime p such that: - $p \mid a_i$ for each $i \neq n$ - $p \nmid a_n$ - $p^2 \nmid a_0$
Then, this polynomial is irreducible over $\mathbb{Q}$ and equivalently over $\mathbb{Z}$.

9.2 Algebraic Extensions

Definition: The element $\alpha \in K$ is said to be **algebraic** over F if α is a root of some nonzero polynomial with coefficients in F. Otherwise, α is said to be transcendental over F. The extension K/F is algebraic if every element of K is algebraic over F.

From the Euclidean algorithm, we get:

Definition: Let α be algebraic over F. Then there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. This polynomial is called the **minimal polynomial** of α and we say the degree of α is the degree of this polynomial.

Proposition 1

Let α be algebraic over F, and let $F(\alpha)$ be the field generated by α over F.
Then:

$$F(\alpha) \cong \frac{F[x]}{(m_\alpha(x))}$$

This proves that in particular:

$$[F(\alpha) : F] = \deg \alpha$$

Thus, the degree of a simple extension is exactly the degree of the minimal polynomial, and we have an explicit way of computing simple extensons corresponding to algebraic elements.

Proposition 2

The element α is algebraic over F iff the simple extension $F(\alpha)/F$ is finite.

This tells us that the property that α is algebraic over F is equivalent to the property that $[F(\alpha) : F]$ is finite. In particular, we have the corollary:

Proposition 3

If an extension K/F is finite, then it is algebraic.

A simple algebraic extension is finite, but in general the converse is not true, since there are infinite algebraic extensions.

Example Let F be a field of characteristic 2, and K an extension of degree 2 (called a quadratic extension). Let $\alpha \in K$ be an element not in F. It must be algebraic. Its minimal polynomial cannot be degree 1 (since $\alpha \notin F$); and so it is quadratic. It looks like:

$$m_\alpha(x) = x^2 + bx + c$$

For some $b, c \in F$. Furthermore, $K = F(\alpha)$. The roots are given by:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

And $b^2 - 4c$ is not a square in F, since if it were then $\alpha \in F$.

Now, $F(\alpha) \subset F(\sqrt{b^2 - 4c})$ since α is an element of the field on the right. Conversely, $\sqrt{b^2 - 4c} = \pm(b + 2\alpha)$ so we have the reverse inclusion.

We have just shown that any quadratic extension is of the form $F(\sqrt{D})$ where D is an element of F which is not a square in F; conversely, every such extension has degree 2.

Theorem 5

Let $F \subseteq K \subseteq L$ be fields. Then:

$$[L : F] = [L : K][K : F]$$

This is an analogous theorem to the one for groups; indeed this connection is deeper than it appears.

Corollary

Suppose L/F finite extension, and K a subfield of L containing F. Then $[K : F]$ divides $[L : F]$.

Definition: An extension K/F is **finitely generated** if there are element $\alpha_1, \ldots, \alpha_k$ in K such that:

$$K = F(\alpha_1, \ldots, \alpha_k)$$

As expected, we can obtain this field by recursively compounding a series of simple extensions, i.e.:

$$(F(\alpha))(\beta) = F(\alpha, \beta)$$

Where $F(\alpha, \beta)$ is the smallest field containing F, α, and β.

Theorem 6

> The extension K/F is finite iff K is generated by a finite number of algebraic elements over F. If these elements have degrees $n_1, \ldots, n_k$ then, K is algebraic of degree at most $n_1 n_2 \ldots n_k$.

To see this, notice that if K/F is finite of degree n, then say $\alpha_1, \ldots, \alpha_n$ is a basis for K as a vector space over F. Then:

$$[F(\alpha_i) : F] \mid [K : F] = n$$

Therefore, by Proposition 2 each α_i is algebraic. Conversely, if K is generated by a finite number of algebraic elements, then it is generated as a vector space by polynomials of those elements.

Corollary

> Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F forms a subfield K of L.

Suppose that α, β are algebraic over F. Then, note that $\alpha \pm \beta, \alpha\beta, \alpha/\beta, \alpha^{-1}$ are all algebraic, and lie in the finite extension $F(\alpha, \beta)$; and since this extension is finite, these elements are algebraic. Thus, the collection of algebraic elements is closed under addition, multiplication, and inverses.

Theorem 7

> If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

We also ask about ``intersections'' of fields.

Definition: Let K_1, K_2 be subfields of K. The composite field of K_1, K_2, denoted $K_1 K_2$, is the smallest subfield of K containing both K_1, K_2. It is equivalently the intersection of all subfields of K containing both K_1 and K_2.

Indeed, if K_1, K_2 are finite extensions, then if we combine their bases, we can construct a set of generators for K_1K_2. From this discussion, we can see:

Proposition 4

Let K_1, K_2 be two finite extensions of a field F contained in K. Then:

$$[K_1K_2 : F] \leq [K_1 : F][K2 : F]$$

Corollary

Suppose that $[K_1 : F] = n$, and $[K_2 : F] = m$, then if n, m are relatively prime then:

$$[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$$

10 Field Theory, Part 2: Splitting Fields, Algebraic Closure

10.1 Splitting Fields

As we saw, if $f(x)$ is any polynomial in $F[x]$, then there exists an extension K of F in which $f(x)$ has a root α. Equivalently, f has a factor $x - \alpha$ in $K[x]$. This motivates the following definition.

Definition: An extension K of F is called a **splitting field** for the polynomial $f(x) \in F[x]$ if f factors completely into linear factors in $K[x]$, but does not factor completely over any proper subfield of K containing F.

Theorem 1

For any field F and $f(x) \in F[x]$, there exists a splitting field for $f(x)$.

We proceed by induction on the degree n of f. If $n = 1$, $E = F$ is a splitting field.

If not, then f either splits completely ($E = F$ again), or else it has a reducible factor $p(x)$ of degree at least 2. In Part 1, we showed there is an extension E_1 of F containing a root α of $p(x)$. Thus, in E_1, $f(x)$ has an irreducible factor of degree at most $n - 1$.

By induction, there exists an extension E of E_1 containing all the roots of $f(x)$ other than α. Since $\alpha \in E_1 \subseteq E$, E is an extension of F in which $f(x)$ splits completely. Now, let K be the intersection of all subfields of E which contain F and also all the roots of $f(x)$; K is the splitting field.

We use the terminology ``the'' splitting field; indeed we shall show it is unique.

Definition: If K is an algebraic extension of F which is a splitting field over F for a collection of polynomials in $F[x]$, then K is called a **normal extension** of F.

``Splitting field'' and ``normal extension'' are used more or less interchangeably.

Proposition 1

A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F

We can adjoin one root of $f(x)$ to generate an extension of degree at most n (equal iff f is irreducible). Over this field, $f(x)$ has at least one linear factor. Thus, adjoining another root yields an extension of degree at most $n-1$. By the multiplicativity of extension degrees, the result follows.

Example: Cyclotomic Fields An important example that will be studied later is that of a **cyclotomic field**. We consider the splitting field of the polynomial:

$$x^n - 1$$

Over $\mathbb{Q}$. The roots are called the nth roots of unity. With multiplication, they form a cyclic group; indeed this group is precisely $\mathbb{Z}/n\mathbb{Z}$.

Definition: A **primitive** nth root of unity is a generator for the cyclic group of all nth roots of unity

We use ζ_n to denote a primitive nth root of unity. Evidently, ζ_n^a is also a primitive root, if a is relatively prime to n.

Since ζ_n generates this entire group, $x^n - 1$ splits completely over the field $\mathbb{Q}(\zeta_n)$.

Definition: The field $\mathbb{Q}(\zeta_n)$ is called the **cyclotomic field** of nth roots of unity.

A particular case is when $n = p$ is prime. Then the factorizatino is given by:

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$$

And the latter term (denoted Φ_p) is irreducible, which follows from substituting in $(x+1)$ for x and using Eisenstein's Criterion. Thus, we have that Φ_p is the minimal polynomial of ζ_p over the rationals, so that:

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

Next, we show that indeed the splitting field is unique.

Theorem 2

> Let $\varphi : F \to F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ and denote its image under φ as $f'(x)$ (obtained by applying φ to the coefficients).
>
> Let E be a splitting field for $f(x)$ over F; let E' be a splitting field for $f'(x)$ over F'. Then we can extend φ to an isomorphism $\sigma : E \to E'$.

We proceed by induction on n, the degree of $f(x)$. If $f(x)$ splits completely in F, then $f'(x)$ splits completely in F', and we are done.

Now, assume that $p(x)$ is an irreducible factor of $f(x)$ which has degree at least 2. Let $p'(x)$ be the image in $F'(x)$. Then if $\alpha \in E$ is a root of $p(x)$ and $\beta \in E'$ is a root of $p'(x)$, then by Part 1 Theorem 3, we can extend φ to an isomorphism σ':

$$\sigma' : F(\alpha) \to F'(\beta) \sigma' : \alpha \mapsto \beta$$

Denote $F_1 = F(\alpha)$ and $F_1' = F'(\beta)$; we have just constructed an isomorphism of fields $\sigma' : F_1 \to F_1'$. Over F_1, we can write:

$$f(x) = (x - \alpha) f_1(x) f'(x) = (x - \beta) f_1'(x)$$

Where each of f_1, f_1' has degree $n - 1$.

Notice that E is a splitting field for f_1 over F_1; if f_1 splits in any subfield, then we have found a subfield of E in which $f(x)$ splits. Similarly, E' is a splitting for f_1' over F_1'.

Thus, since f_1, f_1' have degree $n - 1$, by induction there is a map $\sigma : E \to E'$ which extends the isomorphism $\sigma' : F_1 \to F_1'$.

Thus, we have shown that σ extends σ' which in turn extends φ; thus we have extended an isomorphism of fields to an isomorphism of splitting fields.

Corollary

Any two splitting fields for $f(x) \in F[x]$ over F are isomorphic.

Take the proof above and let φ be the identity from F to itself.

Now that we have looked at field extensions of F which contains the root of a particular polynomial of degree n over F (which necessarily exist and have degree at most $n!$), we ask the question of whether there is an extension of F which contains the roots of all polynomials over F. As you might expect, there are going to be some Zorn's Lemma shenanigans.

Definition: $\overline{F}$ is called an algebraic closure of F if $\overline{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$.

Thus, in a way $\overline{F}$ contains all the elements which are algebraic over F.

Definition: A field K is said to be algebraically closed if every polynomials with coefficients in K has a root in K.

We'd better hope that algebraically closed fields exist (the complex numbers should be one). We also should hope that algebraic closures exist for arbitrary fields. Finally, one should expect that an algebraic closure is itself algebraically closed.

Proposition 2

Let $\overline{F}$ be an alegbraic closure of F. Then $\overline{F}$ is algebraically closed.

Let $f(x)$ be a polynomial in $\overline{F}[x]$ with a root α. Then α generates an algebraic extension $\overline{F}(\alpha)$ of F. However, since $\overline{F}(\alpha)/\overline{F}$ is algebraic, and $\overline{F}/F$ is algebraic, $\overline{F}(\alpha)/F$ is algebraic. But then $\alpha \in \overline{F}$, since α is algebraic over F, so that $\overline{F}$ is algebraically closed.

Proposition 3

For a field F there exists an algebraically closed field K which contains F.

This proof is not too enlightening; continue at your own risk.

For each non-constant monic polynomial f with coefficients in F, we associate an indeterminate x_f. Let S denote the set of all such indeterminates; it is in bijection with the set of polynomials in $F[x]$ with degree at least 1.

$$F[S] = F[\dots, x_f, \dots]$$

In this polynomial ring, consider the ideal I generated by the polynomials $f(x_f)$. We claim that this is a proper ideal.

If the ideal is not proper, then in particular 1 is an element. So there exists a finite linear combination:

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) = 1$$

Where each $g_i \in F[S]$. For convenience, we denote x_i instead of x_{f_i}. Finally, let $x_{n+1}, \dots x_m$ denote the remaining letters occuring in the polynomials g_i. We can rewrite the above relation:

$$g_1(x_1, \dots x_m) f_1(x_1) + \cdots + g_n(x_1, \dots, x_m) f_n(x_n) = 1$$

Now, let F' be a (finite) extension of F which contains a root α_i of each $f_i(x)$. Then if we let $x_i = \alpha_i$ and set $x_{n+1} = \cdots = x_m = 0$, then the equation above reads $0 = 1$, which is impossible. Thus, the ideal above must be proper.

Since I is a proper ideal, it is contained in some maximal ideal $\mathcal{M}$ (Zorn's Lemma appears here). Then the quotient:

$$K_1 = \frac{F[S]}{\mathcal{M}}$$

Is a field which contains F. Furthermore, each of the polynomials f has a root in K_1 by construction, since $f(x_f) \in I$ and therefore the image of x_f is a root.

We repeat this construction with K_1 to obtain a field K_2 in which all polynomials with coefficients in K_1 has a root. In this way, we get a sequence of fields:

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_j \subseteq K_{j+1} \subseteq \ldots$$

And each polynomial with coefficients in K_j has a root in K_{j+1}. Now, denote:

$$K = \bigcup_{j \geq 0} K_j$$

K is a field which contains F and the cofficients of any polynomial in K lie in some field K_N and thus in K; thus the polynomial has a root in $K_{N+1} \subset K$. Thus, K is algebraically closed.

Proposition 4

> Let K be an algebraically closed field and F a subfield of K. Then the collection of elements $\overline{F}$ of K that are algebraic over F is an algebraic closure of F. The algebraic closure is unique up to isomorphism.

By definition, $\overline{F}$ is an algebraic extension of F. Furthermore, K contains all the roots of polynomials with coefficients in F (indeed, with coefficients in K); so, in $\overline{F}[x]$ every polynomial in $F[x]$ splits completely; thus, $\overline{F}$ is an algebraic closure of F.

Thus, if we can locate a field F as a subfield of an algebraically closed field, then we create an algebraic closure $\overline{F}$ by collecting all alements of K which are algebraic over F.

The uniqueness follows from the fact that the splitting field is unique up to isomorphism (and Zorn's Lemma is involved, as you might expect).

Theorem 3 (Fundamental Theorem of Algebra)

> The field $\mathbb{C}$ is algebraically closed.

This theorem will be proven later using Galois theory.

Corollary

> $\mathbb{C}$ contains an algebraic closure for any of its subfields. In particular, $\overline{\mathbb{Q}}$, the collection of complex numbers which are algebraic over $\mathbb{Q}$, is an algebraic closure of $\mathbb{Q}$.

From the above theorem, we can think of any discussion of F as taking place in the context of the (generally larger) field $\overline{F}$. A composite of any collection of algebraic extensions can be viewed as subfields of an algebraic closure. For example, in $\mathbb{Q}$, all of the computation is ``really'' happening in $\mathbb{C}$.

10.2 Separable Extensions

Let F be a field and $f(x)$ a polynomial. Over a splitting field we can write:

$$f(x) = (x - \alpha_1)^{n_1} \dots (x - \alpha_k)^{n_k}$$

With α_i all distinct roots.

Definition: A polynomial over F is called separable if its roots are all distinct; otherwise, a polynomial is inseparable.

Note that since splitting fields are isomorphic, with an isomorphism that is bijective on the roots, separability is in a sense an ``instrinsic'' property of polynomials irrespective of the splitting field.

Definition: The **formal derivative** of the polynomial:

$$f(x) = a_n x^n + \dots + a_1 x + a_0 Df(x) = n a_n x^{n-1} + \dots + a_1$$

We're not actually taking derivatives here; there are no limits.

Proposition 5

> A polynomial $f(x)$ has a multiple root α iff α is also a root of $Df(x)$. In particular, this means that $f(x)$ and $Df(x)$ are both divisible by the minimal polynomial for α.

Suppose that α is a multiple root. Then over a splitting field:

$$f(x) = (x - \alpha)^n g(x)$$

Taking the derivative:

$$Df(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n Dg(x)$$

And so there is a common factor of $(x - \alpha)$ as desired.

This tells us that f is separable iff $(f, Df) = 1$.

Conversely, suppose that α is a root of both f and Df. Then we can write:

$$f(x) = (x - \alpha)h(x)$$

Taking the derivative yields:

$$Df(x) = h(x) + (x - \alpha)Dh(x)$$

By assumption, $Df(\alpha) = 0$; thus, $h(\alpha) = 0$, and we are done.

Note that the above proof holds over arbitrary characteristic.

Corollary

> Over a field of characteristic 0, a polynomial is separable iff it is the product of distinct irreducibles. In particular, an irreducible polynomial is separable.

Suppose that $p(x)$ is irreducible with degree n. Then the derivative has degree $n - 1$, and must thus be relatively prime to $p(x)$. Thus, p is separable. Note also that distinct irreducibles do not have any zeroes in common (since if they did, both divide the minimal polynomial and one must be a factor of the other).

However, in characteristic p, the derivative could simply have degree 0. For example:

$$D(x^{pm}) = pmx^{pm-1} = 0$$

So, the above proof only works if we take an irreducible polynomial whose derivative is nonzero.

However, suppose the derivative of $p(x)$ is zero. Then every exponent (from the above discussion) must be a multiple of p, the characteristic of F. So:

$$p(x) = a_m x^{mp} + a_{m-1}x^{(m-1)p} + \cdots + a_1 x^p + a_0$$

So indeed $p(x)$ is a polynomial in x_p.

Proposition 6

> Let F be a field of characteristic p. Then:
>
> $$(a + b)^p = a^p + b^p (ab)^p = a^p b^p$$
>
> This follows from the binomial theorem. In particular, it tells us that $\varphi(a) = a^p$ is an injective field homomorphism from F to F.

Definition: The map $\varphi(a) = a^p$ for a field of characteristic p is called the **Frobenius endomorphism**.

Corollary

> If $\mathbb{F}$ is a finite field of characteristic p, then the Frobenius map is an automorphism, i.e. $\mathbb{F} = \mathbb{F}^p$.

Now, we return to the problem of locating irreducible polynomials over fields of characteristic p.

Proposition 7

> A polynomial over a finite field $\mathbb{F}$ is separable iff it is the product of distinct irreducibles. An irreducible polynomial is separable.

Let $\mathbb{F}$ be a finite field and $p(x) \in \mathbb{F}[x]$ is irreducible. If $p(x)$ is inseparable, then its derivative is zero, so from above we can write $p(x) = q(x^p)$ for some polynomial $q(x) \in \mathbb{F}[x]$. Then we let:

$$q(x) = a_m x^m + \cdots + a_1 x + a_0$$

By the Frobenius automorphism, we can denote $a_i = b_i^p$. Thus we can write:

$$\begin{aligned} p(x) = q(x^p) &= a_m (x^p)^m + \cdots + a_1 x^p + a_0 \\ &= b_m^p (x^p) m + \cdots + b_1^p x^p + b_0^p \\ &= (b_m x^m)^p + \cdots + (b_1 x)^p + b_0^p \\ &= (b_m x_m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0)^p \end{aligned}$$

And thus shows that $p(x)$ is the pth power of a polynomial in $\mathbb{F}[x]$ and hence is not irreducible.

We generalize the concept of the Frobenius automorphism:

Definition: A field K of characteristic p is called perfect if $K = K^p$. Any field of characteristic 0 is called perfect.

As we showed, finite fields are perfect. With the above proof, we proved the more general statement that irreducible polynomials over perfect fields are separable. If K is not perfect, there are inseparable irreducible polynomials.

Example (Existence & Uniqueness of Finite Fields) The polynomial $x^{p^n} - x$ over $\mathbb{F}_$ has derivative:

$$p^n x^{p^n - 1} - 1 = -1$$

Thus, the derivative has no roots at all. Therefore, this polynomial is separable.

Now, let $n > 0$ and consider the splitting field of the above polynomial. Since it is separable, it has p^n roots exactly. Now, let α, β be any two roots. Then:

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta(\alpha^{-1})^{p^n} = \alpha^{-1}$$

Thus, the roots of this polynomial form a subfield of the splitting field; hence it must be the splitting field. Finally, since the number of elements is p^n, we must have:

$$[\mathbb{F} : \mathbb{F}_p] = n$$

This shows the existence of finite fields of size p^n. Now, we show uniqueness.

If $\mathbb{F}$ is a finite field of characteristic p, then we denote $n = [\mathbb{F} : \mathbb{F}_p]$, i.e. the degree over its prime subfield. Thus, $\mathbb{F}$ has exactly p^n elements. Since the multiplicative group has order $p^n - 1$, we must have:

$$\alpha^{p^n-1} = 1$$

For any $\alpha \neq 0$ in $\mathbb{F}$. Therefore, $\alpha^{p^n} = \alpha$, and thus $\mathbb{F}$ is contained in the splitting field for $x^{p^n} - x$; by counting considerations, $\mathbb{F}$ is indeed this splitting field, which is unique up to isomorphism.

We saw that if $p(x)$ is irreducible over a field of characteristic p, then if it is not separable its derivative is zero, hence $p(x) = p_1(x^p)$ for some polynomial $p_1(x)$. Continuing this process, there is a unique power p^k so that:

$$p(x) = p_k(x^{p^k})$$

Where p_k has nonzero derivative.

Thus, if p is an irreducible polynomial over F with char. p, then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{\text{sep}}(x) \in F[x]$ such that:

$$p(x) = p_{\text{sep}}(x^{p^k})$$

Definition: Suppose p is an irreducible polynomial over F with char. p. Then we call teh degree of $p_{\text{sep}}(x)$ the separable degree of $p(x)$, and the integer p^k is denoted the inseparable degree of $p(x)$.

Definition: A field K is **separable** over F is every element of K is the root of some separable polynomial over F (or equivalently, if the minimal polynomial of every element is separable).

Corollary

> Every finite extension of a perfect field is separable. In particular, every finite extension of $\mathbb{Q}$ or a finite field is separable.

As we saw before, every finite extension is algebraic. Furthermore, every algebraic element can be realized as the root of some unique minimal polynomial which is irreducible. Finally, by the above discussion, irreducible polynomials over perfect fields are separable.

10.3 Cyclotomic Polynomials and Extensions

We now prove that the cyclotomic extension discussed earlier:

$$\mathbb{Q}(\zeta_n)/\mathbb{Q}$$

Has degree exactly $\varphi(n)$, where φ denotes the totient.

Definition: Let μ_n denote the group of nth roots of unity over $\mathbb{Q}$.

As seen before, this is nothing more than the cyclic group of size n.

If d is a divisor of n, then we have:

$$\mu_d \subseteq \mu_n$$

Conversely, every element of μ_n has an order which is a divisor of n, and thus, we can write:

Definition: Define the nth cyclotomic polynomial $\Phi_n(x)$ to be the polynomial whose roots are the primitive nth roots of unity. Then:

$$\Phi_n(x) = \prod_{\zeta \in \mu_n \text{ primitive}} (x - \zeta) = \prod_{(a,n)=1\ ,\ 1 \leq a < n} (x - \zeta_n^a)$$

The roots of the polynomial $x^n - 1$ gives us the factorization:

$$x^n - 1 = \prod_{d|n} \prod_{\zeta \in \mu_d \text{ primitive}} (x - \zeta)$$

But the inner product is exactly $\Phi_d(x)$ so we can write:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

And taking the degrees we get:

$$n = \sum_{d|n} \varphi(d)$$

Now, we can compute $\Phi_n(x)$ recursively by dividing out the prior cyclotomic polynomials.

Lemma

$\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ with degree $\varphi(n)$.

Theorem 4

The cyclotomic polynomial $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Corollary

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

11 The Fundamental Theorem of Galois Theory

11.1 Introduction

Beginning with a polynomial $f(x)$, there exists a finite extension of F which contains the roots of $f(x)$. Galois THeory aims to relate the group of permutations fo the roots of f to the algebraic structure of its splitting field. In a similar way to representation theory, we study an object by how it acts on another.

Definition: An isomorphism σ of K with itself is called an automorphism of K. The collection of automorphism K is denoted $Aut(K)$.

Definition: If F is a subset of K (like a subfield), then an automorphism σ is said to fix F if it fixes every element of F.

Note that any field has at least one automorphism: the identity map, called the trivial automorphism.

Note that the prime subfield is generated by 1, and since any automorphism sends 1 to 1, any automorphism of a field fixes its prime subfield. For example, $\mathbb{Q}$ and $\mathbb{F}_p$ have only the trivial automorphism.

Definition: Let K/F be an extension of fields. Then, $Aut(K/F)$ is the collection of automorphisms of K which fix F.

Note that the above discussion gives us that $Aut(K) = Aut(K/F)$, if F is the prime subfield. Note that under composition, there is a group structure on automorphisms.

Proposition 1

$Aut(K)$ is a group under composition and $Aut(K/F)$ is a subgroup.

Proposition 2

Let K/F be a field extension, and $\alpha \in K$ algebraic over F. Then for any $\sigma \in Aut(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α. In other words, $Aut(K/F)$ permutes the roots of irreducible polynomials.

Suppose that α satisfies the equation:

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$$

Where $c_i \in F$. Then apply the automorphism σ to obtain:

$$(\sigma\alpha)^n + c_{n-1}(\sigma\alpha)^{n-1} + \cdots + c_0 = 0$$

And thus, $\sigma\alpha$ is a root of the same polynomial over F as α.

In general, if K is generated over F by some elements, then an automorphism is completely determined by its action on the generators.

In particular, if K/F is finite, then it is finitely generated over F by algebraic elements. In this case, the number of automorphisms fixing F is finite, and $Aut(K/F)$ is a finite group. In this case, the automorphisms of a finite extension are permutations of the roots of a finite number of equations (though not every permutation necessarily gives an automorphism).

We have described a field associated to each extension; we now reverse the process.

Proposition 3

> Let $H \leq Aut(K)$ be a subgroup of $Aut(K)$. The collection of all elements F of K which are fixed by H is a subfield.

This follows from readily from the definition of an field isomorphism.

Note here that we do not necessarily need a subgroup, but just a subset of K.

Proposition 4

> The above association is inclusion reversing: - If $F_1 \subseteq F_2 \subseteq K$ then $Aut(K/F_2) \leq Aut(K/F_1)$. - If $H_1 \leq H_2 \leq Aut(K)$ are two subgroups of automorphisms with fixed fields F_1 and F_2 then $F_2 \subseteq F_1$.

It maybe should be clear here that we are heading towards a bijection of some sort. We begin by investigating the size of the automorphism group of a splitting field.

Let F be a field and let E be the splitting field over F of $f(x)$. We know that we can extend an isomorphism $\varphi : F \to F'$ to an isomorphism $\sigma : E \to E'$, where E' is the splitting field over F' of $f'(x)$.

We now show that the number of such extensions is at most $[E : F]$, with equality if f is separable over F. We proceed by induction. If $[E : F] = 1$, then $E = F$ and there is only one extension (the identity).

If $[E : F] > 1$, then $f(x)$ has at least one irreducible factor $p(x)$ of degree greater than 1 which maps to $p'(x)$. Fix α, a root of $p(x)$. Then, if σ is any extension of φ to E, then σ restricted to $F(\alpha)$ is an isomorphism τ which maps $F(\alpha)$ to $F'(\beta)$, where β is a root of $p'(x)$. We have the two extensions:

$$\begin{aligned} \sigma &: E \to E' \\ \tau &: F(\alpha) \to F'(\beta) \\ \varphi &: F \to F' \end{aligned}$$

Now conversely, say β is a root of $p'(x)$. Then we can by the same process construct such a diagram.

Counting the number of extensions σ of φ is now counting the number of diagrams.

To extend φ to τ is to count the number of distinct roots β of $p'(x)$. Since $p(x)$ and $p'(x)$ both have degree $[F(\alpha) : F]$, the number of extensions of φ to τ is at most $[F(\alpha) : F]$, with equality if the roots are distinct.

Now, since E is the splitting field of f over $F(\alpha)$ and E' is the splitting field of f' over $F'(\beta)$, and by hypothesis $[E : F(\alpha)] < [E : F]$, we apply the induction hypothesis to say that the number of extensions of τ to σ is at most $[E : F(\alpha)]$, with equality if f has distinct roots.

Finally, since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that the number of extensions of φ to σ is at most $[E : F]$, with equality if $f(x)$ has distinct roots.

In particular, when $F = F'$ and φ is the identity map, the isomorphisms σ are exactly the automorphisms of E fixing F.

Corollary 1

Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then:

$$|Aut(E/F)| \leq [E : F]$$

With equality if $f(x)$ is separable over F.

Therefore, the splitting field of a separable polynomial is exactly the ``bijective'' correspondence we are looking for, in which $[E : F] = |Aut(E/F)|$.

Definition: Let K/F be a finite extension. Then K is said to be **Galois** over F and K/F is a Galois extension if $|Aut(E/F)| = [K : F]$. The group of automorphisms is called the Galois group of K/F, denoted $Gal(K/F)$.

Corollary 2

> If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.

We will see that the converse is also true.

Note also that this tells us that the splitting field of any polynomial over $\mathbb{Q}$ is Galois, since the splitting field of a polynomial is the same as the one obtained by removing multiple factors, which is separable.

Definition: If $f(x)$ is a separable polynomial over F, then the Galois group of f over F is the Galois group of the spliting field of $f(x)$ over F.

11.2 The Fundamental Theorem of Galois Theory

Definition: A character of a group G with values in a field L is a homomorphism from G to the multiplicative group $L^\times$.

Definition: The characters $\chi_1, \chi_2, \ldots, \chi_n$ are linearly independent if they are linearly independent functions on G.

Theorem 1

> If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters of G, then they are linearly independent.

Now, consider an injective homomorphism σ of a field K into a field L, which is called an embedding of K into L. In particular, σ can be viewed as a character of $K^\times$ with values in L.

Corollary 3

> If $\sigma_1, \ldots, \sigma_n$ are distinct embeddings of K into L, then they are linearly independent as functions on K. In particular, the distinct automorphisms of a field K are linearly independent as functions on K.

Theorem 2

> Let $G = \sigma_1, \ldots \sigma_n$ be a subgroup of automorphisms of a field K and let F be its fixed field. Then:
>
> $$[K : F] = n = |G|$$

This proof will be omitted; it follows from analyzing systems of equations.

Corollary 4

Let K/F be any finite extension. Then:

$$|Aut(K/F)| \leq [K : F]$$

With equality iff F is the fixed field of $Aut(K/F)$. This tells us that K/F is Galois iff F is the fixed field of $Aut(K/F)$.

To prove this, let F_1 be the fixed field of $Aut(K/F)$. In other words:

$$F \subseteq F_1 \subseteq K$$

By Theorem 2, we have:

$$[K : F_1] = |Aut(K/F)|$$

Hence, we have:

$$[K : F] = |Aut(K/F)|[F_1 : F]$$

And this proves the corollary.

Corollary 5

Let G be a finite subgroup of automorphisms of a field K and let F be its fixed field. Then every automorphism of K fixing F is contained in G, i.e.:

$$Aut(K/F) = G$$

Therefore, K/F is Galois, with Galois group G.

Note that by definition $G \leq Aut(K/F)$. But by the theorem we have $|G| = [K : F]$. By the previous corollary we have $|Aut(K/F)| \leq [K : F] = |G|$. This gives:

$$[K : F] \leq |Aut(K/F)| \leq [K : F]$$

And therefore, if we have a subgroup of automorphisms, then K is a Galois extension over its fixed field.

Corollary 6

> If $G_1 \neq G_2$ are distinct finite subgroups of automorphisms of a field K, then their fixed fields are also distinct.

If the fixed fields $F_1 = F_2$, then by definition F_1 is fixed by G_2. But then $G_2 \neq G_1$, and similarly $G_1 \leq G_2$ adn thus the two groups are equal.

The corollaries above tell us that taking fixed field for distinct finite subgroups of $Aut(K)$ gives distinct subfields of K over which K is Galois. The degrees of the extensions are given by the orders of the subgroups.

The next result completely characterizes Galois extensions.

Theorem 3

> The extension K/F is Galois iff K is the splitting field of some separable polynomial over F. If this is the case then every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K (K/F is in particular separable).

We showed earlier that the splitting field of a separable polynomial is Galois. We now show, essentially, the converse.

Let $G = Gal(K/F)$ and let $\alpha \in K$ be a root of $p(x)$, an irreducible polynomial in $F[x]$ which has a root in K. Consider the elements:

$$\alpha, \sigma_2(\alpha), \ldots, \sigma_n(\alpha) \in K$$

Where σ_i represent the elements of the Galois group. Of this list, denote the distinct elements by:

$$\alpha, \alpha_2, \ldots, \alpha_r$$

If $\tau \in G$ then since G is a group applying τ to the first list just permutes it. In particular, teh following polynomial has coefficients which are fixed by all the elements of G:

$$f(x) = (x - \alpha)(x - \alpha_2) \ldots (x - \alpha_r)$$

The coefficients thus lie in the fixed field of G. However, note that K/F is Galois iff F is the fixed field of $Aut(K/F)$, so the fixed field of G is exactly F. Thus, $f(x) \in F[x]$.

Since $p(x)$ is irreducible and has α as a root, $p(x)$ is the minimal polynomial for α over F, and it follows that $p(x)$ divides $f(x)$ in $F[x]$. So we have:

$$p(x) = f(x)$$

This shows that $p(x)$ is separable and all its roots lie in K.

To complete the proof, suppose K/F is Galois and let $\omega_1, \ldots, \omega_n$ be a basis for K/F. let $p_i(x)$ be the minimal polynomial for ω_i. Then $p_i(x)$ is separable and has all its roots in K. Let $g(x)$ be the polynomial obtained by removing multiple factors in this product. Then the splitting field of the two polynomials is the same and this field is K. Hence, K is the splitting field of the separable polynomial $g(x)$.

Definition: Let K/F be a Galois extension. If $\alpha \in K$ then the elements $\sigma\alpha$ for $\sigma \in Gal(K/F)$ are called the Galois conjugates of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the conjugate field of E over F.

The proof of Theorem 3 shows that in a Galois extension K/F, if we have $\alpha \in K$ which is a root of a minimal polynomial over F, then the other roots are precisely the distinct conjugates of α under the Galois group of K/F.

The theorem also says that K is not Galois over F if we can find an irreducible polynomial over F which has a root in K but not all its roots in K. Now we have four characterizations of Galois extensions K/F:

- Splitting fields of separable polynomials over F.
- Fields where F is precisely the fixed field of $Aut(K/F)$ (in general, the fixed field may be larger than F).
- Fields with $[K : F] = |Aut(K/F)|$.
- Finite, normal, and separable extensions.

Theorem (Fundamental Theorem of Galois Theory)

Let K/F be a Galois extension and let $G = Gal(K/F)$. Then there is a bijection between subfields:

$$F \subseteq E \subseteq K$$

And subgroups of the Galois group:

$$1 \subseteq H \subseteq G$$

In particular, the correspondence identifies E to the elements of G which fix E. Conversely, it identifies H with the fixed field of H. - The correspondence is inclusion reversing. - $[K : E] = |H|$, and $[E : F] = [G : H]$. - K/E is always Galois, with Galois group $Gal(K/E) = H$. - E is Galois over F iff H is a normal subgroup in G. If this is the case then $Gal(E/F) \cong G/H$. More generally, the isomorphisms of E which fix F correspond with cosets of H in G. - If E_1, E_2 correspond to H_1, H_2, then the intersection $E_1 \cap E_2$ corresponds

to the group generated by H_1, H_2. The composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$.

We will number these points 1 through 5 and prove each separately.

Part 1 Given any subgroup H of G, we saw that there is a unique fixed field $E = K_H$. The correspondence is thus injective from subgroups to subfields. We now need to see that it is surjective, i.e. we can find a subgroup of the Galois group which fixes any subfield.

Now, if K is the splitting field of a separable polynomial $f(x) \in F[x]$ then it is an element of $E[x]$ for any subfield $F \subseteq E \subseteq K$. Thus, K is also the splitting field of f over E, and therefore K/E is Galois. Thus, E is the fixed field of $Aut(K/E) \leq G$. This shows that indeed our correspondence is bijective. Concretely, the automorphisms fixing E are precisely $Aut(K/E)$ since K/E is Galois.

The Galois correspondence is evidently inclusion reversing.

Part 2 If $E = K_H$ is the fixed field of H (which is Galois), then by Theorem 2 $[K : E] = |H|$, and similarly $[K : F] = |G|$. Taking the quotient gives $[E : F] = [G : H]$.

Part 3 Since E is the fixed field of a subgroup $H \leq G$, by Corollary 5, K/E is Galois with Galois group $Gal(K/E) = H$.

Part 4

Lemma

Let E be the fixed field of a subgroup H. Then σ is an embedding of E iff it is the restriction of some automorphism $\sigma \in G$ to E.

Let $E = K_H$ be the fixed field of the subgroup H. Then every $\sigma \in G$, when restricted to E, gives an embedding of E with a subfield $\sigma(E)$ of K. We shall show that these are indeed the only embeddings of E.

Conversely, let $\tau : E \to \tau(E) \subseteq \overline{F}$ be any embedding of E (into a fixed algebraic closure $\overline{F}$ containing K) which fixes F. Then, if $\alpha \in E$ has minimal polynomial m_α over F then $\tau(\alpha)$ is another root of $m_\alpha(x)$ and so K contains $\tau(\alpha)$ as well. Thus, $\tau(E) \subseteq K$.

As above, K is the splitting field of $f(x)$ over E and so it is also the splitting field of $\tau f(x) = f(x)$ (since τ fixes F) over $\tau(E)$.

So, we can extend τ to an isomorphism σ from K to K. Since σ fixes F, what we have just shown is that every embedding τ of E fixing F can be extended to an automorphism σ of K fixing F. In other words, every embedding of E is the action of some $\sigma \in G$.

Proof Now, two automorphisms $\sigma, \sigma' \in G$ restrict to the same embedding of E iff $\sigma^{-1}\sigma'$ is the identity on E. But then $\sigma^{-1}\sigma' \in H$ since the automorphisms of K which fix E are exactly H. Another way of saying this is that $\sigma' \in \sigma H$.

What we have just shown is that distinct embeddings of E are in bijection with cosets σH of H in G. In particular, this gives us that:

$$|\text{Emb}(E/F)| = [G : H] = [E : F]$$

Where Emb denotes the set of embeddings of E into a fixed algebraic closure of F. Note that Emb(E/F) contains the automorphisms $Aut(E/F)$, since any automorphism admits to an embedding by our lemma.

The extension E/F is Galois iff $|Aut(E/F)| = [E : F]$. By the equality above, this is the case iff each embedding of E is an automorphism of E, i.e. $\sigma(E) = E$.

Now note that if $\sigma\alpha \in \sigma(E)$, then:

$$(\sigma h \sigma^{-1})(\sigma\alpha) = \sigma(h\alpha) = \sigma\alpha$$

For any $\alpha \in E$, since H fixes E. Thus $\sigma H \sigma^{-1}$ fixes $\sigma(E)$. The group fixing $\sigma(E)$ has order equal to $[K : \sigma(E)] = [K : E] = |H|H$, so indeed $\sigma H \sigma^{-1}$ is precisely the group fixing $\sigma(E) = E$.

Because the Galois correspondence is a bijection, $\sigma H \sigma^{-1} = H$ and hence H is normal. Thus, E is Galois over F iff H is normal in G.

Furthermore, this proof shows that the group of cosets G/H is identified with the group of automorphisms of the Galois extension E/F. Thus, $G/H \cong Gal(E/F)$.

Part 5 Suppose H_1 is the subgroup of elements fixing E_1 and H_2 the subgroup of elements fixing E_2. Then any element in $H_1 \cap H_2$ fixes both E_1 and E_2 and hence fixes the composite. Conversely, if an automorphism σ fixes the composite E_1E_2, then in particular $\sigma \in H_1 \cap H_2$. Similarly, the intersection $E_1 \cap E_2$ corresponds to the subgroup generated by H_1, H_2, and this proves the final part.