

Algebra Qualifying Exam Syllabus and Notes

Toni A. Watson

January 1, 2005

Contents

0 Preliminaries	7
1 Groups	9
1.1 Introduction	9
1.1.1 Popular Groups	10
1.2 Centralizers and Normalizers	11
1.3 Cyclic Groups	12
1.4 Symmetric groups	14
1.5 Lagrange's theorem	15
1.6 Quotient Groups and Homomorphisms	15
1.7 Normal Subgroups	18
1.8 Isomorphism Theorems	19
1.9 Normal series	20
1.10 Jordan Hölder Theorem	21
1.11 Group Actions	21
1.11.1 Class Formula	22
1.11.2 Automorphisms	23
1.12 Sylow's Theorems	24
1.13 Solvable Groups	25
1.13.1 Solvability of p -groups	27
1.14 Category Theory	27
1.15 Direct Products	29
1.15.1 Semidirect Products	30
1.15.2 Fundamental Theorem of Finitely Generated Abelian Groups	31
1.16 Exercises	32
2 Rings	33
2.1 Introduction	33
2.1.1 Left, Right and Two-sided Ideals	34
2.1.2 Quotients, Homomorphisms and Isomorphism theorems	36
2.1.3 Zorn's Lemma	37
2.1.4 Rings of Fractions and Quotient Fields	37
2.1.5 Chinese Remainder Theorem	38
2.1.6 Euclidian Domains	39
2.1.7 Principal Ideal Domains (PIDs) and Unique Factorization Domains (UFDs)	40

2.1.8	Polynomial rings	42
2.1.9	Gauss' Lemma	42
2.1.10	Factorization	43
2.1.11	Simple rings	44
2.1.12	Artinian and Noetherian Rings	44
2.2	Wedderburn's theorem for simple Artinian rings	45
2.3	Hilbert Basis Theorem	45
2.4	Localization	46
2.5	Local rings	46
3	Modules	47
3.1	Elementary Module Theory	47
3.1.1	Quotients and Isomorphism Theorems	49
3.1.2	Direct sums (internal and external) and Free Modules	49
3.2	Tensor products	50
3.3	Exact Sequences	52
3.3.1	Dual Modules	53
3.3.2	Finitely generated modules over P.I.D.s	54
3.3.3	Exactness properties of tensor products	54
3.4	Exterior algebra	54
3.5	Projective and Injective modules	55
3.6	Homology	56
3.7	Derived functors incl. Tor and Ext	56
4	Field Theory	57
4.1	Characteristics	57
4.2	Extensions	57
4.3	Algebraic Extensions and Finite Fields	58
4.4	Splitting Fields	60
4.4.1	Normal Extensions	60
4.4.2	Separability	60
4.4.3	Roots of Unity	61
4.5	Algebraic Closure	61
4.6	Transcendence Basis	62
4.7	Galois Theory	62
4.7.1	Fundamental Theorem of Galois Theory	62
4.7.2	Galois groups of polynomials as permutation groups	62
4.7.3	Cyclic Extensions	62
4.7.4	Ruler and Compass Constructions	62
4.7.5	solvability by radicals	63
4.7.6	norms and traces	63
4.7.7	computations of Galois groups	63

5	Linear Algebra	65
5.1	Vector Spaces	65
5.2	Linear Transformations and Matrices	68
5.3	Invariant Subspaces and Characteristic Polynomials	69
5.4	Similarity and Canonical Forms	70
5.5	Inner Products and Bilinear Forms	71
6	Representation Theory (of finite groups)	73
6.1	Introduction	73
6.1.1	Direct Sums and Tensor Products	74
6.1.2	Examples	74
6.2	Irreducibility	74
6.3	Characters	75
6.4	Schur's Lemma	75
6.5	Subgroups	75

Chapter 0

Preliminaries

Definition 0.1 (Euler Phi Function) Given $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$,

$$\varphi(n) = p_1^{\alpha_1-1}(p_1 - 1) \cdots p_r^{\alpha_r-1}(p_r - 1)$$

represents the number of integers k ($1 \leq k \leq n$) such that $(n, k) = 1$.

Definition 0.2 Let A be any nonempty set. A partition of A is a decomposition of A into nonempty disjoint subsets, called cells, such that each element of A appears in exactly one cell.

Proposition 0.1 Let A be a nonempty set.

- (1) If \sim defines an equivalence relation on A , then the set of equivalence classes \sim form a partition of A .
- (2) If $\{A_i \mid i \in I\}$ is a partition of A then there is an equivalence relation on A whose equivalence classes are precisely the sets A_i for $i \in I$.

Define a relation on \mathbb{Z} by $a \sim b$ if and only if $n \mid (b - a)$. If $a \sim b$ then it is said that $a \equiv b \pmod{n}$ for any integer $n \in \mathbb{Z}$

Definition 0.3 The equivalence class (or residue class) of a , written \bar{a} , consists of the integers that differ from a by an integer multiple. i.e.,

$$\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$$

Observe that there are precisely n distinct equivalence classes mod n .

Definition 0.4 $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{a} \cdot \bar{c} = \bar{1}\}$.

It follows from the definition of residue classes that if any representative of \bar{a} is relatively prime to n , then all representatives are relatively prime. Applying this fact to the definition of $\mathbb{Z}/n\mathbb{Z}^\times$ we can obtain another definition for the group:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$$

Corollary 0.1 $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Chapter 1

Groups

1.1 Introduction

Definition 1.1 A group is an ordered pair (G, \star) where G is a set and \star is a binary operation on G satisfying the following axioms:

- (i) (Associativity) $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in G$.
- (ii) (Identity element) There exists an identity element e in G such that for all $a \in G$ $a \star e = a = e \star a$.
- (iii) (Inverse element) For each $a \in G$, there is an inverse element $a^{-1} \in G$ such that

$$a \star a^{-1} = e = a^{-1} \star a.$$

The group is called abelian if additionally,

- (iv) $a \star b = b \star a$ for all $a, b \in G$.

It is also nice to identify other ordered pairs whose algebraic structures have weaker assumptions. In particular, a *semigroup* is a set with an associative binary operation and a *monoid* is a set with an identity element for the binary operation.

Definition 1.2 Let G be a group. The subset H of G is subgroup of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Proposition 1.1 A subset H of a group G is a subgroup if and only if

- (1) $H \neq \emptyset$
- (2) for all $x, y \in H$, $xy^{-1} \in H$

Proof:

If H is a subgroup, then (1) and (2) hold trivially.

Conversely suppose (1) and (2) hold and let $x \in H$. Then, by (2), $xx^{-1} = 1 \in H$ so H contains the identity element. This, together with (2) again, implies that $1x^{-1} = x^{-1} \in H$ so $x \in H \Rightarrow x^{-1} \in H$. Finally, if $x, y \in H$ then, by (2) again, $x(y^{-1})^{-1} = xy \in H$ (since $y^{-1} \in H$ by previous step). So H is closed under multiplication. Hence, H is a subgroup. ★

Proposition 1.2 *If $\{H_i\}$ is any nonempty collection of subgroups of G , then $\bigcap H_i$ is a subgroup of G .*

Proof: $1 \in \bigcap H_i$ so $\bigcap H_i$ is nonempty. Additionally, suppose $x, y \in \bigcap H_i$. Then $x, y \in H_i$ for each i . Since each H_i is a subgroup, of G , $xy^{-1} \in H_i$ for each $i \implies xy^{-1} \in \bigcap H_i$. Hence, by the subgroup criterion, $\bigcap H_i$ is a subgroup of G . ★

Proposition 1.3 *If H is finite, then H is a subgroup if H is nonempty and closed under multiplication.*

Proof: Let $H = \{h_1, \dots, h_n\}$ and suppose $x \in H$. Since H is closed under multiplication x, x^2, \dots are distinct in H . Since H is finite, there are integers a and b with $a < b$ such that $x^a = x^b$. If $m = b - a$, then $x^m = x^{b-a} = x^0 = 1$ so $1 \in H$. Since $x^{m-1} = x^{-1}$ is also in H , H is closed under inverses. Hence, $H \leq G$. ★

1.1.1 Popular Groups

MATRIX GROUPS:

$$GL_n(\mathbb{F}) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } \mathbb{F} \text{ such that } \det(A) \neq 0\}$$

is called the *General Linear Group over \mathbb{F}* of degree n .

Additionally, $GL_n(\mathbb{F})$ is a nonabelian group under multiplication. However, under addition, it is not a group (note that the zero matrix is not in $GL_n(\mathbb{F})$).

The set of matrices $A \in GL_n(\mathbb{F})$ such that $\det(A) = 1$ is called the *Special Linear Group over \mathbb{F}* and is denoted $SL_n(\mathbb{F})$.

Proposition 1.4

- (1) *If \mathbb{F} is a field and $|\mathbb{F}| < \infty$, then $|\mathbb{F}| = p^m$ for some prime p and integer m .*
- (2) *If $|\mathbb{F}| = q < \infty$, then $|GL_n(\mathbb{F})| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.*
- (3) $|SL_n(\mathbb{F})| = |GL_n(\mathbb{F})|/(q - 1)$

DIHEDRAL GROUP:

$$D_n = \langle a, b \mid a^n = b^2 = 1, ab = ba^{-1} \rangle$$

$|D_n| = 2n$ for all $n \in \mathbb{Z}^+$. Be advised that, in some texts, the dihedral group is denoted D_{2n} . Clearly, this isn't a standard convention.

SYMMETRIC GROUPS:

Let Ω be any nonempty group and S_Ω be the set of all bijections from Ω to itself. The set S_Ω is a group under function composition and is called the symmetric group on the set Ω . If $\Omega \subset \mathbb{Z}^+$, then $S_\Omega = S_n$ and is called the symmetric group of degree n . Additionally, $|S_n| = n!$ and is nonabelian for $n \geq 3$.

Example 1.1 Let $\Omega = \{\clubsuit, \heartsuit, \spadesuit\}$. Then the operation, $\sigma : \Omega \rightarrow \Omega$ defined by

$$\sigma : \begin{cases} \spadesuit \mapsto \clubsuit \\ \heartsuit \mapsto \spadesuit \\ \clubsuit \mapsto \heartsuit \end{cases}$$

is a bijection and; therefore, an element of S_Ω . In cycle notation, σ can be expressed as $(\heartsuit \spadesuit \clubsuit)$. In fact, $S_\Omega = \{id, (\clubsuit \heartsuit), (\clubsuit \spadesuit), (\heartsuit \spadesuit), (\heartsuit \clubsuit \spadesuit), (\heartsuit \spadesuit \clubsuit)\}$.

The symmetric group will be discussed in more detail within section 1.4.

QUATERNION GROUP:

The quaternions group, \mathcal{Q}_8 , is defined by

$$\mathcal{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product \cdot and is computed as follows:

$$\begin{aligned} 1 \cdot a &= a \cdot 1 = a && \text{for all } a \in \mathcal{Q}_8 \\ (-1) \cdot (-1) &= 1, && (-1) \cdot a = a \cdot (-1) = -a \quad \text{for all } a \in \mathcal{Q}_8. \\ i \cdot i &= j \cdot j = k \cdot k = -1 \\ i \cdot j &= k, && j \cdot i = -k \\ j \cdot k &= i, && k \cdot j = -i \\ k \cdot i &= j, && i \cdot k = -j. \end{aligned}$$

As a subgroup of $GL_2(\mathbb{C})$, we can equivalently present \mathcal{Q}_8 as

$$\mathcal{Q}_8 = \langle A, B \mid A^4 = I, A^2 = B^2, B^{-1}AB = A^{-1} \rangle$$

where

$$A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Observe that \mathcal{Q}_8 is a nonabelian group of order 8.

1.2 Centralizers and Normalizers

Definition 1.3 Let A be a nonempty subset of a group G . Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the centralizer of A in G . Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A .

Definition 1.4 Define $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all of the elements of G . This subset of G is called the center of G .

Definition 1.5 Let $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. The normalizer of A in G is the set $N_G(A) = \{g \in G \mid gAg^{-1} \subseteq A\}$.

The normalizer of A is the largest subgroup of G in which A is normal.

It is clear that the center, centralizer and normalizer are all subgroups of G . Additionally, though these definitions seem quite similar, one can differentiate between the subgroups by recalling a couple of facts:

- (1) The set A is not necessarily a subgroup (for example, it may not contain the identity) and
- (2) $gAg^{-1} = A$ means that for some $a, b \in A$, $gag^{-1} = b$ with b not necessarily equal to a . To this end, we can say $C_G(A) \subseteq N_G(A)$.

Note that if G is abelian, all of the elements of G commute. In this case, $Z(G) = G$ and $N_G(A) = C_G(A)$.

1.3 Cyclic Groups

Proposition 1.5 *Let G be an arbitrary (finite) group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$ then $x^d = 1$ where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m .*

Proof:

First suppose $x^n = 1$ and $x^m = 1$. Since $d = (m, n)$, by the Euclidean Algorithm (cf § 2.1), there are integers s and t such that $d = sm + tn$. Then

$$x^d = x^{sm+tn} = x^{sm}x^{tn} = (x^m)^s(x^n)^t = 1^s1^t = 1$$

Additionally, let $|x| = n < \infty$. If $x^m = 1$, then since $|n|$ is the smallest positive integer such that $x^n = 1$, $|m| > |n|$. Then, by the Division Algorithm (cf § 2.1), there are integers q and r with $|r| < |n|$ such that $m = qn + r$. Then

$$\begin{aligned} x^m = x^{qn+r} &= x^{qn}x^r = x^r = 1 \implies r = 0 \\ \implies x^m &= x^{qn} \\ \implies m &= qn \implies n|m \end{aligned}$$



The idea behind this proposition is used quite frequently in our treatment of the cyclic group.

Definition 1.6 *A group, H , is cyclic if H can be generated by a single element, i.e. there is some element $x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\} = \langle x \rangle$.*

In a cyclic group, every element in H is some power (multiple, if the group is additive) of x . It then follows by the laws of exponents that any cyclic group is abelian. **However**, It is **not** the case that every abelian group is cyclic. To see this, consider $\mathbb{Z}_2 \times \mathbb{Z}_2$. No multiple of the element $(0, 1)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$ produces the element $(1, 1)$, contrary to the definition of a cyclic group. Thus $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Additionally, cyclic groups can be generated by more than one element. For example, an easy experiment will show that $\langle 2, 3 \rangle$ generates \mathbb{Z}_6 under addition. So a cyclic group can be generated by a finite collection of elements. However, the converse is not true. In particular, if a group is generated by a finite number of elements, it does not mean that the group is cyclic. Consider, as an example, the dihedral group, D_n . For $n \geq 3$, D_n is nonabelian so it cannot be cyclic (since all cyclic groups are abelian), but it is generated by two elements, namely its rotations, r , and reflections, s .

Theorem 1.1 Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $\langle x \rangle$ and $\langle y \rangle$ are cyclic groups of order n , then the map

$$\begin{aligned} \varphi : \langle x \rangle &\rightarrow \langle y \rangle \\ \varphi(x^k) &= y^k \end{aligned} .$$

is well defined and an isomorphism.

(2) if $\langle x \rangle$ is an infinite cyclic group, then the map

$$\begin{aligned} \varphi : \mathbb{Z} &\rightarrow \langle x \rangle \\ \varphi(k) &= x^k \end{aligned} .$$

is well defined and is an isomorphism.

Proposition 1.6 Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

(1) If $|x| = \infty$, then $|x^a| = \infty$

(2) If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.

(2') If $|x| = n < \infty$, and a is a positive integer dividing n , then $|x^a| = \frac{n}{a}$.

Theorem 1.2 Let $H = \langle x \rangle$ be a cyclic group.

(1) Every subgroup of H is cyclic. In particular, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

(2) If $|H| = \infty$, then for any distinct nonnegative integers a and b , $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m , $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m . This tells us that the nontrivial subgroups of H correspond bijectively with \mathbb{Z}^+ .

(3) If $H = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of order a . This subgroup is the cyclic subgroup $\langle x^d \rangle$, where $d = \frac{n}{a}$. Furthermore, for every integer m , $\langle x^m \rangle = \langle x^{(m,n)} \rangle$, which tells us that the subgroups of H correspond bijectively with the positive divisors of n .

Definition 1.7 If A is any subset of the group G , define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

to be the subgroup of G generated by A .

Example 1.2 Let G is a cyclic group. If $a, b \in G$ such that neither a nor b are squares, then the product ab is a square.

Proof:

Since G is cyclic, then $G = \langle x \rangle$. For $a, b \in G$, $a = x^\alpha$ and $b = x^\beta$ for $\alpha, \beta \in \mathbb{Z}$. Since a and b are not squares, then $\alpha = 2m + 1$ and $\beta = 2n + 1$ for $n, m \in \mathbb{Z}$ and

$$ab = x^\alpha x^\beta = x^{\alpha+\beta} = x^{2n+1+2m+1} = (x^{m+n+1})^2.$$



1.4 Symmetric groups

Recall that if Ω is a set, S_Ω is the set of all bijections from Ω to itself (i.e. the set of all permutations of Ω) and the set S_Ω is a group under function composition. Note that the elements of S_Ω are the permutations of S_Ω , not the elements of Ω themselves. In the special case when Ω is equal to a finite subset of \mathbb{Z}^+ , then we say that S_n is the symmetric group of degree n .

We will now discuss these special groups in more detail.

Definition 1.8 *A cycle is a string of integers that represents the element, σ , of S_n that cyclically permutes these integers (and fixes all other integers).*

Definition 1.9 *The length of a cycle is the number of integers that appear in it. A cycle of length t is called a t -cycle. Any two cycles are called disjoint if they have no numbers in common. If $t = 2$ then the t -cycle is called a transposition.*

Proposition 1.7 *Every permutation can be uniquely written as a union of disjoint cycles where each of the disjoint cycles commute. Additionally each permutation can also be written as a product of transpositions.*

Proposition 1.8 *The order of a permutation is the least common multiple of the lengths of the cycles in its cycle decomposition.*

Definition 1.10 *Consider the homomorphism $\epsilon : S_n \rightarrow \{\pm 1\}$ ($\{\pm 1\} = \langle \mathbb{Z}_2, \cdot \rangle$). Given $\sigma \in S_n$,*

(1) $\epsilon(\sigma)$ is the sign of σ and

(2) σ is called an even permutation if $\epsilon(\sigma) = 1$ and an odd permutation if $\epsilon(\sigma) = -1$.

Proposition 1.9 *An m -cycle is an odd permutation if and only if m is even. Analogously, the permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.*

In particular, a permutation is even if and only if it can be written as a product of an even number of transpositions.

Theorem 1.3 *If $n \geq 2$, then the collection of all even permutations of $\{1, 2, \dots, n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n .*

Definition 1.11 *The subgroup of S_n consisting of the even permutations of n letters is called the alternating group, A_n , on n letters.*

Equivalently, we can say that A_n is the kernel of the homomorphism ϵ .

Proposition 1.10 *Let σ, τ be elements of the symmetric group S_n and suppose σ has the cycle decomposition*

$$(a_1 \dots a_{k_1})(b_1 \dots b_{k_2}) \dots$$

Then $\tau\sigma\tau^{-1}$ has the cycle decomposition

$$(\tau(a_1) \dots \tau(a_{k_1}))(\tau(b_1) \dots \tau(b_{k_2})) \dots$$

In other words, $\tau\sigma\tau^{-1}$ is obtained by replacing every i^{th} entry in σ with the $\tau(i)^{\text{th}}$ entry.

Proof:

If $\sigma(i) = k$, then

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau\sigma(i) = \tau(k)$$

Therefore, if the ordered pair (i, j) appears in σ then $(\tau(i), \tau(j))$ must appear in $\tau\sigma\tau^{-1}$. ★

This result will prove to be quite useful during our later discussion of conjugacy classes (c.f. §1.11)

Definition 1.12

(1) If $\sigma \in S_n$, is the product of disjoint cycles of length n_1, \dots, n_r where $n_1 \leq \dots \leq n_r$ (including 1-cycles), then the integers n_1, \dots, n_r are called the cycle type of σ .

(2) If $n \in \mathbb{Z}^+$, a partition of n is any nondecreasing sequence of positive integers whose sum is n .

1.5 Lagrange's theorem

Theorem 1.4 If G is a finite group and H is a subgroup of G , then the order of H divides the order of G and the number of left (right resp.) cosets of H in G (called the index $|G : H|$) equals $\frac{|G|}{|H|}$.

The full converse to Lagrange's theorem is not true. In particular, if n divides the order of G , then there needn't be a subgroup of order n . For example, consider the group A_4 . If the converse were true, then there should be a group of order 6, since 6 divides 12. Yet, it can be later shown that A_4 has no subgroup of order 6. However, if a group G is **finite abelian**, then there is a subgroup of order n for every n dividing the order of G . Nonetheless, if G is finite, there are partial converses to Lagrange's Theorem, namely, via the Cauchy and Sylow theorems which will be discussed in later sections.

Corrolary 1.1 If G is a finite group and $x \in G$, then the order of x divides the order of G . In particular, $x^{|G|} = 1$ for all x in G .

Theorem 1.5 (Cayley's Theorem) Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n , then G is isomorphic to a subgroup of S_n .

1.6 Quotient Groups and Homomorphisms

Definition 1.13 Let $(G, *)$ and (H, \cdot) be groups. A map $\varphi : G \rightarrow H$ such that $\varphi(x * y) = \varphi(x) \cdot \varphi(y)$ for all $x, y \in G$ is called a homomorphism.

Definition 1.14 If $\varphi : G \rightarrow H$ is a homomorphism, then the kernel of φ is the set $\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$.

Proposition 1.11 Let G and H be groups and let $\varphi : G \rightarrow H$ be a homomorphism.

(1) $\varphi(1_G) = 1_H$

- (2) $\varphi(g^{-1}) = [\varphi(g)]^{-1}$ for all $g \in G$.
- (3) $\varphi(g^n) = [\varphi(g)]^n$ for all $n \in \mathbb{Z}$.
- (4) $\ker(\varphi)$ is a subgroup of G .
- (5) $\text{Im}(\varphi)$, the image of φ under G , is a subgroup of H .

Proof:

For simplicity, the subscripts are omitted.

- (1) $\varphi(1) = \varphi(1 * 1) = \varphi(1)\varphi(1) \implies \varphi(1) = 1$ by the cancellation laws.
- (2) $\varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) \implies [\varphi(g)]^{-1} = \varphi(g^{-1})$
- (3) This clearly holds for $n = 1$, by the Induction Principle, (3) holds for all $n \in \mathbb{Z}$.
- (4) By (1), $1 \in \ker(\varphi)$. Now suppose $g, h \in \ker(\varphi)$. Then

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)[\varphi(h)]^{-1} = 1 \cdot 1 = 1$$

By the Subgroup Criterion, $\ker(\varphi)$ is a subgroup of G .

- (5) An argument identical to (4) shows that $\text{Im}(\varphi)$ is a subgroup of H .



Definition 1.15 Let $\varphi : G \rightarrow H$ with kernel K . The quotient group G/K ("G modulo K" or "G mod K"), is the group whose elements are the fibers of φ such that if X is the fiber above a and Y is the fiber above b , then the product of X with Y is defined to be the fiber above the product ab .

This notation emphasizes the fact that the kernel, K , acts as a single element in the quotient group G/K .

Proposition 1.12 Let $\varphi : G \rightarrow H$ be a homomorphism of groups with kernel K . Let $X \in G/K$ such that $X = \varphi^{-1}(a)$ for $a \in G/K$. Then

- (1) For any $u \in X$, $X = \{uk \mid k \in K\}$
- (2) For any $u \in X$, $X = \{ku \mid k \in K\}$.

Definition 1.16 For any $N \leq G$, let

$$gN = \{gn \mid n \in N\} \quad \text{and} \quad Ng = \{ng \mid n \in N\}$$

be the left and right cosets (respectively) of N in G .

Any element of a coset is called the representative for the coset.

Theorem 1.6 *Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with the operation defined by*

$$uK \circ vK = (uv)K$$

forms a group, G/K .

Specifically, this operation is well defined in the sense that if u_1 is any element in uK and v_1 is any element in vK , then $u_1v_1 \in uvK$. In particular, the multiplication does not depend on the choice of representatives for the cosets. Note that this theorem is still valid if "right cosets" had been used in place of "left cosets."

Proposition 1.13 *Let N be any subgroup of G . The set of left cosets of N in G for a partition of G . Furthermore, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$.*

In particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proposition 1.14 *Let G be a group and let N be a subgroup of G . Then the operation on the set of left cosets of N on G described by*

$$uN \cdot vN = (uv)N$$

is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.

Proof:

★

Definition 1.17 *Let H and K be subgroups of a group, G , then*

$$HK = \{hk \mid h \in H, k \in K\}.$$

HK is the smallest group containing both H and K .

Proposition 1.15 *If H and K are finite subgroups of a group,*

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

This proposition helps to illustrate that HK is not necessarily a subgroup of G . Consider, for example, $G = S_3$. If $H = \langle(12)\rangle$ and $K = \langle(23)\rangle$. $|H| = |K| = 2$ and $|H \cap K| = 1$. By the above proposition, $|HK| = 4$. But LaGrange's Theorem tells us that if HK is a subgroup then $|HK|$ divides $|G|$. But $4 \nmid 6$ so HK is not a subgroup of G .

Proposition 1.16 *If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.*

Proof:

Since HK is a group, then $1 \in HK$ so HK is nonempty. Suppose $x, y \in HK$ then $x = hk$ and $y = h'k'$ for $h, h' \in H$ and $k, k' \in K$. Then

$$xy^{-1} = (hk)(h'k')^{-1} = hkk'^{-1}h'^{-1} = h\tilde{k}h'^{-1} = \tilde{k}hh'^{-1} = \tilde{k}h^* = h^*\tilde{k} \in HK$$

By the subgroup criterion, HK is a subgroup of G .

★

Corrolary 1.2 Let H and K be subgroups of the group G . The number of distinct ways of writing each element of the set HK in the form hk for $h \in H$ and $k \in K$ is equal to $|H \cap K|$. In particular, if $H \cap K = 1$ then each element of HK can be written uniquely in the form hk .

Corrolary 1.3 If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G . In particular, if $K \trianglelefteq G$, then $HK \leq G$ for any $H \leq G$.

Example 1.3 (August 2002 MA Exam) If G is a finite group and $H \leq G$ such that $G = HZ$, where Z is the center of G , then $H \trianglelefteq G$.

Proof:

$G = HZ \implies g = hz$ for each $g \in G$. Then for $h' \in H$,

$$\begin{aligned} gh'g^{-1} &= hzh'(hz)^{-1} \\ &= hzh'z^{-1}h^{-1} \\ &= hzz^{-1}h'h^{-1} \quad \text{since } z \in Z \\ &= hh'h^{-1} \in H \end{aligned}$$

so $H \trianglelefteq G$. ★

Definition 1.18 Let $N \trianglelefteq G$. The homomorphism $\pi : G \rightarrow G/N$ defined by $\pi(g) = gN$ is called the natural projection of G onto G/N . If $\overline{H} \leq G/N$ is a subgroup of G/N , the complete preimage of \overline{H} is the preimage of \overline{H} under the natural projection homomorphism.

1.7 Normal Subgroups

Definition 1.19 An element gng^{-1} is called the conjugate of $n \in N$ by g . The set $gNg^{-1} = \{gng^{-1} | n \in N\}$ is called the conjugate of N by g . The element g is said to normalize N if $gNg^{-1} = N$.

Definition 1.20 A subgroup N of a group G is called normal if every element of G normalizes N , i.e. if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

Proposition 1.17 Let N be a subgroup of the group G . Then the following are equivalent:

- (1) $N \trianglelefteq G$.
- (2) $N_G(N) = G$.
- (3) $gN = Ng$ for all $g \in G$.
- (4) If $uN \circ vN = (uv)N$ is well defined, then the set of left cosets form a group.

Example 1.4 If $H \leq G$ and $|G : H| = 2$, then $H \trianglelefteq G$.

Proof:

If $G = H \sqcup xH = H \sqcup Hx$, So this implies that $Hx = xH \implies H = xHx^{-1}$. ★

Proposition 1.18 *A subgroup N of a group G is normal if and only if it is the kernel of some homomorphism from G to another group.*

Definition 1.21 *A nontrivial group G is said to be simple if it has no nontrivial proper normal subgroups. That is, $H \trianglelefteq G$ if and only if $H = \{1\}$ or $H = G$.*

The most common example of a simple group is A_n for $n \geq 5$. In fact, A_5 is often used to prove the simplicity of other groups.

1.8 Isomorphism Theorems

Theorem 1.7 (First Isomorphism Theorem) *If $\varphi : G \rightarrow H$ is a group homomorphism then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \varphi(G)$.*

Corrolary 1.4

- (1) φ is injective if and only if $\ker \varphi = \{1\}$.
- (2) $|G : \ker \varphi| = |\varphi(G)|$

Theorem 1.8 (Second Isomorphism Theorem) *Let G be a group and let A and B be subgroups of G and assume $A \leq N_G(B)$. Then $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.*

Theorem 1.9 (Third Isomorphism Theorem) *Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.*

Theorem 1.10 (Fourth Isomorphism Theorem) *Let G be a group and let N be a normal subgroup of G . Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\bar{A} = A/N$ of G/N . In particular, every subgroup of \bar{G} is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties for all $A, B \leq G$ with $N \leq A$ and $N \leq B$:*

- (1) $A \leq B$ if and only if $\bar{A} \leq \bar{B}$,
- (2) If $A \leq B$, then $|A : B| = |\bar{A} : \bar{B}|$,
- (3) $\overline{\langle A, B \rangle} = \langle \bar{A}, \bar{B} \rangle$
- (4) $\overline{A \cap B} = \bar{A} \cap \bar{B}$, and
- (5) $A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq \bar{G}$

1.9 Normal series

Definition 1.22 In a group G , a sequence N_0, \dots, N_n of subgroups such that

$$1 = N_0 \leq N_1 \leq \dots \leq N_k = G$$

is called a *subnormal series* if $N_i \trianglelefteq N_{i+1}$. If each N_i is normal in G , then the subnormal series is said to be *normal*.

The factors of the series are the quotient groups N_{i+1}/N_i and the length of the series is the number of strict inclusions (or, equivalently, the number of nontrivial factors). It's clear from the definition that every subnormal series is a normal series. However, the converse is only true if G is an abelian group (since all subgroups of an abelian group are normal).

Definition 1.23 Given a subnormal series

$$1 = N_0 \leq N_1 \leq \dots \leq N_k = G,$$

a *one step refinement* is a series of the form

$$1 = N_0 \leq N_1 \leq N_i \leq H \leq N_{i+1} \leq \dots \leq N_k = G$$

where $N_i \trianglelefteq H \trianglelefteq N_{i+1}$. A *refinement* is the subnormal series obtained from a finite sequence of one step refinements. The refinement is said to be *proper* if it has length larger than that of the original subnormal series.

Definition 1.24 If a subnormal series has the additional property that N_{i+1}/N_i is abelian for $0 \leq i \leq k-1$, then the series is called a *solvable series*.

Solvable series will be considered in more detail within §1.13.

Definition 1.25 If a subnormal series has the additional property that N_{i+1}/N_i is a simple group for $0 \leq i \leq k-1$, then the series is called a *composition series*.

An interesting note about composition series is the fact that if $H \trianglelefteq G$, then every normal subgroup of G/N is of the form G/K where $K \trianglelefteq G$ contains H . Accordingly, every composition series can be obtained from any subnormal series via a series of one step refinements.

Definition 1.26 A normal subgroup N of G is called *maximal* if there are no normal subgroups of G properly containing N . In particular, N is maximal in G if and only if G/N is simple.

Proposition 1.19 Every subnormal series is a composition series if and only if it has no proper refinements.

Theorem 1.11 (Schreier) Any two subnormal (or normal) series of a group G have refinements that are equivalent.

1.10 Jordan Hölder Theorem

Theorem 1.12 (Jordan Hölder) *Let G be a finite group with $G \neq 1$. Then*

- (1) G has a composition series and
- (2) The composition factors in a composition series are unique. Namely, if

$$1 = N_0 \leq N_1 \leq \cdots \leq N_r = G \quad \text{and} \quad 1 = M_0 \leq M_1 \leq \cdots \leq M_s = G$$

are two composition series for G , then $r = s$ and there is some permutation π of $\{1, 2, \dots, r\}$ such that

$$N_{i+1}/N_i \cong M_{\pi(i)+1}/M_{\pi(i)}$$

Theorem 1.13 (Feit-Thompson) *If G is a simple group of odd order, then $G \cong \mathbb{Z}_p$ for some prime p .*

1.11 Group Actions

Definition 1.27 *A group action of a group G on a set A is a map from $G \times A \rightarrow A$ (written as $g \cdot a$ for all $g \in G$ and $a \in A$) satisfying the following properties:*

- (1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G, a \in A$, and
- (2) $1 \cdot a = a$ for all $a \in A$.

Note: The group action as defined is a *left action* since the group elements appear on the left. If the elements appeared on the right then the group action would be a *right action*.

Proposition 1.20 *Let G act on the set A . For each fixed $g \in G$ we get a map $\sigma_g : A \rightarrow A$ defined by*

$$\sigma_g(a) = g \cdot a.$$

Then,

- (1) for each fixed $g \in G$, σ_g is a permutation of A , and
- (2) the map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

A FEW GOOD OBSERVATIONS

The homomorphism from $G \rightarrow S_A$ is known as the *associated permutation representation* to the given action. Observe that if $\varphi : G \rightarrow S_A$ is a homomorphism, the map from $G \times A$ to A defined by $g \cdot a = \varphi(g)(a)$ satisfies all group properties. Therefore, the process is reversible.

If G acts on a set A and $g \cdot a = a$ for all $g \in G$, then the action is said to be the *trivial action*. In particular, distinct elements of G produce the same permutation on A so the associated representation, $G \rightarrow S_A$ is the trivial homomorphism that maps every element of G to the identity.

Definition 1.28 If G acts on a set B and distinct elements of G induce distinct permutations of B , the action is said to be faithful. That is, if $g \cdot a = b$ for $a, b \in B$ such that $a \neq b$.

Accordingly, the associated permutation representation is injective.

Definition 1.29 The kernel of the action of G on B is defined to be $\{g \in G \mid g \cdot b = b \text{ for all } b \in B\}$.

Accordingly, the trivial action is not faithful if $|G| > 1$.

Definition 1.30 If G is a group acting on a set S and s is some fixed element of S , the stabilizer of s in G is the set $G_s = \{g \in G \mid g \cdot s = s\}$.

Proposition 1.21 Let G be a group acting on the nonempty set A . The relation on A is defined by

$$a \sim b \text{ if and only if } a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation.

For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a .

Definition 1.31 Let G be a group acting on the nonempty set A .

- (1) The equivalence class $\{g \cdot a \mid g \in G\}$ is called the orbit of G containing a .
- (2) The action of G on A is called transitive if there is only one orbit, i.e., given any two elements, $a, b \in A$, there is some $g \in G$ such that $a = g \cdot b$.

Example 1.5

1.11.1 Class Formula

Definition 1.32 Consider the group action on itself by conjugation, i.e. $g \cdot a = gag^{-1}$ for all $g \in G, a \in G$. Two elements a and b of G are said to be conjugate in G if there is some $g \in G$ such that $b = gag^{-1}$ (i.e. if they are in the same orbit of G)

The orbits of G acting on itself by conjugation are called the conjugacy classes of G .

Definition 1.33 Two subsets S and T of G are said to be conjugate in G if there is some $g \in G$ such that $T = gSg^{-1}$.

Recall our earlier discussion of the symmetric group. We now have the tools for the following proposition:

Proposition 1.22 Two elements of S_n are conjugate if and only if they have the same cycle type.

Proposition 1.23 The number of conjugates of a subset S in a group G is the index of the normalizer of S , $|G : N_G(S)|$. In particular, the number of conjugates of an element s in G (or equivalently, the size of orbit of s) is the index of the centralizer of s , $|G : C_G(s)|$

Theorem 1.14 (Class Equation) *Let G be a finite group and let g_1, g_2, \dots, g_r be representatives of distinct conjugacy classes of G not contained in the center of G . Then*

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

Example 1.6 *If $|G| = p^\alpha$, then $|G|$ has a nontrivial center.*

Proof:



1.11.2 Automorphisms

Definition 1.34 *Let G be a group. An isomorphism from G onto itself is called an automorphism of G . The set of all automorphisms of G is denoted by $\text{Aut}(G)$.*

One should note that $\text{Aut}(G)$ is itself a group under function composition. Additionally, if H is a normal subgroup of G , then $G/C_G(H)$ is isomorphic to a subgroup of H . This tells us that conjugate elements and conjugate subgroups have the same order.

Corollary 1.5 *For any subgroup H of a group G , the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.*

Definition 1.35 *Let G be a group and $g \in G$. Conjugation by g is called an inner automorphism of G . This subgroup of $\text{Aut}(G)$ is denoted by $\text{Inn}(G)$.*

This definition, together with the above Corollary gives us the relation,

$$\text{Inn}(G) \cong G/Z(G).$$

Additionally, if H is a normal subgroup of G , conjugation to an element of G when restricted to H is an Automorphism of H but not necessarily an inner automorphism of H .

Definition 1.36 *A subgroup H of a group G is called characteristic in G , denoted $H \text{ char } G$ if every automorphism of G maps H to itself, i.e., if $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$.*

A Few Good Observations

1. Characteristic subgroups are normal.
2. If H is the unique subgroup of a given order, then H is characteristic in G .
3. If $K \text{ char } H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$ (so although normality is not normally transitive, a characteristic subgroup of a normal group is normal).

Proposition 1.24 *If G is a cyclic group of order n , then $\text{Aut}(G) \cong (\mathbb{Z}_n)^\times$.*

Proof:



Proposition 1.25

- (1) If p is an odd prime and $n \in \mathbb{Z}^+$, then the automorphism group of the cyclic group of order p is a cyclic group of order $p - 1$. More generally, the automorphism group of a cyclic group of order p^n is equal to $p^{n-1}(p - 1)$.
- (2) For all $n \geq 3$, the automorphism group of the cyclic group of order 2^n is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$, and in particular, is not cyclic but has a cyclic subgroup of index 2.
- (3) Let p be prime and let V be an (additive) abelian group with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n -dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, namely

$$\text{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p)$$

- (4) For all $n \neq 6$, $\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n$. For $n = 6$, $|\text{Aut}(S_6) : \text{Inn}(S_6)| = 2$.
- (5) $\text{Aut}(D_4) \cong D_4$ and $\text{Aut}(Q_8) \cong S_4$.

1.12 Sylow's Theorems

Theorem 1.15 (Cauchy's Theorem) If G is a finite group, then for every prime, p dividing the order of G , there is an element of order p .

Definition 1.37 Let G be a group and let p be a prime.

- (1) If G has order p^α for some $\alpha \geq 1$ then G is called a p -group. Subgroups of G which are p -groups are called p -subgroups.
- (2) If G has order $p^\alpha m$ where $p \nmid m$, then a subgroup of order p^α is called a Sylow p -subgroup of G .

Notation: The set of Sylow p -subgroups is denoted $\text{Syl}_p(G)$ and the number of Sylow p -subgroups is denoted $n_p(G)$ (though out of laziness, the (G) is often dropped).

Theorem 1.16 (Sylow's Theorem) Let G be a group of order $p^\alpha m$ where p is a prime not dividing m . Then

- (1) Sylow p -subgroups exist;
- (2) If $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_q(G)$ for primes p and q (note: p and q may or may not be distinct), then there exists a $g \in G$ such that Q is contained in some conjugate of P , i.e. $Q \leq gPg^{-1}$
- (3) $n_p(G) \equiv 1 \pmod{p}$ and $n_p(G)$ divides $|G|$.

Note that Sylow's theorem (2) implies that if $P, Q \in \text{Syl}_p(G)$, then $P \cong Q$.

Corollary 1.6 If $P \in \text{Syl}_p(G)$ then $N_G(N_G(P)) = N_G(P)$

Corollary 1.7 Let $P \in \text{Syl}_p(G)$. Then The following are equivalent:

- (1) P is the unique Sylow p -subgroup, i.e. $n_p(G) = 1$;

(2) $P \trianglelefteq G$;

(3) P is characteristic in G

Proposition 1.26 *Let G be a group of order $p^\alpha m$ where p is a prime not dividing m . Then G contains a subgroup of order p^k for every $k \in \{0, \dots, \alpha\}$ such that every subgroup of order p^k is normal in some subgroup of order p^{k+1} .*

Lemma 1.1 *If $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_q(G)$ then $P \cap N_G(Q) = P \cap Q$.*

Proposition 1.27 *If $|G| = 60$ and G has more than one Sylow 5-subgroup, then G is simple.*

Proposition 1.28 *If G is a simple group of order 60, then $G \cong A_5$.*

1.13 Solvable Groups

Definition 1.38 *For any group, G , define the following sequences of subgroups inductively,*

$$C_{(0)} = 1 \quad C_{(1)} = Z(G)$$

and $C_{(i+1)} = C_{(i+1)}/Z_{(i)} = Z(G/C_i)$. That is C_{i+1} is the complete preimage of $Z(G/C_i)$ under the natural transformation $G \rightarrow G/C_i$. We then obtain a sequence of normal subgroups of G :

$$1 = C_0 \leq C_1 \leq C_2 \leq \dots$$

This series is called the ascending central series of G .

Definition 1.39 *A group G is called nilpotent if there exists an $n \in \mathbb{Z}$ such that $C_n = G$*

Proposition 1.29 *If H is a proper subgroup of a nilpotent group, then it has a nontrivial normalizer. In particular, $H \not\cong N_G(H)$.*

Proposition 1.30 *Every p group is nilpotent.*

Proposition 1.31 *If G is a finite nilpotent group, and if n divides the order of G , then G contains a subgroup of order n .*

Recall the definition of a solvable series (see §1.9):

Definition 1.40 *A group, G , is solvable if there is a chain of subgroups*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \dots, s-1$.

Proposition 1.32 *A finite group G is solvable if and only if it has a composition series whose factors are cyclic of prime order.*

Theorem 1.17 *A finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n .*

Definition 1.41 Let G be a group and let $x, y \in G$ and let A, B be nonempty subsets of G .

- (1) The commutator of x and y is defined $[x, y] = x^{-1}y^{-1}xy$.
- (2) The group generated by commutators of elements from A and from B is defined $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$.
- (3) The commutator (or derived) subgroup of G is defined $G' = \langle [x, y] \mid x, y \in G \rangle$.

Proposition 1.33 Let G be a group. Let $x, y \in G$ and let $H \leq G$. Then

- (1) $xy = yx[x, y]$
- (2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$.
- (3) $\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any automorphism σ of G
- (4) G' char G and G/G' is abelian
- (5) G/G' is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.
- (6) If $\phi : G \rightarrow A$ is any homomorphism of G into an abelian group A , then ϕ factors through G' , i.e. $G' \leq \ker \phi$ and the following diagram commutes:

$$\begin{array}{ccc} G & \longrightarrow & G/G' \\ & \searrow \phi' & \downarrow \\ & & A \end{array}$$

Definition 1.42 For any group, G , define the following sequences of subgroups inductively,

$$G^{(0)} = G \quad G^{(1)} = [G, G] \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad \text{for all } i \geq 1.$$

This series is called the derived or commutator series of G .

Occasionally, the terms of this series is written $G^{(0)} = G', G^{(2)} = G''$, etc. Additionally, each $G^{(i)}$ is characteristic in G . It is important to note, however, that it doesn't necessarily follow that $G^{(i)} = G^i$ for $i \geq 2$. Consider, for example, the group S_3 . $G^2 = [S_3, A_3] = A_3$, but $G^{(2)} = [A_3, A_3] = 1$.

Theorem 1.18 A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

Theorem 1.19 Let G be a finite group.

- (1) (Burnside) If $|G| = p^a q^b$ for primes p and q , then G is solvable.
- (2) (Philip Hall) If for every prime p dividing $|G|$, we factor the order of G as $|G| = p^a m$ where $(p, m) = 1$ and G has a subgroup of order m , then G is solvable.
- (3) (Feit-Thompson) If $|G|$ is odd, then G is solvable
- (4) (Thompson) If for every pair of elements, $x, y \in G$, $\langle x, y \rangle$ is a solvable group, then G is solvable.

Proposition 1.34

- (1) Every subgroup and every homomorphic image of a solvable group is solvable.
- (2) If N is a normal subgroup of a group G such that N and G/N are solvable, then G is solvable.

Theorem 1.20 For $n \geq 5$, S_n is unsolvable.

1.13.1 Solvability of p -groups

Theorem 1.21 If p is a prime and P is a group of prime power order, i.e. $|P| = p^\alpha$ for $\alpha \geq 1$, then

- (1) P has a nontrivial center.
- (2) If H is a normal nontrivial subgroup of P , then H intersects the center of P nontrivially, i.e., $H \cap z(P) \neq 1$. In particular, every normal subgroup of order p is contained in the center.
- (3) If H is a normal subgroup of P , then H contains a subgroup of order p^β that is normal in P for each divisor, p^β of $|H|$. In particular, P has a normal subgroup of order p^β for every $\beta \in \{1, \dots, \alpha\}$.
- (4) Every proper subgroup of P is a proper subgroup of its normalizer in P , i.e., if $H < P$, then $H < N_P(H)$
- (5) Every maximal subgroup of P is normal in P and of index p .

Corrolary 1.8 Every group of prime power order is solvable.

Corrolary 1.9 If $|P| = p^2$ for some prime p , then P is isomorphic to either \mathbb{Z}_{p^2} or $\mathbb{Z}_p \times \mathbb{Z}_p$.

1.14 Category Theory

Definition 1.43 A category is a class \mathcal{C} of objects together with

- (i) a class of disjoint sets, called morphisms, between the objects in \mathcal{C} . For each pair of objects A and B , $Mor_{\mathcal{C}}(A, B)$ denotes the class of morphisms between A and B ; and
- (ii) For each triple of objects A , B , and C , the morphism is a composition. In particular,

$$Mor_{\mathcal{C}}(B, C) \times Mor_{\mathcal{C}}(A, B) \rightarrow Mor_{\mathcal{C}}(A, C).$$

For any class \mathcal{C} of objects, $Mor_{\mathcal{C}}(*, *)$ is a monoid.

Definition 1.44 A category \mathcal{D} is a subcategory of \mathcal{C} if whenever an object is in \mathcal{D} , the object is in \mathcal{C} . Accordingly, for objects A, B , $Mor_{\mathcal{D}}(A, B) \subseteq Mor_{\mathcal{C}}(A, B)$.

Example 1.7 The following are examples of categories:

Category	Objects	Arrows
Set	all small sets	functions between the sets
Grp	all small groups	group homomorphisms
Ab	all small (additive) abelian groups	group homomorphisms
Rng	all small rings	ring homomorphisms
R-Mod	all small left modules over the ring R	linear maps
Top	small topological spaces	continuous maps

Definition 1.45 Two objects are said to be equivalent if there exist $f, g \in \text{Mor}_{\mathcal{C}}(A, B)$ such that $gf = 1_A$ and $fg = 1_B$

Definition 1.46 Let \mathcal{C} be a category and $\{A_i | i \in I\}$ a family of objects of \mathcal{C} . A product for the family $\{A_i | i \in I\}$ is an object P of \mathcal{C} together with a family of morphisms $\{\pi_i : P \rightarrow A_i | i \in I\}$ such that for any object B and family of morphisms $\{\varphi_i : B \rightarrow A_i | i \in I\}$, there is a unique morphism $\psi : B \rightarrow P$ such that $\pi_i \circ \psi = \varphi_i$ for all $i \in I$.

A product P is often denoted by $P = \prod A_i$. Simply stated, a Product for $\{A_1, A_2\}$ is a diagram $A_1 \xleftarrow{\pi_1} P \xrightarrow{\pi_2} A_2$ such that for any other diagram of the form $A_1 \xleftarrow{\varphi_1} B \xrightarrow{\varphi_2} A_2$, there exists a unique morphism $\psi : B \rightarrow P$ where the following diagram commutes:

$$\begin{array}{ccc}
 & B & \\
 \varphi_1 \swarrow & \downarrow \psi & \searrow \varphi_2 \\
 A_1 & \xleftarrow{\pi_1} P \xrightarrow{\pi_2} & A_2
 \end{array}$$

Note that, in general, it is not necessary for a family of objects to have a product, though, for families relevant to the qualifying exam, products always exist.

Theorem 1.22 If $\{P, \{\pi_i\}\}$ and $\{Q, \{\psi_i\}\}$ are both products of the family $\{A_i\}$, then P and Q are equivalent.

Definition 1.47 Let \mathcal{C} be a category and $\{A_i | i \in I\}$ a family of objects of \mathcal{C} . The coproduct for the family $\{A_i | i \in I\}$ is an object S of \mathcal{C} together with a family of morphisms $\{\iota_i : A_i \rightarrow S | i \in I\}$ such that for any object B and family of morphisms $\{\psi_i : A_i \rightarrow B | i \in I\}$, there is a unique morphism $\varphi : S \rightarrow B$ such that $\varphi \circ \iota_i = \psi_i$ for all $i \in I$.

The coproduct S is often denoted by $P = \coprod A_i$. Simply stated, a coproduct for $\{A_1, A_2\}$ is a diagram $A_1 \xrightarrow{\iota_1} S \xleftarrow{\iota_2} A_2$ such that for any other diagram of the form $A_1 \xrightarrow{\psi_1} B \xleftarrow{\psi_2} A_2$, there exists a unique morphism $\varphi : S \rightarrow B$ where the following diagram commutes:

$$\begin{array}{ccc}
 A_1 & \xrightarrow{\iota_1} S \xleftarrow{\iota_2} & A_2 \\
 \searrow \psi_1 & \downarrow \varphi & \swarrow \psi_2 \\
 & B &
 \end{array}$$

Theorem 1.23 If $(S, \{\iota_i\})$ and $(S', \{\kappa_i\})$ are both coproducts for the family $\{A_i\}$ of objects in a category, \mathcal{C} then S and S' are equivalent.

Definition 1.48 Let \mathcal{C} and \mathcal{D} be categories. A functor, $F : \mathcal{C} \rightarrow \mathcal{D}$ assigns to each object A in \mathcal{C} an object $F(A)$ in \mathcal{D} . A covariant functor is a functor that assigns to each morphism $f \in \text{Mor}_{\mathcal{C}}(A, B)$ a morphism $F(f) \in \text{Mor}_{\mathcal{D}}(F(A), F(B))$ such that $F(1) = 1$ and $F(fg) = F(f)F(g)$. A contravariant functor is a functor that assigns to each morphism $f \in \text{Mor}_{\mathcal{C}}(A, B)$ a morphism $F(f) \in \text{Mor}_{\mathcal{D}}(F(A), F(B))$ such that $F(1) = 1$ and $F(fg) = F(g)F(f)$.

A functor is either covariant or contravariant. Accordingly, one can think of a covariant functor as a functor and contravariant functor as a a functor with an "antimorphism."

Definition 1.49 Given two functors $F, G : \mathcal{C} \rightarrow \mathcal{D}$, a natural transformation $T : F \rightarrow G$ assigns a morphism $T_A : F(A) \rightarrow G(A)$ to each object A in \mathcal{C} such that for each morphism $f : A \rightarrow B$ in \mathcal{C} , the following diagram commutes:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ T_A \downarrow & & \downarrow T_B \\ B & \xrightarrow{G(f)} & G(B) \end{array}$$

1.15 Direct Products

Definition 1.50 The direct product $G_1 \times G_2 \times \cdots \times G_n$ of the groups G_1, G_2, \dots, G_n with the operations $\star_1, \star_2, \dots, \star_n$, respectively, is the set of n -tuples, (g_1, \dots, g_n) where $g_i \in G_i$ with the operation defined component wise:

$$(g_1, \dots, g_n) \star (h_1, \dots, h_n) = (g_1 \star_1 h_1, \dots, g_n \star_n h_n).$$

The collection of groups doesn't necessarily have to be finite.

Proposition 1.35 If G_1, \dots, G_n is a finite collection of finite groups, then the order of their direct product is $|G_1| \cdots |G_n|$. If the collection is infinite, or if G_i is infinite for any i , then the direct product is also infinite.

Proposition 1.36 Let $G_1 \times \cdots \times G_n$ be the direct product of groups G_1, \dots, G_n

- (1) For each fixed i , the set of elements of G which have the identity of G_j in the j^{th} position for all $j \neq i$, and arbitrary elements of G_i in position i , is a subgroup of G that is isomorphic to G_i , i.e.,

$$G_i \cong \{(1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}$$

If we identify G_i with this subgroup, then we find that $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

- (2) For each fixed i , define $\pi_i : G \rightarrow G_i$ by

$$\pi_i(g_1, \dots, g_n) = g_i$$

Then π_i is a surjective homomorphism such that

$$\begin{aligned} \ker \pi_i &= \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n)\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$

(3) Under the identifications in part (1), if $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then $xy = yx$

Theorem 1.24 Suppose G is a group with subgroups H and K such that

- (1) $H \cap K = 1$
- (2) H and K are normal in G .

Then $HK \cong H \times K$

Proof:

★

If H and K satisfy these conditions, it is said that H and K are complements of one another.

1.15.1 Semidirect Products

Theorem 1.25 Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. Let \cdot denote the (left) action of K on H determined by φ . Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define multiplication on G by

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

- (1) This multiplication makes G into a group with $|G| = |H||K|$
- (2) The sets $\{(h, 1) \mid h \in H\}$ and $\{(1, k) \mid k \in K\}$ are subgroups of G with

$$H \cong \{(h, 1) \mid h \in H\} \quad \text{and} \quad K \cong \{(1, k) \mid k \in K\}$$

- (3) $H \trianglelefteq G$
- (4) $H \cap K = 1$
- (5) for all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Proof:

★

Definition 1.51 The group G described in the above Theorem is referred to as the semidirect product of H and K with respect to φ . The semidirect product is usually denoted $H \rtimes_{\varphi} K$.

Proposition 1.37 Let H and K be groups and let $\varphi : K \rightarrow \text{Aut}(H)$ be a homomorphism. Then the following are equivalent:

- (1) $H \rtimes K$ and $H \times K$ agree (i.e., the identity map is a group isomorphism)
- (2) φ is the trivial homomorphism from K into $\text{Aut}(H)$
- (3) $K \trianglelefteq H \rtimes K$

Proof:

Suppose (1) holds. Then for $a, c \in H$ and $b, d \in K$

$$\begin{aligned}(a, b)(c, d) &= (ab \cdot c, bd) \\ &= (ac, bd)\end{aligned}$$

So $b \cdot c = b$ since b is arbitrary in K , φ is trivial and (2) holds.

Suppose now, (2) holds. Then

$$\begin{aligned}(a, c)(1, b)(a, c)^{-1} &= (a, c)(1, b)(c^{-1} \cdot a^{-1}, c^{-1}) \\ &= (ac \cdot 1, bc)(c^{-1} \cdot a^{-1}, c^{-1}) = (a, bc)(a^{-1}, c^{-1}) \\ &= (acb \cdot a^{-1}, bcc^{-1}) \\ &= (aa^{-1}, b) = (1, b)\end{aligned}$$

So $K \trianglelefteq H \rtimes K$.

Finally, suppose (3) holds. Then

$$\begin{aligned}(a, 1)(1, b)(a, 1)^{-1} &= (a, 1)(1, b)(a^{-1}, 1) \\ &= (a, b)(a^{-1}, 1) \\ &= (ab \cdot a^{-1}, b)\end{aligned}$$

So $ab \cdot a^{-1} = aba^{-1}b^{-1} = 1 \implies ab = ba$. So

$$\begin{aligned}(a, b)(c, d) &= (ab \cdot c, bd) \\ &= (abc b^{-1}, bd) \\ &= (ac, bd)\end{aligned}$$

So $H \rtimes K$ and $H \times K$ agree. ★

Theorem 1.26 *Suppose G is a group with subgroups H and K such that*

(1) $H \trianglelefteq G$, and

(2) $H \cap K = 1$.

Let $\varphi : K \rightarrow \text{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H . Then, $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K .

1.15.2 Fundamental Theorem of Finitely Generated Abelian Groups

Definition 1.52

(1) *A group G is finitely generated if there is a finite subgroup, A , of G such that $G = \langle A \rangle$.*

(2) For each $r \in \overline{\mathbb{Z}}^+$, let $\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of \mathbb{Z} where $\mathbb{Z}^0 = 1$. The group \mathbb{Z}^r is called a free abelian group of rank r .

Theorem 1.27 (Fundamental Theorem of Finitely Generated Abelian Groups) *Let G be a finitely generated abelian group then*

(1)

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$

for some integers r, n_1, \dots, n_s satisfying the following conditions:

(a) $r \geq 0$ and $n_j \geq 2$ for all j , and

(b) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$

(2) the above expression is unique.

Definition 1.53 *The integer r is called the free rank or Betti number of G and the integers n_j are called the invariant factors of G . The above description of G is called the invariant factor decomposition.*

If it is known that G is a finite abelian group of order n , then the Fundamental Theorem can be used to find all possibilities, up to isomorphism, for G . In particular, for the finite sequences n_1, \dots, n_s we can apply the following rules to classify G :

1. $n_j \geq 2$ for all j ,
2. $n_1 \geq n_2 \geq \cdots \geq n_s$
3. $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$ and
4. $n_1 n_2 \cdots n_s = n$

Proposition 1.38 *Let $m, n \in \mathbb{Z}^+$. Then*

(1) $\mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_{mn}$ if and only if $(m, n) = 1$.

(2) If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then $\mathbb{Z}_n \cong \mathbb{Z}_{p^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_k}}$.

Chapter 2

Rings

2.1 Introduction

Definition 2.1 A ring, R , is a set, together with two binary operations $+$ and \times , such that

(i) $(R, +)$ is an abelian group

(ii) Multiplication is associative: $(a \times b) \times c = a \times (b \times c)$ for $a, b, c \in R$

(iii) The left and right distributive laws hold: for all $a, b, c \in R$,

$$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$

Additionally,

(iv) A ring is commutative if multiplication is commutative

(v) A ring is said to have an identity if there exists $1 \in R$ such that

$$a = a \times 1 = 1 \times a \quad \text{for all } a \in R.$$

Definition 2.2 Let R be a ring. A nonzero element d of R is called a zero divisor if there exists a nonzero element b in R such that either $db = 0$ or $bd = 0$. If R is a commutative ring with identity that does not contain zero divisors then R is an integral domain.

Definition 2.3 Let S be a ring with identity, $1 \neq 0$. An element u in S is called a unit if there is some v in S such that $uv = vu = 1$. The set of units in S is denoted S^\times . If S is such that every non-zero element is a unit, then S is called a division ring (or skew field). Additionally, if S is commutative, then S is a field.

If A division ring is not commutative, then it is said to be a strictly skew field. Observe that fields do not contain zero divisors because a zero divisor cannot be a unit. Hence, a field is automatically an integral domain. However, it doesn't necessarily follow that an integral domain is a field (though there are certain conditions under which an integral domain will be a field).

Proposition 2.1 *Let a, b and c be elements of any ring with a not a zero divisor. If $ab = ac$ then either $a = 0$ or $b = c$. In particular, if a, b, c are any elements of an integral domain, and $ab = ac$ then either $a = 0$ or $b = c$.*

Proposition 2.2 *Any finite integral domain is a field.*

Proof:

Since R is finite, $R = \{0, 1, r_1, \dots, r_{n-2}\}$. Define $\varphi : R \rightarrow R$ by $r \mapsto ar$ for some (fixed) nonzero $a \in R$. Since $\varphi(x) = \varphi(y)$ implies $ax = ay$ and the cancelation laws further implies, $x = y$, φ is injective. Since $1 \in R$, there must be some $b \in R$ such that $ab = 1$. So a is a unit in R . Since a was arbitrarily chosen in R , it follows that every nonzero element is a unit so R is a field. ★

Definition 2.4 *A subring of a ring R is a subgroup of R that is additionally closed under multiplication.*

When checking to see if a subset, S , of R is a subring, it is sufficient to check that S is nonempty and closed under multiplication and subtraction.

(note: \mathbb{Z}_n cannot be a subring of \mathbb{Z} because \mathbb{Z}_n is not a subset of \mathbb{Z}).

Some Cool Rings

Quadratic Integer Ring:

Let D be a squarefree integer (like 2).

Then $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$, a subset of \mathbb{C} is the quadratic field and

$$\mathbb{Z}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$$

is the subring of $\mathbb{Q}(\sqrt{D})$ called the Quadratic Integer Ring.

Polynomial Ring:

Let R be a commutative ring with identity, then $R[x]$ is a commutative polynomial ring with 1 and The ring R , appears in $R[x]$ as the constant polynomials.

2.1.1 Left, Right and Two-sided Ideals

Definition 2.5 *Let R be a ring, let I be a subset of R and let $r \in R$.*

(1) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.

(2) A subset I of R is a left ideal of R if

(i) I is a subring of R , and

(ii) I is closed under left multiplication by elements from R , i.e. $rI \subseteq I$ for all $r \in R$.

Similarly, I is a right ideal if (i) holds and in place of (ii) one has

(ii)' I is closed under right multiplication by elements from R , i.e. $Ir \subseteq I$ for all $r \in R$.

(3) A subset I that is both a left and right ideal is called an ideal (or two-sided ideal) of R .

Proposition 2.3 *Let R be a ring and let I be an ideal of R . Then the (additive) quotient group R/I is a ring under the binary operations:*

$$(r + I) + (s + I) = (r + s) + I \quad \text{and} \quad (r + I) \times (s + I) = (rs) + I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R .

Definition 2.6 *When I is an ideal of a ring R , the ring R/I with the operations in the previous proposition is called the quotient ring of R by I .*

Definition 2.7 *Let A be any subset of the ring R .*

- (1) *Let (A) denote the smallest ideal of R containing A , called the ideal generated by A .*
- (2) *Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$, i.e. $RA = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R \text{ and } a_i \in A, n \in \mathbb{Z}^+\}$ where $RA = 0$ if $A = \emptyset$. Similarly, $AR = \{a_1r_1 + \cdots + a_nr_n \mid r_i \in R \text{ and } a_i \in A, n \in \mathbb{Z}^+\}$ and $RAR = \{r_1a_1r_1 + \cdots + r_na_nr_n \mid r_i \in R \text{ and } a_i \in A, n \in \mathbb{Z}^+\}$.*
- (3) *An ideal generated by single element is called a principal ideal.*
- (4) *An ideal generated by a finite set is called a finitely generated ideal.*

Observe that if R is commutative, then $RA = AR = RAR = (A)$.

Definition 2.8 *Let I and J be ideals of R .*

- (1) *The sum of I and J is defined as $I + J = \{a + b \mid a \in I, b \in J\}$.*
- (2) *The product of I and J , denoted IJ , is the set of all finite sums of the elements of the form ab with $a \in I$ and $b \in J$.*
- (3) *For any $n \geq 1$, define the n^{th} power of I , denoted I^n , to be the set consisting of all of the finite sums of elements of the form $a_1a_2 \cdots a_n$ with $a_i \in I$ for all $i \in \{1, \dots, n\}$. Equivalently, I^n is defined inductively by $I^n = II^{n-1}$.*

Proposition 2.4 *Let I be an ideal of R*

- (1) *$I = R$ if and only if I contains a unit*
- (2) *Assume R is commutative. Then R is a field if and only if its only ideals are $\{0\}$ and R .*

Proof:



Corollary 2.1 *If R is a field then any nontrivial ring homomorphism from R into another ring is an injection.*

Proof:

Recall that a ring homomorphism, φ , is injective if $\text{Ker}(\varphi) = \{0\}$. If φ is nontrivial, then $\text{Ker}(\varphi)$ is a proper ideal of R . Since R is a field, $\text{Ker}(\varphi) = \{0\}$, so φ is an injection. ★

Definition 2.9 *An ideal M in an arbitrary ring S is called maximal if $M \neq S$ and the only ideals containing M are M and S .*

Proposition 2.5 *In a ring with identity, every proper ideal is contained in a maximal ideal.*

Proposition 2.6 *Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.*

Proof:

★

Definition 2.10 *Let R be a commutative ring (with or without identity*). An ideal P is a prime ideal in R if $P \neq R$ and whenever $ab \in P$, at least one of a or b is an element of P .*

Proposition 2.7 *Assume R is commutative. The ideal P is a prime ideal if and only if the quotient ring R/P is an integral domain.*

Corollary 2.2 *Assume R is commutative. Every maximal ideal of R is a prime ideal.*

Proof:

If M is a maximal ideal, then R/M is a field. Since every field is an integral domain, R/M is an integral domain which implies that M is a prime ideal. ★

2.1.2 Quotients, Homomorphisms and Isomorphism theorems

Theorem 2.1 (First Isomorphism Theorem for Rings) *If $\varphi : R \rightarrow S$ is a homomorphism of rings then the kernel of φ is an ideal of R and the image of φ is a subring of S and $R/\text{ker}\varphi$ is isomorphic as a ring to $\varphi(R)$.*

If I is any ideal of R , then The map

$$R \rightarrow R/I \quad \text{defined by} \quad r \mapsto r + I$$

is a surjective ring homomorphism with kernel I (this is the natural projection map). Thus every ideal is the kernel of a ring homomorphism and vice versa.

Theorem 2.2 *Let R be a ring.*

- (1) (Second Isomorphism Theorem for Rings) *Let A be a subring and let B be an ideal of R . Then $A+B = \{a+b \mid a \in A, b \in B\}$ is a subring of R , $A \cap B$ is an ideal of A and $(A+B)/B \cong A/(A \cap B)$.*

- (2) (Third Isomorphism Theorem for Rings) *Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.*
- (3) (Fourth Isomorphism Theorem for Rings) *Let I be an ideal of R . The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings that contain I and the set of subrings of R/I . Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I .*

2.1.3 Zorn's Lemma

Definition 2.11 *A partial order on a nonempty set A is a relation \preceq on A satisfying the following properties:*

- (i) (Reflexivity) $x \preceq x$ for all $x \in A$
- (ii) (Antisymmetry) If $x \preceq y$ and $y \preceq x$ then $x = y$ for all $x, y \in A$
- (iii) (Transitivity) If $x \preceq y$ and $y \preceq z$, then $x \preceq z$.

Definition 2.12 *Let the nonempty set A be partially ordered by \preceq*

- (1) *A subset B of A is called a chain (totally ordered set or tower) if for all $x, y \in B$, either $x \preceq y$ or $y \preceq x$.*
- (2) *A upper bound for a subset B of A is an element $u \in A$ such that $b \preceq u$ for all $b \in B$*
- (3) *A maximal element, m , of A is any element such that for all $x \in A$, if $m \preceq x$, then $m = x$.*

Lemma 2.1 (Zorn's Lemma) *If A is a nonempty partially ordered set in which every chain has an upper bound, then A has a maximal element.*

Theorem 2.3 *The following are equivalent:*

- (1) *Zorn's Lemma*
- (2) *Well Ordering Principle*
- (3) *Axiom of Choice*

2.1.4 Rings of Fractions and Quotient Fields

Theorem 2.4 *Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0 or zero divisors and is closed under multiplication. Then there is a commutative ring, Q with 1, such that Q contains R as a subring and every element of D is a unit in Q . The ring Q has the following additional properties:*

- (1) *every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$, then Q is a field.*
- (2) (uniqueness) *Q is the "smallest" ring containing R in which all of the elements of D become units. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q .*

Definition 2.13 Let R, D , and Q be as in the above Theorem

- (1) The ring Q is called the ring of fractions or quotient ring of D with respect to R and is denoted $D^{-1}R$.
- (2) If R is an integral domain and $D = R - \{0\}$, then Q is called the field of fractions or quotient field of R .

Corollary 2.3 Let R be an integral domain and Q the quotient field of R . If a field \mathbb{F} contains a subring R' isomorphic to R , then the subfield of \mathbb{F} generated by R' is isomorphic to Q .

To get an idea of Quotient Fields, lets look at an example:

Suppose $R = \mathbb{Z}$. This tells us that $F = \mathbb{Q}$. If $p(x), q(x) \in \mathbb{Q}[x]$, then for some integer, N , where N is the common denominator for all the coefficients in $p(x)$ and $q(x)$ (for example), $Np(x)$ and $Nq(x)$ have integer coefficients. Then $\frac{p(x)}{q(x)} = \frac{Np(x)}{Nq(x)}$ can be written as the quotient of two polynomials with integer coefficients. Hence, the quotient field of $\mathbb{Q}[x]$ is the same as the quotient field of $\mathbb{Z}[x]$.

2.1.5 Chinese Remainder Theorem

Definition 2.14 The ideals A and B of the ring R are said to be comaximal if $A + B = R$

Recall that the product, AB , is defined as the ideal consisting of all of the finite sums of the elements xy where $x \in A$ and $y \in B$. So if $A = (a)$ and $B = (b)$ then $AB = (ab)$. More generally, the product of ideals A_1, \dots, A_k would be the finite sums of elements $x_1 \cdots x_k$ where $x_i \in A_i$ for each $i \in \{1, \dots, k\}$. So, if $A_i = (a_i)$, then $\prod_{i=1}^k A_i = (a_1 \cdots a_k)$

Proposition 2.8 Assume R is a commutative ring. If the ideals I and J of R are comaximal, then $IJ = I \cap J$.

Proof:

★

Theorem 2.5 (Chinese Remainder Theorem) Let A_1, \dots, A_k be ideals of R . Then the map

$$R \rightarrow R/A_1 \times \cdots \times R/A_k \quad \text{defined by} \quad r \mapsto (r + A_1, \dots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap \cdots \cap A_k$. If for each $i, j \in \{1, \dots, k\}$, where $i \neq j$, the ideals A_i and A_j are comaximal, then the map is surjective and $A_1 \cap \cdots \cap A_k = \prod_{i=1}^k A_i$, so

$$R/(A_1 \cdots A_k) = R/(A_1 \cap \cdots \cap A_k) \cong R/A_1 \times \cdots \times R/A_k.$$

Corollary 2.4 Let $n \in \mathbb{Z}^+$ and let $p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ be its prime factorization. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_t^{\alpha_t}\mathbb{Z})$$

as rings, so in particular, there is an isomorphism of the multiplicative groups

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_t^{\alpha_t}\mathbb{Z})^\times$$

In considering the orders of these groups, we obtain the Euler-phi formula discussed in the preliminaries section of these notes.

2.1.6 Euclidian Domains

Definition 2.15 Let R be an integral domain.

Any function $N : R \rightarrow \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a norm on R . If $N(a) > 0$ for $a \neq 0$ then N is defined to be a positive norm.

Definition 2.16 The integral domain R is said to a Euclidean Domain (or possess a Division Algorithm) if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$, there exist elements $r, q \in R$ such that

$$a = qb + r \quad \text{with} \quad r = 0 \text{ or } N(r) < N(b)$$

The element q is called the quotient and the element r the remainder.

Proposition 2.9 Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R , then $I = (a)$, where a is any nonzero element of I of minimum norm.

Proof:

Let I be any nonzero ideal of R .

Define a total linear ordering on the set $S = \{N(\alpha) \mid \alpha \in I\}$. By the Well Ordering Principle, S has a minimal element, a . Since $d \in I$, $(a) \subseteq I$.

Conversely, suppose b is any element of I , since R is a Euclidean Domain, there exist elements r and q such that $b = qa + r$ with $r = 0$ or $N(r) \leq N(a)$. Since a has minimal norm, $r = 0$ and $b = qa$. This implies that $b \in (a)$ so $I \subseteq (a)$. Hence, $I = (a)$. ★

Definition 2.17 Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

(1) a is said to be a multiple of b if there is an element $x \in R$ such that $a = xb$. In this case, it is said that b divides a (i.e., $b \mid a$).

(2) A greatest common divisor of a and b (written (a, b)) is a nonzero element such that

(i) $d \mid a$ and $d \mid b$

(ii) If $d' \mid a$ and $d' \mid b$, then $d' \mid d$

Proposition 2.10 If a and b are nonzero elements in the commutative ring R such that the ideals generated by a and b is a principal ideal (d) , then d is the greatest common divisor of a and b .

Proposition 2.11 Let R be an integral domain. If two elements d and d' of R generated the same principal ideal, i.e. $(d) = (d')$, then $d' = ud$ for some unit $u \in R$. In particular, if d and d' are both greatest common divisors of a and b , then $d' = ud$ for some unit, u .

Theorem 2.6 Let R be a Euclidean Domain and let a and b be nonzero elements of R . Then if d is the greatest common divisor of a and b , the principal ideal (d) is the ideal generated by a and b . In particular, d can be written as an R -linear combination of a and b , i.e., there are elements $s, t \in R$ such that

$$d = sa + bt$$

Definition 2.18 Let $\tilde{R} = R^\times \cup \{0\}$ denote the collection of units of R together with 0. If, given an element $u \in R - \tilde{R}$, there is some $z \in \tilde{R}$ such that $u|(x - z)$ in R for every $x \in R$, then u is said to be a universal side divisor. In particular, every $x \in R$ can be written as $x = qu + z$ where $q \in R$ and z is a unit or zero.

Proposition 2.12 Let R be an integral domain that is not a field (i.e. there exists an $a \in R$ such that a is not a unit). If R is a Euclidean domain, then there are universal side divisors in R .

Consider the following example:

Proposition 2.13 $\mathbb{Z}[\sqrt{-5}]$ is not a Euclidean Domain.

Proof:

★

2.1.7 Principal Ideal Domains (PIDs) and Unique Factorization Domains (UFDs)

Definition 2.19 A Principal Ideal Domain (PID) is an integral domain in which every ideal is principal.

Since every ideal in a Euclidean Domain is principal, it follows that every Euclidean Domain is a PID.

Proposition 2.14 Let R be a PID and let a and b be nonzero elements of R . Let d be a generator for the principal ideal generated by a and b . Then

- (1) d is a greatest common divisor for a and b
- (2) d can be written as an R -linear combination of a and b , i.e. there are elements $x, y \in R$ such that

$$ax + by = d$$

Proposition 2.15 Every nonzero prime ideal in a PID is a maximal ideal

Proof:

Let (p) be a nonzero prime ideal in the PID, R . Since every ideal is contained in some maximal (proper) ideal, there is a maximal ideal $M = (m)$ (since R is a PID) such that $(p) \subseteq (m)$. So, $p \in (m) \Rightarrow p = rm$ for some $r \in R$. Since (p) is a prime ideal, $rm \in (p)$ so at least one of r or m lies in (p) .

If $m \in (p)$, then $(m) = (p)$, so (p) is maximal. If $r \in (p)$ and $m \notin (p)$, then $r = pt$ for some $t \in R$. Then $p = rm = ptm \Rightarrow tm = 1 \Rightarrow m$ is a unit which contradicts the fact that (m) is a proper ideal. So $(p) = (m)$ and (p) is maximal. ★

Corrolary 2.5 If R is any commutative ring such that the polynomial ring $R[x]$ is a PID (or Euclidean Domain), then R is necessarily a field.

Definition 2.20 Define N to be a Dedekind-Hasse norm if N is a positive norm and for every nonzero $a, b \in R$, either a is an element of (b) or there is a nonzero element in the ideal (a, b) of norm strictly smaller than the norm of b (i.e., either b divides a in R or there exist $s, t \in R$ such that $0 < N(sa - tb) < N(b)$).

Proposition 2.16 *The integral domain R is a PID if and only if R has a Dedekind-Hasse norm.*

Definition 2.21 *Let R be an integral domain.*

- (1) *Suppose $r \in R$ is nonzero and is not a unit. Then r is called irreducible in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R . Otherwise, r is said to be reducible.*
- (2) *The nonzero element $p \in R$ is called prime in R if the ideal (p) generated by p is a prime ideal. In other words, a nonzero element p is prime if it is not a unit and whenever $p|ab$ for any $a, b \in R$, then either $p|a$ or $p|b$.*
- (3) *Two elements a and b of R differing by a unit are said to be associate in R (i.e. $a = ub$ for some unit u in R).*

Proposition 2.17 *In an integral domain, a prime element is always irreducible*

Proof:

Suppose (p) is a nonzero prime ideal and $p = ab$. Then $ab = p \in (p)$, so by definition of a prime ideal, either $a \in (p)$ or $b \in (p)$. Therefore, $a = pr$ for some $r \in R$. This implies that $p = ab = prb \Rightarrow rb = 1 \Rightarrow b$ is a unit. Therefore, p is irreducible. ★

Proposition 2.18 *In a PID, a nonzero element is a prime if and only if it is irreducible*

Definition 2.22 *A Unique Factorization Domain (UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:*

- (i) *r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 \cdots p_m$ and*
- (ii) *The decomposition in (i) is unique up to associates. Namely, if $r = q_1 \cdots q_n$ is another factorization of r , then $m = n$ and there is some renumbering of the factors so that p_i is associated to q_i for $i = 1, \dots, m$.*

Theorem 2.7 *Every PID is a UFD and therefore Every Euclidian Domain is a UFD*

Note that every UFD is not necessarily a PID, but UFDs and PIDs share certain properties. One such property is the following:

Proposition 2.19 *In a UFD, a nonzero element is prime if and only if it is irreducible*

Corrolary 2.6 *The integers, \mathbb{Z} are a UFD*

Corrolary 2.7 *Let R be a PID. Then there exists a multiplicative Dedekind-Hasse norm on R .*

A REALLY GOOD OBSERVATION:

$$\text{Field} \subset \text{Euclidean Domain} \subset \text{PID} \subset \text{UFD} \subset \text{Integral Domain}$$

2.1.8 Polynomial rings

Definition 2.23 Let R be a ring. A polynomial ring, $R[x]$ is the set of all polynomials $f(x)$ with coefficients in R such that $f(x)$ is expressed as a formal sum, i.e.,

$$f(x) = \sum_{i=0}^{\infty} a_i x^i.$$

Proposition 2.20 Let R be an integral domain and $p(x), q(x)$ nonzero elements of $R[x]$. Then

- (i) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$
- (ii) The units of $R[x]$ are just the units of R
- (iii) $R[x]$ is an integral domain.

Proposition 2.21 Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I). Then

$$R[x]/(I) \cong (R/I)[x]$$

In particular, if I is a prime ideal of R , then (I) is a prime ideal of $R[x]$.

Note that, however, that if I is maximal in R , it is not the case that (I) is maximal in $R[x]$. In fact, if I is maximal in R , then (I, x) is maximal in $R[x]$.

Definition 2.24 The polynomial ring in the variables x_1, \dots, x_n with coefficients in R , denoted by $R[x_1, \dots, x_n]$ is defined inductively by

$$R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$$

Theorem 2.8 R is a UFD if and only if $R[x]$ is a UFD.

Corollary 2.8 If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

Proof:

If there are finitely many variables, then the Corollary follows by the above theorem, since a polynomial ring of n variables can be considered as a polynomial ring in one variable with coefficients in a polynomial ring in $n - 1$ variables. If there are infinitely many variables, then the polynomial ring is defined as the arbitrary union of polynomial rings in k_i variables so again, the Corollary follows. ★

2.1.9 Gauss' Lemma

Proposition 2.22 (Gauss' Lemma) Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Corollary 2.9 Let R be a UFD, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

2.1.10 Factorization

Lemma 2.2 *The prime number $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

Proposition 2.23 (1) *(Fermat's Theorem on sums of squares) The prime p is the sum of two integer squares, i.e., $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$. With the exception of interchanging $\pm a$ and $\pm b$, the expression of p as a sum of two squares is unique.*

(2) *The irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ are as follows:*

- (a) $1 + i$ (which has norm 2)
- (b) the primes $p \in \mathbb{Z}$ where $p \equiv 3 \pmod{4}$ (which have norm p^2), and
- (c) $a \pm bi$, the distinct irreducible factors of $p = a^2 + b^2 = (a + bi)(a - bi)$ for the primes $p \in \mathbb{Z}$ with $p \equiv 1 \pmod{4}$ (both of which have norm p).

Theorem 2.9 *Let \mathbb{F} be a field and let $f(x) \in \mathbb{F}[x]$. An element $a \in \mathbb{F}$ is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$ in $\mathbb{F}[x]$.*

Corollary 2.10 *A nonzero polynomial $f(x) \in \mathbb{F}[x]$ of degree n can have at most n zeros of \mathbb{F} .*

Definition 2.25 *A nonconstant polynomial $f(x) \in \mathbb{F}[x]$ is irreducible over \mathbb{F} if it cannot be expressed as a product $g(x)h(x)$ for any $g(x), h(x) \in \mathbb{F}[x]$.*

Theorem 2.10 *Let $f(x) \in \mathbb{F}[x]$ such that $\deg(f(x)) = 2$ or 3 . Then $f(x)$ is reducible over \mathbb{F} if and only if it has a zero in \mathbb{F} .*

Proposition 2.24 *Let $p(x) \in \mathbb{Z}[x]$ be a polynomial of degree n . If $r/s \in \mathbb{Q}$, is in lowest terms (i.e., $(r, s) = 1$), and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$. In particular, if $p(x)$ is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in \mathbb{Q} .*

In Pre-calculus, this theorem was known as the Rational Roots Theorem.

Proposition 2.25 *Let I be any proper ideal of the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ is irreducible, then $p(x)$ is irreducible in $R[x]$.*

Note that, in general, the converse is not true. For example, consider $p(x) = x^2 + 4x + 5$ in $\mathbb{Z}[x]$. In $\mathbb{Z}_2[x]$, $p(x) \equiv x^2 + 1 \pmod{2}$ which is irreducible.

Proposition 2.26 (Eisenstein's Criterion) *Let P be a prime ideal of the integral domain R and let $f(x) \in R[x]$ be a monic polynomial of degree $n \geq 1$. Suppose $a_i \in P$ for $i \in \{0, \dots, n-1\}$ and $a_0 \notin P^2$. Then, $f(x)$ is irreducible in $R[x]$.*

Corollary 2.11 (Eisenstein's Criterion for $\mathbb{Z}[x]$) *Let p be a prime in \mathbb{Z} and let $f(x) \in \mathbb{Z}[x]$ be monic of degree $n \geq 1$. Then if $p|a_i$ for all $i \in \{0, \dots, n-1\}$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.*

Proposition 2.27 *The maximal ideals of $\mathbb{F}[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $\mathbb{F}[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible over \mathbb{F} .*

Proposition 2.28 *Let $g(x)$ be a nonconstant element of $\mathbb{F}[x]$. Then*

$$\mathbb{F}[x]/(g(x)) \cong \prod_{i=1}^k \mathbb{F}[x]/(f_i(x)^{n_i})$$

where each $f_i(x)^{n_i}$ is irreducible in $\mathbb{F}[x]$.

Corrolary 2.12 *Every polynomial $f(x) \in \mathbb{F}[x]$ can be written as a product of irreducibles.*

Corrolary 2.13 *If G is a finite multiplicative subgroup of the multiplicative group \mathbb{F}^\times , then G is cyclic. In particular, the multiplicative group of nonzero elements of a finite field is cyclic.*

2.1.11 Simple rings

Definition 2.26 *A nonzero ring R is simple if the zero ideal is maximal.*

Note that every commutative simple ring is a field and every simple ring is a prime ring.

proof that a matrix ring over a division ring is simple.

Lang 656

2.1.12 Artinian and Noetherian Rings

Definition 2.27 *A commutative ring is said to be Noetherian (or satisfies the ascending chain condition (ACC) on ideals) if there is no infinite increasing chain of ideals in R , i.e., whenever $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ is an ascending chain of ideals, there exists an $n \in \mathbb{Z}^+$ such that $I_m = I_n$ for all $m \geq n$.*

Proposition 2.29 *If I is an ideal of a Noetherian ring R , then R/I is a Noetherian ring.*

Proof:

★

It follows from the first isomorphism theorem that any homomorphic image of a Noetherian ring is Noetherian.

Proposition 2.30 *$\mathbb{Z}[\sqrt{-5}]$ is Noetherian.*

Proof:

★

Theorem 2.11 *TFAE:*

- (1) *R is a Noetherian Ring*
- (2) *Every nonempty set of ideals of R contains a maximal element under inclusion*
- (3) *Every ideal of R is finitely generated.*

It is important to note that by condition (3), every PID is Noetherian. In particular, $\mathbb{F}[x_1, \dots, x_n]$ is Noetherian, while $\mathbb{F}[x_1, x_2, \dots]$ is not (since the ideal (x_1, x_2, \dots) cannot be finitely generated).

Definition 2.28 For any commutative ring R , the Krull dimension (or simply dimension) of R is the maximum possible length of a chain $P_0 \subset P_1 \subset \dots$ of distinct prime ideals in R . The dimension of R is said to be infinite if R has arbitrary long chains of distinct prime ideals.

Definition 2.29 The Jacobson radical of R is the intersection of all maximal ideals of R and is denoted by $\text{Jac } R$

Definition 2.30 A commutative ring R is said to be Artinian (or satisfy the descending chain condition (DCC) on ideals) if there is no infinite decreasing chain of ideals in R , i.e. whenever $I_1 \subseteq I_2 \subseteq \dots$ is a decreasing chain of ideals, there exists a $k \in \mathbb{Z}^+$ such that $I_k = I_j$ for all $j \geq k$. Similarly, an R -module, M is said to be Artinian if it satisfies the DCC on submodules.

Theorem 2.12 Let R be an Artinian Ring.

- (1) There are only finitely many maximal ideals in R .
- (2) The quotient $R/(\text{Jac } R)$ is a direct product of a finite number of fields. More precisely, if M_1, \dots, M_n are the finitely many maximal ideals in R , then

$$R/(\text{Jac } R) \cong \mathbb{F}_1 \times \dots \times \mathbb{F}_n$$

where \mathbb{F}_i is the field R/M_i for $1 \leq i \leq n$.

- (3) Every prime ideal of R is maximal, i.e. the R has Krull dimension 0. The Jacobson radical of R equals the nilradical of R and is a nilpotent ideal, i.e. $(\text{Jac } R)^n = 0$ for some $n \geq 1$
- (4) The ring R is isomorphic to the direct product of a finite number of Artinian local rings
- (5) Every Artinian Ring is Noetherian

It is not necessary for a Noetherian to be Artinian. For example, \mathbb{Z} has the infinite descending chain $(2) \subseteq (4) \subseteq \dots$

Corollary 2.14 The ring R is Artinian if and only if R is Noetherian with Krull dimension 0.

2.2 Wedderburn's theorem for simple Artinian rings

Theorem 2.13 A simple Artinian ring R is isomorphic to the $n \times n$ matrix over a division ring Δ . It then follows that $Z(\Delta) = \mathbb{F}$ for some field. Hence, R is an \mathbb{F} -algebra with $Z(R) = \mathbb{F}$.

2.3 Hilbert Basis Theorem

Theorem 2.14 (Hilbert Basis Theorem) If R is a Noetherian ring then so is the polynomial ring $R[x]$.

Corollary 2.15 The polynomial ring $\mathbb{F}[x_1, x_2, \dots, x_n]$ with coefficients in a field \mathbb{F} , is a Noetherian ring.

2.4 Localization

multiplicative sets; (Lang) 15.4 Dummit

2.5 Local rings

Chapter 3

Modules

3.1 Elementary Module Theory

Definition 3.1 Let R be a ring (not necessarily commutative nor with 1). A left R -module is a set M together with

- (1) A binary operation $+$ on M under which M is an abelian group, and
- (2) A map $R \times M \rightarrow M$ defined by $(r, m) \mapsto rm$ for all $r \in R$ and for all $m \in M$ which satisfies
 - (i) $(r + s)m = rm + sm$, for all $r, s \in R$, $m \in M$
 - (ii) $(rs)m = r(sm)$, for all $r, s \in R$, $m \in M$, and
 - (iii) $r(m + n) = rm + rn$ for all $r \in R$, $m, n \in M$.

Additionally, if the ring R has a 1,

- (iv) $1m = m$ for all $m \in M$.

When R is a field \mathbb{F} , the axioms for an R -module are exactly the same for a vector space over \mathbb{F} . In other words, modules over a field \mathbb{F} and vector spaces over \mathbb{F} are the same.

Definition 3.2 Let R be a ring and let M be an R -module. An R -submodule of M is a subgroup N of M which is closed under the action of ring elements, i.e., $rn \in N$ for all $r \in R$, $n \in N$.

It is easy to see from these definitions that \mathbb{Z} -modules are the same as abelian groups and \mathbb{Z} -submodules are the same as subgroups.

Proposition 3.1 (Submodule Criterion) Let R be a ring and let M be an R -module. A subset N of M is a submodule of M if and only if

- (1) $N \neq \emptyset$ and
- (2) $x + ry \in N$ for all $r \in R$ and $x, y \in N$

Proof:

Suppose first that N is a submodule of M . Then $0 \in N$ so condition (1) is satisfied. Additionally, for $r \in R$, $y \in N$, $ry \in N$ and, since N is a subgroup of $(M, +)$, if $x \in N$ as well, then $x + ry \in N$.

Conversely, suppose that the two conditions are satisfied. Also suppose that $x, y \in N$ (such elements exist by (1)) and $r \in R$. If $r = -1$, then by (2), $x + ry = x + (-1)y = x - y \in N$. By the subgroup criterion (Proposition 2.1), N is a subgroup of M and $0 \in N$. If $x = 0$ (with y, r arbitrary), then by (2), $x + ry = 0 + ry = ry \in N$. So N is closed under the action of ring elements. Hence, N is a submodule of M . ★

Definition 3.3 Let R be a commutative ring with identity. An R -algebra (or Algebra over R) is a ring A such that:

- (1) $(A, +)$ is a unitary R -module
- (2) $k(ab) = a(kb)$ for all $k \in K$, $a, b \in A$

If, as a ring, an R -Algebra is a division ring, then A is called a division algebra.

Definition 3.4 Let R be a ring and let M and N be R -Modules,

- (1) A map $\varphi : M \rightarrow N$ is an R -module homomorphism if it respects the R -module structures of M and N , i.e.
 - (i) $\varphi(x + y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$ and
 - (ii) $\varphi(rx) = r\varphi(x)$ for all $r \in R$, $x \in M$
- (2) Let M and N be R -modules. $\text{Hom}_R(M, N)$ is the set of all R -module homomorphisms from M into N .
- (3) $\text{Hom}_R(M, M)$ is called the endomorphism ring of M and is denoted by $\text{End}_R(M)$. The elements of $\text{End}_R(M)$ are called endomorphisms.

Proposition 3.2 Let M, N and L be R -modules.

- (1) A map $\varphi : M \rightarrow N$ is an R -module homomorphism if and only if

$$\varphi(rx + y) = r\varphi(x) + \varphi(y) \quad \text{for all } x, y \in M \text{ and } r \in R$$

- (2) Let $\varphi, \psi \in \text{Hom}_R(M, N)$. define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \quad \text{for all } m \in M$$

Then $\varphi + \psi \in \text{Hom}_R(M, N)$ and with this operation $\text{Hom}_R(M, N)$ is an abelian group.

If R is a commutative ring, then for $r \in R$, define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m)) \quad \text{for all } m \in M$$

Then $r\varphi \in \text{Hom}_R(M, N)$ and $\text{Hom}_R(M, N)$ is additionally an R -module.

- (3) If $\varphi \in \text{Hom}_R(L, M)$ and $\psi \in \text{Hom}_R(M, N)$ then $\varphi \circ \psi \in \text{Hom}_R(L, N)$
- (4) With addition as above and multiplication defined as function composition, $\text{Hom}_R(M, M)$ is a ring with 1. When R is commutative, $\text{Hom}_R(M, M)$ is an R -algebra.

3.1.1 Quotients and Isomorphism Theorems

Proposition 3.3 *Let R be a ring, let M be an R -module and let N be a submodule of M . The (additive, abelian) quotient group M/N can be made into an R Module by defining an action of elements of R by*

$$r(x + N) = rx + N \quad \text{for all } r \in R, x + N \in M/N$$

The natural projection map $\pi : M \rightarrow M/N$ defined by $\pi(x) = x + N$ is an R -module homomorphism with kernel N .

Definition 3.5 *Let A, B be submodules of the R -module M . The sum of A and B is the set*

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

Theorem 3.1 First Isomorphism Theorem *Let M, N be R -modules and let $\varphi : M \rightarrow N$ be an R -module homomorphism. Then $\ker \varphi$ is a submodule of M and $M/\ker \varphi \cong \varphi(M)$.*

Second Isomorphism Theorem *Let A and B be submodules of the R -module M , then $(A + B)/B \cong A/(A \cap B)$.*

Third Isomorphism Theorem *Let M be an R -module and let A and B be submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong (M/B)$.*

Fourth (Lattice) Isomorphism Theorem *Let N be a submodule of the R -module M . There is a bijection between the submodules of M which contain N and the submodules of M/N .*

3.1.2 Direct sums (internal and external) and Free Modules

Definition 3.6 *Let A be an R -module and let B be a submodule of A . B is said to be a direct summand of A if there exists a submodule C of A such that $A = B \oplus C$.*

Definition 3.7 *Let M be an R -module and let N_1, \dots, N_k be submodules of M .*

- (1) *The sum of N_1, \dots, N_k is the set of all finite sums of elements from the sets $N_i = \{a_1 + \dots + a_k | a_i \in N_i \text{ for all } i\}$*
- (2) *For any subset A of M , let*

$$RA = \{r_1 a_1 + \dots + r_n a_n \mid r_1, \dots, r_n \in R, a_1, \dots, a_n \in A, n \in \mathbb{Z}^+\}$$

(where the convention is $RA = \{0\}$ if $A = \emptyset$. If A is a finite set, i.e., $A = \{a_1, \dots, a_n\}$ then $RA = Ra_1 + \dots + Ra_n$. RA is then the submodule of M generated by A . If N is a submodule of M and $N = RA$ for some subset A of M , then A is the set of generators (or generating set) of N .

- (3) *A submodule N of M is finitely generated if there is some finite subset A of M such that $N = RA$*
- (4) *A submodule N of M is cyclic if there is an element $a \in M$ such that $N = Ra$, i.e. $N = Ra = \{ra \mid r \in R\}$.*

Theorem 3.2 For any set A , there is a free R -module, $F(A)$ on the set A and $F(A)$ satisfies the following universal property: if M is any R -module and $\varphi : A \rightarrow M$ is any map of sets, then there is a unique R -module homomorphism $\Phi : F(A) \rightarrow M$ such that $\Phi(a) = \varphi(a)$, for all $a \in A$, that is, the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\text{incl.}} & F(A) \\ & \searrow \varphi & \downarrow \Phi \\ & & M \end{array}$$

Corrolary 3.1 Suppose A is a subset of an R -module.

- (1) If F_1 and F_2 are free modules on the same set A , there is a unique isomorphism between F_1 and F_2 . which is the identity map on A .
- (2) If F is any free R -module with basis A , then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ enjoys in the above theorem.

3.2 Tensor products

somewhere in here: Extension of scalars (base change)

Definition 3.8 Let M be a right R -module and N be a left R -module. Let F be the free abelian group on the set $M \times N$ and let K be the subgroup of F generated by all elements of the form

$$\begin{aligned} (m_1 + m_2, n) - (m_1, n) - (m_2, n), \\ (m, n_1 + n_2) - (m, n_1) - (m, n_2) \quad \text{and} \\ (mr, n) - (m, nr) \end{aligned}$$

The quotient group F/K is called the tensor product of M and N and is denoted $M \otimes_R N$. The coset $(m, n) + K$ of the element (m, n) in F is called a tensor and is denoted $m \otimes n$.

If for each $m_1, m_2, m \in M$, $n_1, n_2, n \in N$ and $r, r_i \in R$, the following relations are satisfied in the tensor product:

$$\begin{aligned} \varphi(m_1 + m_2, n) &= m_1 \otimes n + m_2 \otimes n, \\ m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2, \quad \text{and} \\ m \otimes rn &= rm \otimes n \end{aligned}$$

Definition 3.9 Let M be a right R -module, N be a left R -module, and L an abelian group. A map $\varphi : M \times N \rightarrow L$ is called R -balanced (or middle linear) if the following relations hold:

$$\begin{aligned} \varphi(m_1 + m_2, n) &= \varphi(m_1, n) + \varphi(m_2, n), \\ \varphi(m, n_1 + n_2) &= \varphi(m, n_1) + \varphi(m, n_2), \quad \text{and} \\ \varphi(m, rn) &= \varphi(mr, n) \end{aligned}$$

for all $m_1, m_2, m \in M$, $n_1, n_2, n \in N$ and $r \in R$

Definition 3.10 Let R be a commutative ring with 1 and M, N and L be a left R -modules. A map $\varphi : M \times N \rightarrow L$ is called R -bilinear if the following relations hold:

$$\begin{aligned}\varphi(r_1m_1 + r_2m_2, n) &= r_1\varphi(m_1, n) + r_2\varphi(m_2, n), \\ \varphi(m, r_1n_1 + r_2n_2) &= r_1\varphi(m, n_1) + r_2\varphi(m, n_2), \quad \text{and} \\ \varphi(m, rn) &= \varphi(rm, n) = r\varphi(m, n)\end{aligned}$$

for all $m_1, m_2, m \in M$, $n_1, n_2, n \in N$ and $r_1, r_2 \in R$

Definition 3.11 Let R and S be rings with 1. An abelian group M is called an (S, R) bimodule if M is a left S -module and a right R -module such that $s(mr) = (sm)r$ for all $s \in S$, $r \in R$ and $m \in M$

Definition 3.12 Let M be an R -module over the commutative ring R . If, for $m \in M$, $r \in R$, $rm = mr$, then M is said to possess the Standard R -module structure

Theorem 3.3 Suppose R is a ring with 1, M a right R -module and N a left R -module. Let $\iota : M \times N \rightarrow M \otimes_R N$ be an R -balanced map. Then the following conditions hold:

- (1) If L is any abelian group and $\Phi : M \otimes_R N \rightarrow L$ is any group homomorphism, then the composite map $\phi = \Phi \iota$ is an R -balanced map.
1. Conversely, if $\phi : M \times N \rightarrow L$ is an R -balanced map, then there is a unique homomorphism $M \otimes_R N \rightarrow L$ such that $\phi = \Phi \iota$.

Corrolary 3.2 Suppose R is a commutative ring, and M and N two left R -modules. If M is given the Standard R -module structure, then $M \otimes_R N$ is a left R -module with

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

and the map $\iota : M \times N \rightarrow M \otimes_R N$ with $\iota(m, n) = m \otimes n$ is an R -bilinear map. If L is any left R -module, then there is a bijection between the set of R -bilinear maps $M \times N \rightarrow L$ and the set of R -module homomorphisms $M \otimes_R N \rightarrow L$.

From now on, if M is a left R -module, then we will write ${}_R M$. Similarly, if M is a right R -module, then it will be written M_S . If M is an (R, S) -bimodule, then it will be written ${}_R M_S$.

Theorem 3.4 If R is a ring with identity and ${}_R M$ and N_R are unitary modules, then there are R -module homomorphisms

$$N \otimes_R R \cong N \quad \text{and} \quad R \otimes_R M \cong M.$$

Theorem 3.5

Theorem 3.6 If R and S are rings with modules M_S , ${}_R N_S$ and ${}_R L$, then there is an isomorphism

$$(M \otimes_S N) \otimes_R L \cong M \otimes_S (N \otimes_R L).$$

Theorem 3.7

Corrolary 3.3

Corrolary 3.4

Proposition 3.4 *Suppose R is a commutative ring and M and N are left R -module, consider with the standard R -module structure. then there is a unique R -module isomorphism*

$$M \otimes_R N \cong N \otimes_R M$$

mapping $m \otimes n$ to $n \otimes m$.

Proposition 3.5 *Let R be a commutative ring and let A and B be R -algebras. Then the multiplication $(a \otimes b)(c \otimes d) = ac \otimes bd$ is well defined and $A \otimes_R B$ becomes an R -algebra.*

3.3 Exact Sequences

Definition 3.13 *A pair of homomorphisms $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is said to be exact if $Im(\alpha) = Ker(\beta)$. A finite sequence $\star \star \star \star \cdots \star$ is an exact sequence if $Im(\alpha_i) = Ker(\alpha_{i+1})$ for each $i \in \{1, \dots, m-1\}$*

Proposition 3.6 1. *The sequence is exact if and only if*

2. *The sequence is exact if and only if*

Corrolary 3.5 *The sequence*

$$0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \longrightarrow 0$$

is exact if and only if ψ is injective, φ is surjective and $Im(\psi) = Ker(\varphi)$. In this case, we call the sequence a short exact sequence.

Definition 3.14 *Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ and $0 \rightarrow A' \rightarrow B' \rightarrow C' \rightarrow 0$ be two short exact sequences. Then a homomorphism of short exact sequences is a triple α, β, γ of R -module homomorphisms such that the following diagram commutes:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

If each of α, β, γ are isomorphisms, then the homomorphism is an isomorphism of short exact sequences.

Proposition 3.7 (Short Five Lemma) *Let α, β, γ be a homomorphism of short exact sequences*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

(1) *If α and γ are injective, then β is injective.*

(2) *If α and γ are surjective, then β is surjective.*

(3) If α and γ are isomorphisms, then β is an isomorphism.

Proof:

First, let $f : A \rightarrow B$, $g : B \rightarrow C$, $f' : A' \rightarrow B'$ and $g' : B' \rightarrow C'$.

To prove the first claim, suppose α and γ are injective and let $b \in B$ such that $\beta(b) = 0$. Since g' is surjective, $g\beta(b) = 0$. By commutivity of the diagram, $\gamma g(b) = 0$. Since γ is injective, $g(b) = 0$. Now, by exactness, for $a \in A$, $f(a) = b$ so $\beta f(a) = 0$. Again, commutivity implies that $f'\alpha(a) = 0$. Since f' is injective, $\alpha(a) = 0$ and since α is injective, $a = 0$. Hence, $b = f(a) = f(0) = 0$. So β is injective.

The second claim is proved similarly. In particular, suppose α and γ are surjective, and let $b' \in B'$. Surjectivity of γ and g' implies that $g'(b') = \gamma(c)$ for some $c \in C$. Since g is surjective, $c = g(b)$ for some $b \in B$ so $\gamma g(b) = g'(b')$. By commutivity of the diagram, $g'\beta(b) = \gamma g(b) = g'(b')$ so $\beta(b) - b' \in \text{Ker}(g')$. By exactness, $(\beta(b) - b') \in \text{Im}(f')$ so for some $a' \in A'$, $f'(a') = (\beta(b) - b')$. Since α is surjective, there is an $a \in A$ such that $\alpha(a) = a'$ so $f'\alpha(a) = (\beta(b) - b')$. Again, commutivity implies $f'\alpha(a) = \beta f(a) = (\beta(b) - b')$. So $b' = \beta(b) - \beta(f(a)) = \beta(b - f(a))$. Since f is injective, $b = f(a)$. Hence, $b' = \beta(b)$. And β is surjective.

The last assertion follows immediately from the first two. ★

Theorem 3.8 Let $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$ be a short exact sequence. Then the following are equivalent:

- (i) There is an R -module homomorphism $\gamma : C \rightarrow B$ such that $\gamma\beta = 1_B$;
- (ii) There is an R -module homomorphism $\delta : B \rightarrow A$ such that $\delta\alpha = 1_A$;
- (iii) The given sequence is isomorphic (with identity maps on A and C) to the direct sum short exact sequence $0 \rightarrow A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \rightarrow 0$. In particular, $B \cong A \oplus C$.

Recall that the maps $\iota : A \rightarrow A \oplus C$ and $\pi : A \oplus C \rightarrow C$ are the inclusion and projection maps respectively.

Proof:

★

Definition 3.15 If a short exact sequence satisfies the equivalent conditions of the above theorem, then the sequence is said to be split or is a split exact sequence

3.3.1 Dual Modules

Definition 3.16 Let M be a free module over a commutative ring R . A Dual Module, M^* is the free module of R -module homomorphisms from M to R , i.e., $M^* = \text{Hom}_R(M, R)$. Elements of M^* are called functionals.

If R is a field, then M^* is known as the dual space.

Proposition 3.8 $\dim(M^*) = \dim(M)$

Definition 3.17 The double dual M^{**} is the dual to the dual module M^* .

Proposition 3.9 $M^{**} \cong M$.

Proposition 3.10 Let M, N and L be free modules over R and let $\star \star \star$ be an exact sequence. Then the sequence

$$\star \star \star$$

is also exact.

3.3.2 Finitely generated modules over P.I.D.s

3.3.3 Exactness properties of tensor products

Proposition 3.11 Let F be a right R -module. Then the following are equivalent and define F to be a flat module:

1. For any left R -modules, L, M and N , if

$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$

is a short exact sequence, then

$0 \rightarrow L \otimes_R F \rightarrow M \otimes_R F \rightarrow N \otimes_R F \rightarrow 0$

is also a short exact sequence.

2. For any left R -modules L and M , if $0 \rightarrow L \rightarrow M$ is exact (i.e., ϕ is injective), then

$0 \rightarrow L \otimes_R F \rightarrow M \otimes_R F$

is an exact sequence of abelian groups.

Proposition 3.12 Let R be an integral domain.

1. The field of fractions Q is flat or something like that
- 2.
3. A projective R -module is flat.

3.4 Exterior algebra

Definition 3.18 Let M be a module over a commutative ring with 1. For each integer $k \geq 1$, define

$$\mathcal{T}^k(M) = \underbrace{M \otimes_R M \otimes_R \cdots \otimes_R M}_{k \text{ times}}$$

with $\mathcal{T}^0(M) = R$. Then the elements of $\mathcal{T}^k(M)$ are called k tensors.

3.5 Projective and Injective modules

Proposition 3.13 *Let P be an R -module. Then for any R -modules L, M and N , the following are equivalent and define P as a projective module:*

1. *If*

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

is a short exact sequence then

$$0 \longrightarrow \text{Hom}_R(P, L) \xrightarrow{\psi'} \text{Hom}_R(P, M) \xrightarrow{\varphi'} \text{Hom}_R(P, N) \longrightarrow 0$$

is a short exact sequence.

2. *For any R -modules M and N , if $M \xrightarrow{\varphi} N \longrightarrow 0$ is exact, then every R -module homomorphism from P into N lifts to an R -module homomorphism into M , i.e., given $f \in \text{Hom}_R(P, N)$ there is a lift $F \in \text{Hom}_R(P, M)$ such that the following diagram commutes:*

$$\begin{array}{ccc} & P & \\ & \swarrow F & \downarrow f \\ M & \xrightarrow{\varphi} & N \longrightarrow 0 \end{array}$$

3. *If P is the quotient of the R -module M , then P is isomorphic to a direct summand of M , i.e., every short exact sequence*

$$0 \rightarrow L \rightarrow M \rightarrow P \rightarrow 0$$

splits.

4. *P is the direct summand of a free R -module*

Since projective modules have a natural relation to free modules, we can reverse the arrows to obtain the notion of an injective module. In particular,

Proposition 3.14 *Let D be an R -module. Then for any R -modules L, M and N , the following are equivalent and define D as an injective module.*

1. *If*

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

is a short exact sequence then

$$0 \longrightarrow \text{Hom}_R(L, D) \xrightarrow{\psi'} \text{Hom}_R(M, D) \xrightarrow{\varphi'} \text{Hom}_R(N, D) \longrightarrow 0$$

is a short exact sequence.

2. For any R -modules L and M , if $0 \longrightarrow L \xrightarrow{\psi} M$ is exact, then every R -module homomorphism from L into D lifts to an R -module homomorphism of M into D , i.e., given $f \in \text{Hom}_R(L, D)$ there is a lift $F \in \text{Hom}_R(M, D)$ such that the following diagram commutes:

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{\psi} & M \\ & & \downarrow f & \swarrow F & \\ & & D & & \end{array}$$

3. If D is the quotient of the R -module L , then D is isomorphic to a direct summand of L , i.e., every short exact sequence

$$0 \rightarrow D \rightarrow L \rightarrow M \rightarrow 0$$

splits.

3.6 Homology

including snake lemma

3.7 Derived functors incl. Tor and Ext

Definition 3.19 Let $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ be a short exact sequence of R modules. Then there is a long exact sequence of abelian groups

where the maps between groups at the same level are dependent only on the maps in the SES and the connecting homomorphisms are boundary maps.

This is just basically the UCT in its general form.

Chapter 4

Field Theory

4.1 Characteristics

Definition 4.1 The characteristic of a field F , denoted $ch(F)$, is defined to be the smallest positive integer p such that $p \cdot 1_F = 0$ if such a p exists and is defined to be 0 otherwise.

Proposition 4.1 The characteristic of a field F , $ch(F)$ is either 0 or a prime p . If $ch(F) = p$, then for any $\alpha \in F$,

$$p \cdot \alpha = \underbrace{\alpha + \cdots + \alpha}_{(p \text{ times})} = 0.$$

Definition 4.2 The prime subfield of a field F is the intersection of all subfields of F . It is isomorphic to either \mathbb{Q} (if $ch(F) = 0$) or \mathbb{F}_p (if $ch(F) = p$).

4.2 Extensions

Definition 4.3 If K is a field containing a subfield isomorphic to the field F , then K is said to be an extension field (or simply an extension) of F , denoted K/F . In particular, every field F is an extension of its prime subfield. The field F is sometimes called the base field of the extension.

In other words, an extension is a monomorphism $\iota : F \rightarrow K$.

Definition 4.4 The degree (relative degree or index, resp.) of a field extension K/F denoted $[K : F]$ is the dimension of K as a vector space over F , i.e. $[K : F] = \dim_F K$. The extension is said to be finite if $[K : F]$ is finite and is said to be infinite otherwise.

Proposition 4.2 Let $\varphi : F \rightarrow F'$ be a homomorphism of fields. Then φ is either identically 0 or is injective so that the image of φ is either 0 or isomorphic to F .

Theorem 4.1 Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.

Theorem 4.2 Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta \equiv x \pmod{(p(x))} \in K$. Then the elements $1, \theta, \dots, \theta^{n-1}$ form a basis for K as a vector space over F , so the degree of the extension is n , i.e. $[K : F] = n$. Hence,

$$K = \{a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} \mid a_0, \dots, a_{n-1} \in F\}$$

consists of all polynomials of degree less than n in θ .

Corollary 4.1 Let K be the field $F[x]/(p(x))$ and let $a(\theta), b(\theta) \in K$ be two polynomials of degree less than n in θ . Then addition is defined by usual polynomial addition and multiplication in K by $a(\theta)b(\theta) = r(\theta)$, where $r(x)$ is the remainder polynomial in $F[x]$ obtained after dividing the polynomial $p(x)$ by $a(x)b(x)$.

Definition 4.5 Let K be an extension of the field F and let $\alpha, \beta, \dots \in K$ be a collection of elements of K . Then the smallest subfield of K containing both F and the elements α, β, γ , denoted $F(\alpha, \beta, \dots)$ is called the field generated by α, β, \dots over F .

Definition 4.6 If the field K is generated by a single element α over F , i.e., $K = F(\alpha)$, then K is said to be a simple extension of F and the element α is called a primitive element for the extension.

Theorem 4.3 Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$, i.e., $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α . Then

$$F(\alpha) \cong F[x]/(p(x)).$$

Corollary 4.2 If $\deg p(x) = n$, then

$$F(\alpha) = \left\{ \sum_{i=0}^{n-1} a_i \alpha^i \mid a_i \in F \right\} \subseteq K$$

4.3 Algebraic Extensions and Finite Fields

Definition 4.7 The element $\alpha \in K$ is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F , then α is said to be transcendental over F . The extension K/F is said to be algebraic if every element of K is algebraic over F .

Proposition 4.3 Let α be algebraic over F . Then there is a unique monic irreducible polynomial $m_{\alpha, F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha, F}(x)$ divides $f(x)$ in $F[x]$.

Corollary 4.3 If L/F is an extension of fields and α is algebraic over both F and L , then $m_{\alpha, L}(x)$ divides $m_{\alpha, F}(x)$ in $L[x]$.

Definition 4.8 The polynomial $m_{\alpha, F}(x)$ is called the minimal polynomial for α over F . The degree of $m_{\alpha, F}(x)$ is called the degree of α .

Essentially, $m_{\alpha, F}(x)$ is the polynomial of smallest degree such that $m(\alpha) = 0$.

Proposition 4.4 *Let α be algebraic over the field F and let $F(\alpha)$ be the field generated by α over F . Then*

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

so that in particular

$$[F(\alpha) : F] = \deg m_{\alpha,F}(x) = \deg \alpha$$

i.e. the degree of α over F is the degree of the extension it generates over F .

Theorem 4.4 (Primitive Element Theorem) *If \mathbb{F} is a field of characteristic 0 and α and β are algebraic over \mathbb{F} then there is an element γ in $\mathbb{F}(\alpha, \beta)$ such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$.*

Proposition 4.5 *The element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F then α satisfies a polynomial of degree at most n over F . If this is true, then the degree of $F(\alpha)$ over F is at most n .*

Corollary 4.4 *If the extension K/F is finite, then it is algebraic.*

Theorem 4.5 (Tower Law) *Let $F \subseteq K \subseteq L$ be fields. Then*

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

The extension degrees are multiplicative so if one side is infinite then the other side is also infinite.

Corollary 4.5 *Suppose L/F is a finite extension and let K be any subfield of L containing F , i.e. $F \subseteq K \subseteq L$. Then*

$$[K : F] \text{ divides } [L : F].$$

Definition 4.9 *An extension K/F is finitely generated if there are elements $\alpha_1, \dots, \alpha_k$ in K such that $K = F(\alpha_1, \dots, \alpha_k)$.*

Lemma 4.1 *$F(\alpha, \beta) = (F(\alpha))(\beta)$, i.e. the field generated over F by α and β is the field generated by β over the field $F(\alpha)$ generated by α .*

This Lemma can be applied to facilitate the determination of degrees of complicated extensions.

Theorem 4.6 *The extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F . More precisely, a field generated over F by a finite number of algebraic elements of degrees n_1, \dots, n_k is algebraic of degree $\leq n_1 \cdots n_k$.*

Corollary 4.6 *Suppose α and β are algebraic over F then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (for $\beta \neq 0$) are all algebraic over F .*

Corollary 4.7 *Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L .*

Theorem 4.7 *If K is algebraic over F and L is algebraic over K then L is algebraic over F .*

Definition 4.10 *Let K_1 and K_2 be two subfields of a field K . Then the composite field of K_1 and K_2 , denoted K_1K_2 , is the smallest subfield of K containing both K_1 and K_2 . Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.*

Proposition 4.6 *Let K_1 and K_2 be two finite extensions of a field F contained in K . Then*

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F -basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \dots, \alpha_n$ and β_1, \dots, β_m are bases for K_1 and K_2 over F , respectively, then the elements $\alpha_i\beta_j$ for $i = 1, \dots, n$ and $j = 1, \dots, m$ span K_1K_2 over F .

Corrolary 4.8 *Suppose that $[K_1 : F] = m$, $[K_2 : F] = n$ where $(m, n) = 1$. then*

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

4.4 Splitting Fields

Definition 4.11 *The extension K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors in $K[x]$ and $f(x)$ does not completely factor into linear factors over any proper subfield of K containing F .*

Theorem 4.8 *For any field F , if $f(x) \in F[x]$, then there exists an extension K of F which is a splitting field for $f(x)$.*

Proposition 4.7 *A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F .*

Corrolary 4.9 *Any two splitting fields for a polynomial $f(x) \in F[x]$ are isomorphic.*

4.4.1 Normal Extensions

Definition 4.12 *If K is an algebraic extension of F which is the splitting field over F for a collection of polynomials $f(x) \in F[x]$, then K is called the normal extension of F .*

In other words, K is normal if every polynomial with a root in K splits in K .

Proposition 4.8 *An extension K/F is normal and finite if and only if K is the splitting field for some polynomial over F .*

4.4.2 Separability

Definition 4.13 *A polynomial $f(x)$ over a field F is said to be separable over F if it has no multiple zeros in a splitting field.*

Alternately, one can define a polynomial to be separable if all of its irreducible factors are separable.

Definition 4.14 *An algebraic extension K/F is a separable extension if every $\alpha \in K$ is separable over F . That is, if the minimal polynomial for each algebraic element is separable.*

Lemma 4.2 *A nonzero polynomial f over a field F is separable if and only if $(f, f') = 1$.*

Proposition 4.9 *If F is a field of characteristic zero, then every irreducible polynomial is separable. If F is a field of characteristic p , then an irreducible polynomial $f \in F[x]$ is inseparable if and only if*

$$f(x) = a_0 + a_1x^p + \cdots + a_rx^{rp}$$

where $\{a_0, \dots, a_r\} \in F$.

The last condition essentially states that f is inseparable if $f(x) = g(x^p)$ for some polynomial g over F .

Example 4.1 *Suppose $F = \mathbb{Z}_p$. and let*

Lemma 4.3 *Suppose K/F is a separable algebraic extension. Let L be a field such that $F \subseteq L \subseteq K$. Then K/L and L/F are separable extensions.*

4.4.3 Roots of Unity

Definition 4.15 *A generator for the cyclic group of all the n^{th} roots of unity is called a primitive n^{th} root of unity and is denoted ζ_n .*

Definition 4.16 *The field $\mathbb{Q}(\zeta_n)$ is called the cyclotomic field of n^{th} roots of unity.*

Definition 4.17 *The n^{th} cyclotomic polynomial $\Phi_n(x)$ is the polynomial whose roots are the primitive n^{th} roots of unity:*

$$\Phi_n(x) = \prod_{\zeta \in \mathbb{Q}(\zeta_n)} (x - \zeta) = \prod_{\substack{1 \leq a < n \\ (a, n) = 1}} (x - \zeta_n^a)$$

4.5 Algebraic Closure

Definition 4.18 *Algebraic Closure*

It is important to note that it is not necessary for an algebraically closed field to be

Proposition 4.10 *For any field F there exists an algebraically closed field K containing F .*

Proposition 4.11 *Let K be an algebraically closed field and let F be a subfield of K . Then the collection of elements \overline{F} of K that are algebraic over F is the algebraic closure of F . In particular, the algebraic closure of F is unique up to isomorphism.*

Definition 4.19 *The field \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} (i.e., \overline{F} contains all the algebraic elements over F).*

Proposition 4.12 *Let \overline{F} be an algebraic closure of F . Then \overline{F} is algebraically closed.*

Proposition 4.13 *For any field F , there is an algebraically closed field K containing F .*

Theorem 4.9 (Fundamental Theorem of Algebra) \mathbb{C} is algebraically closed.

4.6 Transcendence Basis

Definition 4.20

Theorem 4.10

Definition 4.21

Definition 4.22

Theorem 4.11

4.7 Galois Theory

Recall from an earlier section that given a group (ring or field), H , an automorphism is an isomorphism $\sigma : H \rightarrow H$. Also recall that the set of automorphisms of H form a group under function compositions and $\sigma \in \text{Aut}(H)$ maps generators to generators, i.e., for some subgroup (ring or field) A of H , $\sigma(a) = a$ for each $a \in A$.

Definition 4.23 *Let (K/F) be field extension. Then $\text{Aut}(K/F)$ be the collections of automorphisms that fix F*

Note that if F is the prime subfield of F then since every automorphism fixes F , $\text{Aut}(K/F) = \text{Aut}(K)$

Proposition 4.14 *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F . Then for any $\sigma \in \text{Aut}(K/F)$, $\sigma(\alpha)$ is a root of $\mu(\alpha)$*

Essentially, $\text{Aut}(K/F)$ just permutes the roots of any polynomial.

Definition 4.24 *The subfield F of K that is fixed by $\text{Aut}(K/F)$ is called*

4.7.1 Fundamental Theorem of Galois Theory

4.7.2 Galois groups of polynomials as permutation groups

Galois extensions are normal extensions whose automorphism groups don't fix any subfield containing F .

4.7.3 Cyclic Extensions

Definition 4.25 *An extension K/F is said to be cyclic if it is Galois and $\Gamma(K/F)$ is a cyclic group.*

4.7.4 Ruler and Compass Constructions

Definition 4.26 *The points of intersection of any two distinct lines or circles are said to be constructible from a set of Points in \mathbb{R}^2 if there is a finite sequence r_1, \dots, r_n of points such that for each $i \in \{1, \dots, n\}$ the point r_i is constructible from the set $P_0 \cup \{r_1, \dots, r_{i-1}\}$*

Theorem 4.12 *If $r = (x, y)$ is constructible and if K_0 is the subfield of \mathbb{R} generated by the coordinates of the points in P_0 then the degrees $[K_0(x) : K_0]$ and $[K_0(y) : K_0]$ are powers of 2.*

Proposition 4.15 *The cube cannot be duplicated using ruler and compass constructions*

Proposition 4.16 *The angle $\pi/3$ cannot be trisected using ruler and compass constructions.*

4.7.5 solvability by radicals

4.7.6 norms and traces

4.7.7 computations of Galois groups

Chapter 5

Linear Algebra

5.1 Vector Spaces

Definition 5.1 If \mathbb{F} is a field then a vector space, V over \mathbb{F} is an (additive) abelian group equipped with scalar multiplication; that is, there is a function $\varphi : \mathbb{F} \times V \rightarrow V$, defined by $\phi(a, v) = av$ such that for all $a, b, 1 \in \mathbb{F}$ and all $u, v \in V$,

(i) $a(u + v) = au + av$

(ii) $(a + b)v = av + bv$

(iii) $(ab)v = a(bv)$

(iv) $1v = v$.

The elements of V are called vectors while the elements of \mathbb{F} are called scalars.

Definition 5.2 If V is a vector space over a field \mathbb{F} , then a subspace, U , of V is a nonempty subset of V such that

(i) $0 \in U$

(ii) For any $u, u' \in U$ and $\alpha \in \mathbb{F}$, $\alpha u - u' \in U$

Definition 5.3 If U_1, \dots, U_n are subspaces of a vector space V , then $V = U_1 \oplus \dots \oplus U_n$, i.e., is the direct sum of the subspaces, if each element in V can be written uniquely as the sum $\sum u_i$ where $u_i \in U_i$ for each $i \in \{1, \dots, n\}$.

Proposition 5.1 Let U, W be distinct proper subspaces of a vector space V . Then $V = U \oplus W$ if and only if $V = U + W$ and $U \cap W = \{0\}$.

Proof:

First, suppose $V = U \oplus W$. By definition of direct sum, $V = U + W$. Additionally, if $v \in U \cap W$, then $-v \in U \cap W$. So there exist $v \in U$ and $-v \in W$ such that $v + (-v) = 0$, but by uniqueness, $v = -v = 0$, since $0 = 0 + 0$.

Conversely, suppose $V = U + W$ and $U \cap W = \{0\}$. It suffices to show uniqueness of the sum. Suppose for $u \in U, w \in W, u + w = 0$. Then $-u \in W$ which implies that $u \in W$ so $u \in U \cap W$. So $u = 0$. Therefore $0 + w = 0 \implies w = 0$. Hence, $V = U \oplus W$. ★

Definition 5.4 Let V be a vector space over a field \mathbb{F} and let $\{v_1, \dots, v_n\}$ be a collection (list) of vectors in V . A linear combination of $\{v_1, \dots, v_n\}$ in V is a vector v of the form

$$v = a_1v_1 + \dots + a_nv_n$$

where $a_i \in \mathbb{F}$ for each $i \in \mathbb{Z}$.

Additionally, if $X = \{v_1, \dots, v_m\}$ is a list in a vector space V , then

$$\langle v_1, \dots, v_m \rangle,$$

the set of all the \mathbb{F} -linear combinations of $\{v_1, \dots, v_m\}$, is called the subspace spanned by X . Simply stated, $\{v_1, \dots, v_m\}$ spans $\langle v_1, \dots, v_m \rangle$.

Lemma 5.1 Let V be a vector space over a field \mathbb{F} . Then

- (i) If U_1, \dots, U_n are subspaces of V , then $\bigcap U_i$ is a subspace of V .
- (ii) If $X = \{v_1, \dots, v_m\}$ is a list in V , then the intersection of all the subspaces of V containing X is $\langle v_1, \dots, v_m \rangle$, the subspace spanned by v_1, \dots, v_m , and so $\langle v_1, \dots, v_m \rangle$ is the smallest subspace of V containing X .

Definition 5.5 A vector space V is called finite dimensional if it has a finite spanning set; otherwise, V is called infinite dimensional.

Proposition 5.2 If V is a vector space then the following conditions on a set $X = \{v_1, \dots, v_m\}$ spanning V are equivalent:

- (i) X is not the shortest spanning set.
- (ii) some v_i is in the subspace spanned by the others; that is,

$$v_i \in \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m \rangle$$

- (iii) There are scalars, $\alpha_1, \dots, \alpha_m$ not all zero with

$$\alpha_1v_1 + \dots + \alpha_mv_m = 0$$

If the above conditions are satisfied, then the list X is said to be **linearly dependent**; otherwise, X is **linearly independent**.

Corrolary 5.1 If $X = \{v_1, \dots, v_m\}$ is a set spanning a vector space V , then X is the shortest spanning set if and only if X is linearly independent.

Definition 5.6 A basis of a vector space V is a linearly independent list that spans V .

Theorem 5.1 Every finite dimensional vector space V has a basis.

Lemma 5.2 Let u_1, \dots, u_n be elements in a vector space V , and let $v_1, \dots, v_m \in \langle u_1, \dots, u_n \rangle$. If $m > n$, then $\{v_1, \dots, v_m\}$ is a linearly dependent list.

Corrolary 5.2 A homogenous system of linear equations, over a field \mathbb{F} , with more unknowns than equations has a nontrivial solution.

Theorem 5.2 (Invariance of Dimension) If $X = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_m\}$ are bases of a vector space V , then $m = n$

Definition 5.7 If V is a finite dimensional vector space, then its dimension, denoted by $\dim(V)$, is the number of elements in basis of V .

Lemma 5.3 If $X = \{v_1, \dots, v_n\}$ is a linearly dependent list of vectors in a vector space V , then there exists v_r with $r \geq 1$ and $v_r \in \langle v_1, \dots, v_{r-1} \rangle$ (when $r = 1$, we interpret $\langle v_1, \dots, v_{r-1} \rangle$ to mean $\{0\}$).

Proposition 5.3 Let $Z = \{u_1, \dots, u_m\}$ be a linearly independent list in an n -dimensional vector space V . Then there are vectors v_{m+1}, \dots, v_n such that $u_1, \dots, u_m, v_{m+1}, \dots, v_n$ is a basis of V .

Corrolary 5.3 If $\dim(V) = n$ then any list with at least $n + 1$ or more vectors is linearly dependent.

Corrolary 5.4 Let V be a vector space with $\dim(V) = n$. Then a list of n vectors spans V if and only if the vectors are linearly independent.

Corrolary 5.5 Let $U \subseteq V$ be a subspace of a finite dimensional vector space. Then

- (i) U is finite dimensional and $\dim(V) - \dim(U) = \dim(V/U)$;
- (ii) If $\dim(U) = \dim(V)$, then $U = V$.

Theorem 5.3 If U and W are finite dimensional subspaces of a vector space V , then $U \cup W$ is finitely dimensional and

$$\dim(U \cup W) = \dim(U) + \dim(W) - \dim(U \cap W)$$

Proof:

Suppose $\dim(U) = n$ and $\dim(W) = m$. Since $U \cap W$ is a subspace of U and W , $U \cap W$ has finite basis v_1, \dots, v_k where $k \leq n, m$. Continued... ★

Definition 5.8 Let W_1, \dots, W_n be subspaces of a vector space V . Then W_1, \dots, W_n are independent if for each $v_i \in W_i$ $v_1 + \dots + v_n = 0$ implies that $v_i = 0$.

Lemma 5.4 Let V be a finite dimensional vector space and W_1, \dots, W_n subspaces of V . Suppose there is a subspace $W = W_1 + \dots + W_n$. Then the following are equivalent:

- (a) W_1, \dots, W_n are independent.
- (b) For each k and $2 \leq k \leq n$

$$W_k \cap (W_1 + \dots + W_{k-1} + W_{k+1} + \dots + W_n) = \{0\}.$$

- (c) If \mathcal{B}_j is an ordered basis for W_j $1 \leq j \leq n$, then the sequence $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_n)$ is an ordered basis for W .

5.2 Linear Transformations and Matrices

Definition 5.9 If V and W are vector spaces over a field \mathbb{F} , then a mapping $T : V \rightarrow W$ is a linear transformation if for all vectors $u, v \in V$ and all scalars $\alpha \in \mathbb{F}$,

$$(i) \quad T(u + v) = T(u) + T(v)$$

$$(ii) \quad T(\alpha v) = \alpha T(v)$$

Theorem 5.4 Let $\{v_1, \dots, v_n\}$ be a basis of a vector space V over a field \mathbb{F} . If W is a vector space over \mathbb{F} and $\{u_1, \dots, u_n\}$ is a **list** in W , then there exists a unique linear transformation $T : V \rightarrow W$ with $T(v_i) = u_i$ for all i .

Corrolary 5.6 If two linear transformations $S, T : V \rightarrow W$ agree on a basis, then $S = T$.

Definition 5.10 If a linear transformation T maps V into itself, then T is an endomorphism. The set of all endomorphisms is called the endomorphism ring and is denoted $\text{End}(V)$.

Definition 5.11 Let $T : V \rightarrow W$ be a linear transformation. Then

(i) the kernel (null space) of T is $\text{Ker}(T) = \{v \in V \mid T(v) = 0\}$ and

(ii) the image of T is $\text{Im}(T) = \{w \in W \mid w = T(v) \text{ for some } v \in V\}$

Proposition 5.4 Let $T : V \rightarrow W$ be a linear transformation.

(i) $\text{Ker}(T)$ is a subspace of V and $\text{Im}(T)$ is a subspace of W

(ii) T is injective if and only if $\text{Ker}(T) = \{0\}$

Theorem 5.5 Let V be an n dimensional vector space and W an m dimensional vector space (n not necessarily equal to m) and $T : V \rightarrow W$ a linear transformation. Then

$$\dim(V) = \dim(\text{Ker}(T)) + \dim(\text{Im}(T))$$

Proof:

Let $\dim(V) = n$. If $\dim(\text{Ker}(T)) = k$, then $\{v_1, \dots, v_n\}$ forms a basis for $\text{Ker}(T)$. Since $\text{Ker}(T)$ is a subspace of V , there are linearly independent vectors $\{v_{k+1}, \dots, v_n\}$ in V such that the basis for $\text{Ker}(T)$ can be extended to form a basis $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$ for V . Since for each $v \in V$, $v = \alpha_1 v_1 + \dots + \alpha_n v_n$, $\text{Im}(T) \in \langle T(v_1), \dots, T(v_n) \rangle$. Since $T(v_j) = 0$ for $j \leq k$, $\text{Im}(T) \in \langle T(v_{k+1}), \dots, T(v_n) \rangle$. It now suffices to show that $\{T(v_{k+1}), \dots, T(v_n)\}$ is a linearly independent set.

$$\begin{aligned} 0 &= \sum_{i=k+1}^n \beta_i T(v_i) \\ &= \sum_{i=k+1}^n T(\beta_i v_i) \\ &= T\left(\sum_{i=k+1}^n \beta_i v_i\right) \end{aligned}$$

So $\sum_{i=k+1}^n \beta_i v_i \in \text{Ker}(T)$ which implies that

$$\sum_{i=k+1}^n \beta_i v_i = \sum_{j=1}^k \alpha_j v_j$$

Since $\{v_1, \dots, v_n\}$ is a linearly independent set, it follows that $\alpha_j = \beta_i = 0$ for all $i \in \{k+1, \dots, n\}$ and $j \in \{1, \dots, k\}$. So $\{T(v_{k+1}), \dots, T(v_n)\}$ is a linearly independent set and therefore forms a basis for $\text{Im}(T)$. It then follows that $\dim(\text{Im}(T)) = n - (k+1) + 1 = n - k$. Hence

$$\dim(\text{Im}(T)) + \dim(\text{Ker}(T)) = n - k + k = n = \dim(V).$$



★ ★ ◇ ★ ★

Proposition 5.5 *Two finite dimensional vector spaces V and W are isomorphic if and only if $\dim(V) = \dim(W)$.*

Definition 5.12 *A linear transformation $T : V \rightarrow V$ is a scalar transformation if there is a $\alpha \in \mathbb{F}$ where $T(v) = \alpha v$ for all $v \in V$. i.e., $T = \alpha 1_V$. A scalar matrix is a matrix of the form αI where $\alpha \in \mathbb{F}$ and I is the identity matrix*

Observe that by this definition, a scalar transformation $T = \alpha 1_V$ is nonsingular if and only if $\alpha \neq 0$. Its inverse is $\alpha^{-1} 1_V$.

Definition 5.13 *If V is a vector space over \mathbb{F} and S is a subset of V , the annihilator of S is the set S^0 of linear functionals f such that $f(v) = 0$ for each $v \in S$.*

Definition 5.14 *If $A \in \mathcal{M}_{n \times m}(\mathbb{F})$, Then the transpose of A , denoted A^T , is $A_{ij}^T = A_{ji}$.*

Proposition 5.6 *If $A \in \mathcal{M}_{n \times m}(\mathbb{F})$ and $B \in \mathcal{M}_{m \times p}(\mathbb{F})$, then*

$$(AB)^T = B^T A^T$$

Definition 5.15 *Define Symmetric Matrices*

End With Similar Matrices. Remember to comment about similar = action.

5.3 Invariant Subspaces and Characteristic Polynomials

Definition 5.16 *Let V be a vector space over \mathbb{F} and let $T \in L(V, V)$. A characteristic value (or eigenvalue) is a scalar $\alpha \in \mathbb{F}$ such that there is $v \in V$ with $Tv = \alpha v$. If α is an eigenvalue of T , then*

- (a) *if $v \in V$ satisfies $Tv = \alpha v$, then v is called a characteristic vector (or eigenvector).*
- (b) *for a given eigenvalue, α , the set of eigenvectors is called the Characteristic space (or eigenspace) and is denoted S_α*

One useful thing to note is that $S_v = \text{Ker}(T - \alpha I)$ which reveals the fact that S_v is a vector space.

More Stuff

Definition 5.17 *If $T \in L(V)$ is similar to a diagonal matrix, then T is said to be diagonalizable.*

Theorem 5.6 *Every operator on an algebraically field has an eigenvalue*

Proposition 5.7 *Suppose $\dim(V) = n < \infty$. $T \in L(V)$ has n distinct eigenvalues then T is diagonalizable.*

Proposition 5.8 *Suppose $\dim(V) = n$ and $T \in L(V)$. Let $\lambda_1, \dots, \lambda_n$ be distinct eigenvalues of T . Then the following are equivalent:*

1. T is diagonalizable.
- 2.
- 3.
4. $V = \text{Ker}(T - \lambda_1 I) \oplus \dots \oplus \text{Ker}(T - \lambda_n I)$
- 5.

Definition 5.18 *If V is a vector space, then a projection of V is a linear operator E on V such that $E^2 = E$.*

Theorem 5.7 *Every operator on a finite dimensional real vector space has an invariant subspace of dimension 1 or 2.*

Theorem 5.8 *Every operator on an odd dimensional vector space has at least one eigenvalue*

In elementary algebra, this is analogous to the fact that every polynomial of odd degree has at least one root in \mathbb{R} .

These are to be moved around some:

5.4 Similarity and Canonical Forms

In general, one can find a Jordan canonical form, J of a matrix $T \in \mathcal{M}_{n \times n}(\mathbb{F})$ as follows:

1. Identify the eigenvalues of T .
2. Recall that the number of J -blocks for each eigenvalue is the dimension of the eigenspace, that is

$$\dim(E_{\lambda_i}) = \nu(\lambda I - A)$$

3. Apply the Primary Decomposition Theorem (if necessary) to determine the multiplicities of each eigenvalue .

4. If m_λ is the multiplicity of the eigenvalue λ , then the smallest $k \in \{1, \dots, m_\lambda\}$ such that

$$\rho(\lambda I - J)^k = n - m_\lambda$$

is the size of the largest block. The number of blocks of size k is equal to

$$b_1 = \rho(\lambda I - J)^{k-1} - n + m_\lambda.$$

Additionally, this k is the degree of the corresponding invariant factor in the minimal polynomial. So, on the qualifying exam, if given the minimal polynomial, it is sufficient to remember that the degree of the i^{th} invariant factor is the size of the largest corresponding J -block.

In general, you can determine the number of J -blocks of size $k - r$ by considering the powers of $\rho(\lambda I - J)$. In particular, the number of blocks of size $(k - r)$ should be

$$b_{r+1} = \rho(\lambda I - J)^{k-r+1} - n + m_\lambda - \sum_{s=1}^r (r-s)b_s$$

Note that this is merely a conjecture as I am still working out the details, but for the qualifying exam purposes, it is sufficient to only identify the size of the largest block and, possibly, the number of blocks of that largest size.

5. Assemble the Jordan Canonical Form, noting that

$$J = \begin{pmatrix} J_{\lambda_1} & 0 & 0 & 0 \\ 0 & J_{\lambda_2} & 0 & 0 \\ 0 & 0 & \ddots & \\ 0 & 0 & & J_{\lambda_t} \end{pmatrix}$$

5.5 Inner Products and Bilinear Forms

Definition 5.19 Let V be a vector space and $u, v \in V$. An inner product is a function that maps (u, v) to $\langle u, v \rangle \in \mathbb{F}$. Inner products satisfy the following conditions:

positivity

definiteness

additivity (in the first position)

homogeneity (in the first position)

conjugate symmetry

Note that this definition can easily be generalized to k -tuples (u_1, \dots, u_k)

Definition 5.20 A vector space V together with an inner product structure is called an inner product space.

Definition 5.21 *Two vectors $u, v \in V$ are said to be orthogonal if their inner product is zero.*

Definition 5.22 *For $v \in V$, the norm of v is the square root of the inner product with itself, i.e.,*

$$\|v\| = \sqrt{\langle v, v \rangle}$$

Definition 5.23 *If $\dim(V) = 1$ then the norm is just the familiar absolute value.*

Chapter 6

Representation Theory (of finite groups)

6.1 Introduction

Definition 6.1 Let G be a group, \mathbb{F} be a field and V be a vector space over \mathbb{F} . A linear representation of G is any homomorphism ρ from G into $GL(V)$ where n is the degree of the representation.

Since ρ is a homomorphism, it follows that ρ is a representation if and only if

$$\rho(gh) = \rho(g)\rho(h) \quad \text{for all } g, h \in G.$$

Additionally, for every representation $\rho : G \rightarrow GL_n(\mathbb{F})$,

$$\begin{aligned} \rho(1) &= I_n \\ \rho^{-1}(g) &= \rho(g^{-1}) \quad \text{for all } g \in G \end{aligned}$$

A nice way to view the representation ρ is by observing that ρ gives V the structure of a G -module. Accordingly, we can occasionally say V is the representation ρ .

Definition 6.2 Two representations $\rho : G \rightarrow GL_n(\mathbb{F})$ and $\sigma : G \rightarrow GL_m(\mathbb{F})$ are equivalent (isomorphic or similar) if $m = n$ and there exists an $n \times n$ invertible matrix T such that

$$\rho(g) = T(\sigma(g))T^{-1} \quad \text{for all } g \in G$$

Proposition 6.1 The representation similarity is an equivalence relation.

Proof:

1. Since $\rho(g) = I\rho(g)I^{-1} = \rho(g)$, $\rho \sim \rho$
2. If $\rho \sim \sigma$, then there is an invertible matrix T such that $\rho(g) = T(\sigma(g))T^{-1}$. Then $T^{-1}(\rho(g))T = \sigma(g)$ so $\sigma \sim \rho$.
3. If $\rho \sim \sigma$ and $\sigma \sim \tau$ then there exist invertible matrices S and T such that $\rho(g) = S\sigma(g)S^{-1}$ and $\sigma(g) = T\tau(g)T^{-1}$. Since the product of invertible matrices is again invertible, $\rho(g) = ST\tau(g)T^{-1}S^{-1} = ST\tau(g)(ST)^{-1}$. So $\rho \sim \tau$.

Hence, representation similarity is an equivalence relation. ★

Definition 6.3 *The kernel of a representation $\rho : G \rightarrow GL_n(\mathbb{F})$ is the set of elements $g \in G$ such that*

$$\rho(g) = I_n$$

Definition 6.4 *The representation $\rho : G \rightarrow GL_1(\mathbb{F})$ defined by*

$$\rho(g) = 1 \quad \text{for all } g \in G$$

is called the trivial representation of G .

Definition 6.5 *A representation $\rho : G \rightarrow GL_n(\mathbb{F})$ is faithful if $\ker \rho \equiv \{1\}$.*

Proposition 6.2 *A representation $\rho : G \rightarrow GL_n(\mathbb{F})$ is faithful if and only if $\text{Imp } \rho \cong G$.*

6.1.1 Direct Sums and Tensor Products

If V and W are two representations, then the direct sum, $V \oplus W$ and the tensor product $V \otimes W$ are also representations. In the latter case, if $v \in V$ and $w \in W$, then

$$\rho(g)(v \otimes w) = \rho(g)v \otimes \rho(g)w.$$

Definition 6.6 *Suppose V is a vector space with basis $\mathcal{B} = \{e_1, \dots, e_n\}$. Let $\varphi \in \text{Aut}(V)$ such that $\varphi(e_i e_j) = e_i e_j$. Define the subspace $\text{Sym}(V) \subseteq V$ to be the set of elements that directly commute the basis elements *Finish this later**

6.1.2 Examples

Example 6.1 *permutation representation*

Example 6.2 *regular representation*

6.2 Irreducibility

Definition 6.7 *Suppose $\rho : G \rightarrow GL_n(V)$ and let W be a subspace of V . If W is invariant under ρ , that is $\rho(W) \subseteq W$, then $\rho|_W : G \rightarrow GL(W)$ is a subrepresentation of ρ .*

Theorem 6.1 *If $\rho : G \rightarrow GL_n(V)$ is a representation with a ρ -invariant subspace W , then there exists an orthogonal complement W^\perp of W such that W^\perp is also ρ -invariant.*

Definition 6.8 *A representation $\rho : G \rightarrow GL(V)$ is irreducible (or simple) if the only ρ -invariant subspaces are 0 and V .*

In other words, ρ doesn't have any non-trivial subrepresentations.

Theorem 6.2 (Maschke's Theorem) *Every representation is a direct sum of irreducible representations*

6.3 Characters

Definition 6.9 Suppose V is a $\mathbb{C}G$ -module with basis \mathcal{B} then the character of V is the function $\chi : G \rightarrow \mathbb{C}$ defined by

$$\chi(g) = \text{Tr}[g]_{\mathcal{B}}$$

In other words, the character χ of a representation $\rho : G \rightarrow GL_n(\mathbb{C})$ is $\chi(g) = \text{Tr}(\rho(g))$.

More Stuff

Theorem 6.3 Let χ_1, \dots, χ_n be irreducible characters of G , and let g_1, \dots, g_n be representatives of the conjugacy classes of G . Then the following relations hold for any $r, s \in \{1, \dots, n\}$:

1. (Row Orthogonality)

$$\sum_{i=1}^n \frac{\chi_r(g_i) \overline{\chi_s(g_i)}}{|C_G(g_i)|} = \delta_{rs}.$$

2. (Column Orthogonality)

$$\sum_{i=1}^n \chi_i(g_r) \overline{\chi_i(g_s)} = \delta_{rs} |C_G(g_r)|.$$

Theorem 6.4 Given groups G and H with irreducible characters χ_1, \dots, χ_n and ψ_1, \dots, ψ_m respectively, the irreducible characters of the direct product $G \times H$ is given by

$$(\chi \times \psi)(g, h) = \chi(g)\psi(h).$$

Proposition 6.3 For $g \in G$, If χ_S is the character for $\text{Sym}(V)$ and χ_A the character for $\text{Alt}(V)$, then

$$\begin{aligned} \chi_S(g) &= \frac{1}{2} (\chi^2(g) + \chi(g^2)) \quad \text{and} \\ \chi_A(g) &= \frac{1}{2} (\chi^2(g) - \chi(g^2)). \end{aligned}$$

6.4 Schur's Lemma

6.5 Subgroups