Rice University
Department of Mathematics

Introduction to Rings, Fields, and Groups

A first exposure to core concepts in abstract algebra

Author
Gabriel Gress

May 18, 2021

Contents

Contents 1

1 Divisibility, Congruences, Euler's Function 2

2 Rings 3
- 2.1 Subring, Ideals, Factor rings, Ring homomorphisms . . . 3
- 2.2 Factor Ring . . . 4
- 2.3 Ring Homomorphism . . . 4
- 2.4 Direct Sums of Rings . . . 5
- 2.5 Number Theory in Rings . . . 5
- 2.6 Fermat's Last Theorem . . . 8
- 2.7 Finite Fields . . . 9

3 Groups 11
- 3.1 Direct Product of Groups . . . 13
- 3.2 Structure of groups of special sizes . . . 13
- 3.3 Permutation Groups and Group Actions . . . 14

4 Module Theory 17
- 4.1 Modules . . . 17
- 4.2 Free Modules . . . 18
- 4.3 Generators and Relations . . . 19
- 4.4 Noetherian Rings . . . 20
- 4.5 Structure of Abelian Groups . . . 22
- 4.6 Analogues for Polynomial Rings and Linear Operators . . . 22

Chapter 1

Divisibility, Congruences, Euler's Function

All numbers are assumed to be $\mathbb{Z}$

$$a \mid b := \quad \exists c \text{ s.t. } ac = b$$

Definition 1.0.1

We say that $a \equiv b \pmod{m}$ (a is equivalent to b) if $m|a-b$

Definition 1.0.2: Euler's Function

$\varphi(n)$ is defined as the number of integers coprime to n in $\{1, 2, \ldots, n\}$. In other words, it is the magnitude of $\{c \mid 1 \leq c \leq n, (c, n) = 1\}$

Note that if p is prime, then $\varphi(p) = p - 1$.

Theorem 1.0.1

$n = p_1^{k_1} \cdot \ldots \cdot_r^{k_r}$, $p_i \neq p_j$, p prime, $k_i > 0 \implies \varphi(n) = (p_1^{k_1-1} - p_1^{k_1-1}) \cdot \ldots \cdot (p_r^{k_r} - p_r^{k_r-1})$

Theorem 1.0.2: Euler-Fermat Theorem

If c, m are coprime, then $c^{\varphi(m)} \equiv 1 \pmod{m}$.

Theorem 1.0.3: Linear Congruence

A linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $(a, m) \mid b$. Furthermore, the number of pairwise incongruent solutions is (a, m).

Definition 1.0.3: Linear Diophantine equation

A linear Diophantine equation in two variables is $Ax + By = C$ where A, B, C are given integers, A, B not both zero, with integer solutions for x, y.

A linear Diophantine equation is solvable if and only if $(A, B) \mid C$, in which case there are infinite solutions.
Note that a linear Diophantine equation can be transformed into a linear congruence $Ax \equiv C \pmod{|B|}$ or $By \equiv C \pmod{|A|}$

Chapter 2

Rings

Definition 2.0.1: Binary Operation

A binary operation assigns every ordered pair of a set $(a, b) \in S \times S$ a unique element $c \in S$, which can have the following properties:

- For every $a, b, c \in S$, $a(bc) = (ab)c$ (associative)
- For every $a, b \in S$, we have $ab = ba$ (commutative)
- There is an element $e \in S$ satisfying $ea = ae = a$ for every $a \in S$
- If S has an identity e, then there is an inverse of $a \in S$, or a^{-1} satisfying $aa^{-1} = a^{-1}a = e$ (left and right inverses, in particular)

Definition 2.0.2: Rings

A ring is a non-empty set with two operations, $+$ and $\cdot$. The $+$ operation is commutitive, associative, has an identity, and inverses for all elements. The $\cdot$ operation is associative. Both operations have two distributive rules, namely, for all a, b, c,

$$(a + b)c = ac + bc$$
$$a(b + c) = ab + ac$$

If multiplication is commutative, then it is a commutative ring. If multiplication has an identity, and an inverse for all except the additive inverse, then it is a field.
Rings in which two non-zero elements can multiply to a zero element has what are called (left or right) **zero-divisors**. Fields do not have zero-divisors.

2.1 Subring, Ideals, Factor rings, Ring homomorphisms

Definition 2.1.1: Subring

A subring is a subset S of a ring R which is a ring under the restriction of the operations in R. Notationally, we say that $S \leq R$.

$\emptyset \neq S$ is a subring if and only if $a, b \in S \implies a + b, ab, -a \in S$ which is equivalent to $a, b \in S \implies a - b, ab \in S$.

Definition 2.1.2: Ideal

An ideal is a subring $I \leq R$ which is closed under multiplication with elements of R. Notationally, we say that $I \triangleleft R$.

$\emptyset \neq I$ is an ideal if and only if $a, b \in I \implies a - b \in I$, $a \in I, r \in R \implies ar, ra \in I$.
Note: a field has only trivial ideals.

Definition 2.1.3: Principal Ideal

If R is commutative and has an identity, then the principal ideal generated by c is the ideal $(c) = \{rc \mid r \in R\}$.

This is the smallest ideal containing c.

2.2 Factor Ring

Definition 2.2.1: Residue Class

The equivalence class of the integer a with the congruence relation, denoted by $\overline{a}_n$, is the set

$$\{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

In other words, the set of integers congruent to $a \pmod{n}$ is the **residue class** of the integer a modulo n.

We can combine residue classes by taking representative elements and working with them.

Definition 2.2.2: Coset

Let $I \triangleleft R$. A **coset** denoted $r + I$ is the set

$$\{r + i \mid i \in I\}.$$

Two cosets are either equal or disjoint. We define addition and multiplication of cosets by

$$(r+I)+(s+I) = (r+s)+I$$
$$(r+I)(s+I) = rs+I$$

Definition 2.2.3: Factor Ring

Let $I \triangleleft R$. We notate by R/I the **factor ring**, which is the ring with all of the cosets of I as elements, using the coset addition and multiplication defined above.

2.3 Ring Homomorphism

Definition 2.3.1: Ring Homomorphism

Let R, S be rings. A map $\varphi : R \to S$ that preserves operations is a **ring homomorphism**. In other words,

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

Note that $\varphi(0) = 0$ and $\varphi(-a) = -\varphi(a)$. Furthermore, the kernel of a ring homomorphism is an ideal

Definition 2.3.2: Isomorphism

Let R, S be rings. A function $\varphi : R \to S$ that is bijective and a ring homomorphism is a **isomorphism**. If there exists a isomorphism between two rings, we say the rings are **isomorphic**.

Proposition 2.3.1: Equivalence of Isomorphism

A ring homomorphism $\varphi : R \to S$ is an isomorphism if and only if $\mathrm{Ker}\varphi = \{0\}$ and $\mathrm{Im}\varphi = S$

This is of course equivalent to φ being bijective.

Theorem 2.3.1: First Isomorphism Theorem

Let $\varphi : R \to S$ be a ring homomorphism. Then $R/\mathrm{Ker}\varphi \simeq \mathrm{Im}\varphi$.

This means that the homomorphism is completely determined by R.

Definition 2.3.3: Natural Homomorphism

Let $I \triangleleft R$ be an ideal of R. There exists a **natural homomorphism** $\varphi : R \to R/I$ defined by $\varphi : a \mapsto a + I$.

2.4 Direct Sums of Rings

Definition 2.4.1: Direct Sum

The **direct sum** of two rings $R_1 \bigoplus R_2$ (or direct product $R_1 \times R_2$) is the ring of all ordered pairs (r_1, r_2), with $r_i \in R_i$, with addition and multiplication defined by adding and multiplying the components:

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \quad (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2).$$

One can check that this indeed satisfies the properties of a ring.

Definition 2.4.2: Projection

The **projection** subsets are defined by

$$R_1^* := \{(r_1, 0) \mid r_1 \in R_1\}$$
$$R_2^* := \{(0, r_2) \mid r_2 \in R_2\}$$

These projection subsets are isomorphic to R_1, R_2 respectively. Furthermore, R_1^*, R_2^* are ideals in $R_1 \bigoplus R_2$, and every $c \in R_1 \bigoplus R_2$ has a unique decomposition $c = c_1 + c_2$ with $c_i \in R_i$.

Proposition 2.4.1: Unique Decompositions

If I, J are ideals in a ring R such that every $r \in R$ can be uniquely written as $r = i + j$, with $i \in I$, $j \in J$, then $R \cong I \bigoplus J$

2.5 Number Theory in Rings

For the section, assume that R is an integral domain.

Definition 2.5.1: Units and Associates

Let R be an integral domain. An element that divides every element of R is called a **unit**. The corresponding products are called **associates**; the associate of c is the product of c and the unit.

Definition 2.5.2: Irreducibles and Primes

A non-unit, non-zero $r \in R$ is **irreducible** if it can be factored ONLY trivially:

$$r = ab \implies a \text{ or } b \text{ is a unit}$$

A non-unit, non-zero $p \in R$ is a **prime** if it divides a product ONLY trivially:

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

Every prime is irreducible, but the converse is false in many rings.

Definition 2.5.3: Greatest Common Divisor

A **greatest common divisor** of a and b is a common divisor which is a multiple of all common divisors.

Any two gcds are associates; not every pair of elements has a gcd. This is closely related to the ideal (a, b).

Definition 2.5.4: UFD

R is a **unique factorization domain** if every non-zero and non-unit element in R is the product of irreducible elements, and the decomposition is unique aside from associates and the order of the factors.

$\mathbb{Z}, F[x], \mathbb{Z}[x]$ are some examples of UFDs.

Definition 2.5.5: PID

R is a **principal ideal domain** if every ideal of a principal ideal. A PID automatically satisfies the conditions for a UFD. However, the converse does not hold.

Definition 2.5.6: ED

R is a **Euclidean domain** if a division algorithm can be performed in R. This means that there is a function $f : R \setminus \{0\} \to \mathbb{N}$ such that, to any $b \neq 0, a \in R$ there exist $c, d \in R$ satisfying

$$a = bc + d \quad \text{and} \quad f(d) < f(b) \text{ or } d = 0$$

Some examples include $\mathbb{Z}, F[x]$, and the ring of Gaussian integers. Every ED is a PID, and so also a UFD. However, the converse does not hold.

Theorem 2.5.1: Connection with Ideals

- $c \mid d \iff d \in (c) \iff (d) \subset (c)$
- c and d are associates if and only if $(c) = (d)$
- $(d) = (a, b) \implies d = \gcd\{a, b\}$
- $(d) = (a, b) \iff d = \gcd\{a, b\}$ and $d = au + bv, \quad u, v \in R$

Theorem 2.5.2: UFD

An integral domain R is a UFD if and only if

- a strictly increasing sequence

$$(a_1) \subset (a_2) \subset \ldots \subset (a_j) \subset \ldots$$

of principal ideals cannot be infinite; and

- every irreducible element is a prime

Definition 2.5.7: Gaussian Integers

The ring G with elements $a + bi \in \mathbb{C}$, with $a, b \in \mathbb{Z}$, is called the ring of **Gaussian Integers**.

[Norm] Let $\alpha \in \mathbb{C}$. Then the norm of α is defined by $\alpha\overline{\alpha}$

Theorem 2.5.3

$x^2 + y^2 = n$ solvable iff number of solutions

Theorem 2.5.4

The Gaussian Integers form a Euclidean Domain.

Proof. We will show that $f(\alpha) = N(\alpha)$ suffices. Observe that

$$\begin{aligned} \alpha = \beta\rho + \theta &\iff \\ \frac{\alpha}{\beta} = \rho + \frac{\theta}{\beta} &\iff \\ \frac{\alpha}{\beta} - \rho = \frac{\theta}{\beta} &\iff \\ \left|\frac{\alpha}{\beta} - \rho\right| < 1 & \end{aligned}$$

Of course, this is the distance between $\frac{\alpha}{\beta}$ and ρ. But there always exists a lattice point within distance 1 of any $\mathbb{C}$, and so therefore the statement holds. ■

Now we characterize all G-primes.

Proposition 2.5.1

To every Gaussian prime π, there exists exactly one positive prime number p satisfying $\pi \mid p$. Furthermore, every positive prime p is either a Gaussian prime, or the product of two complex conjugate Gaussian primes with norm p.

Theorem 2.5.5

All Gaussian primes take on the form:

- $\varepsilon(1 + i)$
- εq, with q a positive prime of the form $4k - 1$
- π where $N(\pi)$ is a positive prime of the form $4k + 1$

where ε is a unit.

Proposition 2.5.2: Disjoint Partitions of Fields

Let R be a field. Then we can partition R into disjoint sets by taking all sets of the form

$$\left\{a, -a, a^{-1}, (-a)^{-1}\right\}$$

where a is non-zero, and taking the set $\{0\}$.

Theorem 2.5.6: Two Squares Theorem

Consider the equation $x^2+y^2=n$, and let $n = 2^\alpha p_1^{\beta_1}\dots p_r^{\beta_r} q_1^{\gamma_1}\dots q_s^{\gamma_s}$ be the Gaussian factorization of n. Then, $x^2+y^2=n$ is solvable in $\mathbb{Z}$ if and only if all γ_j are even. Furthermore, the number of solutions is

$$4\prod_{j=1}^{r}(\beta_j+1)$$

Proof. First, we write $n = x^2+y^2 = (x+yi)(x-yi)$. Using the Gaussian factorization, we rewrite

$$n = 2^\alpha p_1^{\beta_1}\cdot\ldots\cdot q_1^{\gamma_1}\cdot\ldots = (-i)^\alpha(1+i)^{2\alpha}\pi_1^{\beta_1}\overline{\pi_1}^{\beta_1}\cdot\ldots\cdot q_1^{\gamma_1}$$

Now observe that

$$\begin{aligned}(x+yi)\mid n \implies x+yi &= \varepsilon(1+i)^{\alpha'}\pi_1^{\beta_1'}\overline{\pi_1}^{\beta_1''}\cdot\ldots\cdot q_1^{\gamma_1'}\cdot\ldots\\ \implies x-yi &= \overline{\varepsilon}(1-i)^{\alpha'}\overline{\pi_1}^{\beta_1'}\pi_1^{\beta_1'}\cdot\ldots\cdot q_1^{\gamma_1}\end{aligned}$$

Then because

$$\begin{aligned}n=(x+yi)(x-yi) &\implies\\ 2\alpha=\alpha'+\alpha' &\iff \alpha'=\alpha\\ \beta_1=\beta_1'+\beta_1'' &\iff \beta_1'=0,1,\dots,\beta_1;\beta_1''=\beta_1-\beta_1'\\ \gamma_1=\gamma_1'+\gamma_1' &\iff \gamma_1 \text{ even}, \gamma_1'=\frac{\gamma_1}{2}\\ (-i)^\alpha=\varepsilon\overline{\varepsilon}(-i)^\alpha &\iff 1=\varepsilon\overline{\varepsilon} \text{ which always holds}\end{aligned}$$

Thus, the equation is always solvable if all the γ are even. Looking at the above, the number of solutions will be

$$1\cdot(\beta_j+1)\cdot 1\cdot 4 = 4\prod_{j=1}^{r}(\beta_j+1)$$

■

2.6 Fermat's Last Theorem

Theorem 2.6.1: Fermat's Last Theorem

Let $n\geq 3$. Does $x^n+y^n=z^n$ have positive integer solutions?

It is clear that if it is true for $n=4$, $n=p$ prime, then it holds, as of course it will hold for any multiples. We can rewrite this as

$$x^p = z^p - y^p$$

y is a parameter, so the roots are

$$z^p = y^p \implies z = (y^p)^{\frac{1}{p}} = z, z\rho, z\rho^2, \dots, z\rho^{p-1} \text{ where } \rho = \cos\frac{\pi}{p} + i\sin^2\frac{2\pi}{p}$$

So we can rewrite this as

$$x^p = z^p - y^p = (z-y)(z-\rho y)\dots(z-\rho y^{p-1})$$

Observe that each prime must be a p-th power as they cannot share factors. Let

$$H_p = \left\{a_0 + a_1\rho + \dots + a_{p-2}\rho^{p-2}\right\}, a_j \in \mathbb{Z}$$
$$\rho^{p-1} + \rho^{p-2} + \dots + \rho + 1 = 0$$

If the factors on the RHS are pairwise coprime, then $z - y = \varepsilon_0\theta_0^p$, $z - y\rho = e_1\theta_1^p$ BUT the units are non-trivial for these types of coefficients, AND we don't have UFT.

Then Kummer did a different direction. Note that "if there is a gcd then it is UFT" (not exactly, but dw about it). Then consider for $a, b \in \mathbb{Z}$

$$\gcd(a,b) = d \implies d = au + bv$$

Consider the set

$$\{ak + bl \mid k, l \in \mathbb{Z}\} = \{dn \mid n \in \mathbb{Z}\}$$

Now consider

$$\{ak + bl \mid k, l \in H_p\}$$

If $\exists\gcd(a,b) \implies$ this set is the set of multiples of gcd. So for "ideal numbers" UFT holds and the proof holds. So for "ideal numbers" UFT holds and the proof holds.

2.7 Finite Fields

Theorem 2.7.1

Let F be a finite field. $|F| = p^k$, p prime. Conversely, for every p^k there exists exactly one F such that $|F| = p^k$

Theorem 2.7.2

For any element $a \in F$ a finite field,

$$a + \dots + a = 0$$

where a is added exactly p times.

Theorem 2.7.3

Let F be a finite field. Then

$$F = \left\{0, 1, \alpha, \alpha^2, \dots, \alpha^{|F|-2}\right\}$$

and $\alpha^{|F|-1} = 1$

Theorem 2.7.4: Finite Field Extensions

For all finite fields F,there exists an $H \leq F$ such that $H \cong \mathbb{Z}_p$ for some p. Furthermore, F is a vector space over $\mathbb{Z}^p$.

F is then a field extension of H.

Theorem 2.7.5

For any finite field F, $F \cong \mathbb{Z}_{p[x]}/(g)$ where g is a polynomial over $\mathbb{Z}_p$, $\deg g = k$, g irreducible over $\mathbb{Z}_p$

Chapter 3

Groups

Definition 3.0.1: Group

A **group** is a set G that has an associative operation with an identity e and inverses for all elements. If the operation is commutative, then we say G is **abelian**.

One particular important class of groups are cyclic groups. A **cyclic group** is a group consisting of powers of a single element g, denoted by $\langle g \rangle$.

Definition 3.0.2: Order

Let $g \in G$. The **order of** g, denoted by $o(g)$, is the smallest positive integer k satisfying $g^k = e$. If there is no such k, then we say that $o(g) = \infty$.

In the finite case, the powers of g are periodic, and so the order is the smallest period.

A finite group G is cyclic if and only if $|G| = o(g)$ for some $g \in G$. Lagrange's theorem implies that $o(g) \mid |G|$ for $|G| < \infty$.

Definition 3.0.3: Subgroup

A set $H \subset G$ is a **subgroup** of G if it is a group under the operation of G. We denote this by $H \leq G$.

$H \leq G$ if and only if it contains the identity of G and is closed under the operation in G, and for inverses.

Definition 3.0.4: Coset

Let $H \leq G$ and $g \in G$. Then $gH = \{gh \mid h \in H\}$ is a **left coset**, and $Hg = \{hg \mid h \in H\}$ is a **right coset**.

Two left cosets are either disjoint or equal, and every coset is of the same size.

Theorem 3.0.1: Lagrange's Theorem

Let H be a subgroup of G. Then $|H| \mid |G|$ for $|G| < \infty$.

Important subgroups and their properties:

Definition 3.0.5: Permutations

We define by S_n the set of all bijections of $\{1, 2, \ldots, n\}$ onto itself, with the operation being composition.

Corollary 3.0.1

With "old permutations" we say a permutation is even or odd based on the number of inversions. With this definition, we say that a permutation is even if and only if the permutation is the product of an even number of transpositions.

Let A_n denote the set of even permutations. This is clearly a subgroup of S_n. We would like to show that

$$|S_n : A_n| = 2.$$

Observe that there is a bijection from the even permutations to the odd permutations by simply transposing the first two elements.

The order of an element $g \in S_n$ is the LCM of the lengths of disjoint cycles.

Definition 3.0.6: Normal Subgroup

A subgroup N of G is **normal** if the left and right cosets are the same; i.e.

$$N \leq G \text{ and } gN = Ng$$

for every $g \in G$. We denote this by $N \triangleleft G$.

We can also think of this as $Ng \subset gN$ and $gN \subset Ng$, or in other words, $g^{-1}ng \in N$ and $gng^{-1} \in N$.

$$N \triangleleft G \iff N \leq G \text{ and } g^{-1}ng \in N \text{for every } g \in G, n \in N$$

We call $g^{-1}ng$ a **conjugate** of n.

Observe that, because the trivial subgroups are trivially normal, then all subgroups H of index 2 are normal.
Every group also has a special normal subgroup called the **center**, denoted by $Z(G)$.

$$Z(G) = \{c \in G \mid cg = gc \text{ for every } g \in G\}.$$

Furthermore, every subgroup of the center is normal.

Definition 3.0.7: Factor Group

We denote by G/N the **factor group**, whose elements are the cosets of the normal subgroup N, with operations defined by $(aN)(bN) = (abN)$

Definition 3.0.8: Group Homomorphism

We call a map $\varphi : G_1 \to G_2$ a **group homomorphism** if it preserves the operation; $\varphi(gh) = \varphi(g)\varphi(h)$ for every $g, h \in G_1$.

Naturally, $\varphi(e_1) = \varphi(e_2)$, $\varphi(g^{-1}) = (\varphi(g))^{-1}$, $\mathrm{Ker}(\varphi) = \{g \in G_1 \mid \varphi(g) = e_2\} \triangleleft G_1$, and $\mathrm{Image}(\varphi) = \{\varphi(g) \mid g \in G_1\} \leq G_2$.

If the homomorphism is bijective, then it is an **isomorphism**. A homomorphism φ is an isomorphism if and only if $\mathrm{Ker}\varphi = e_1$ and $\mathrm{Im}\varphi = G_2$.

Theorem 3.0.2: First Isomorphism Theorem

If $\varphi : G_1 \to G_2$ is a homomorphism, then

$$\mathrm{Im}\varphi \cong G_1/\mathrm{Ker}\varphi.$$

Definition 3.0.9: Natural Homomorphism

If $N \triangleleft G$, then $\psi : G \to G/N$ defined by $\psi(g) = gN$ is the natural homomorphism with $\mathrm{Ker}\psi = N$ and $\mathrm{Im}\psi = G/N$.

3.1 Direct Product of Groups

Definition 3.1.1: Direct Product

The **direct product** $G_1 \times G_2$ of groups G_1, G_2 is the group of all ordered pairs (g_1, g_2) where $g_i \in G_i$, with the usual definition of multiplication:

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2).$$

It is clearly a group, and the projection subsets $G_1^* = \{(g_1, e_2) \mid g_1 \in G_1\}$ and $G_2^* = \{(e_1, g_2) \mid g_2 \in G_2\}$ are isomorphic to their respective groups.

Furthermore, G_1^*, G_2^* are normal subgroups in the direct product, and every $u \in G_1 \times G_2$ can be decomposed as $u = u_1u_2$, $u_i \in G_i^*$. The converse holds as well; if N, M are normal subgroups of a group G, and every $g \in G$ can be written as $g = nm$, $n \in N, m \in M$, then $G \cong N \times M$.

Of course, $(G_1 \times G_2)/G_1^* \cong G_2$ and vice versa; we can even take the direct product of more than two groups.

The Fundamental Theorem of Finite Abelian Groups states that every finite Abelian group is the direct product of cyclic groups of prime power size, and the list of the direct factors is uniquely determined.

3.2 Structure of groups of special sizes

Proposition 3.2.1

- If $|G| = p$, then $G \cong Z_p$
- If $|G| = p^2$, then G is Abelian and $G \cong Z_{p^2}$ OR $Z_p \times Z_p$
- Let $p > 2$, if $|G| = 2p$, then $G \cong Z_{2p}$ OR D_p.

Definition 3.2.1: Permutation Groups

Permutation groups are subgroups of S_n.

Theorem 3.2.1: Cayley's Theorem

Every group of size n is isomorphic to a subgroup of S_n.

Proof. Let S_n be all permutations of the group $G = \{e, g_2, \ldots, g_n\}$ and define $\varphi : G \to S_n$ by $\binom{g \mapsto g_i}{gg_i}$. In other words, we assign to $g \in G$ the permutation of G onto itself; we multiply every g_i by the given g from the left. One can check that φ is an injective homomorphism, and so $G \cong \mathrm{Image}(\varphi) \leq S_n$. ■

Definition 3.2.2: Simple

A group G is **simple** if the only normal subgroups are the trivial ones.

Finite simple groups are important, and only recently have they all been characterized.

3.3 Permutation Groups and Group Actions

Definition 3.3.1: Action

An **action** of a group G on a set Ω is a function $\mu : \Omega \times G \to \Omega$ with the following two properties:

- $\mu(\mu(x, g), h) = \mu(x, gh)$ for all $x \in \Omega,\ g, h \in G$.
- $\mu(x, e) = x$ for all $x \in \Omega$.

It immediately foolow that $\mu(\mu(x, g), g^{-1}) = \mu(\mu(x, g^{-1}), g) = x$ for all $x \in \Omega, g \in G$.

Proposition 3.3.1

- For any $g \in G$, the map $\pi_g : \Omega \to \Omega$ defined by $x\pi_g = \mu(x, g)$ is a permutation.
- The map $\theta : G \to S_n$ defined by $g\theta = \pi_g$ is a homomorphism (where S_n is the set of permutations of Ω, so $n = |\Omega|$)
- Conversely, given a homomorphism $\theta : G \to S_n$, there is an action μ of G on Ω given by $\mu(x, g) = x(g\theta)$.

Example 3.3.1

- Let H be a subgroup of G. Let Ω be the set of all right cosets of H in G. Define an action by $\mu(Ha, g) = H(ag)$. This is the action of **right multiplication**.
- Define an action of G on itself ($\Omega = G$) by the rule $\mu(x, g) = g^{-1}xg$. This is the action of **conjugation**.
- Let Ω be the set of all subgroups of G. Then G acts on Ω by **conjugation**: $\mu(H, g) = g^{-1}Hg$.

An equivalence relation on Ω is formed by a group action via the rule that $x \sim y$ if there exists $g \in G$ with $\mu(x, g) = y$. The equivalence classes are called **orbits**. The set Ω decomposes into a disjoint union of orbits.

Definition 3.3.2: Transitivity

We say that an action is **transitive** if there is just one orbit, and **intransitive** otherwise.

Right multiplication is transitive, but conjugation is in general not. The orbits for conjugation of G onto itself are the **conjugacy classes** of G.

Definition 3.3.3: Stabilizer

The **stabilizer** of an element $x \in \Omega$ is the set

$$\{g \in G \mid \mu(x, g) = x\}$$

of elements of G for which the corresponding permutation fixes x. It is denoted G_x.

Theorem 3.3.1: Orbit-Stabilizer Theorem

Given an action of G onto Ω, and $x \in \Omega$, the stabilizers G_x form a subgroup of G. Furthermore, there is a bijection between the orbit of x and the set of right cosets of G_x in G.

If G is finite, the size of the orbit of x is equal to $|G : G_x| = |G| / |G_x|$.

Note that in the action of G by conjugation, we call the stabilizer of x its **centralizer** $C_G(x)$. When considering conjugation of G by conjugation on subgroups, the stabilizer of a subgroup H is its **normalizer**

$$N_G(H) = \left\{ g \in G \mid g^{-1}Hg = H \right\}.$$

Corollary 3.3.1

Every transitive action is isomprohic to an action by right multiplication on the right cosets of a subgroup. Furthermore, the actions on the right cosets of two subgroups H, K are isomorphic if and only if H, K are conjugate.

Note: Let $\mathrm{fix}(g)$ denote the number of elements in Ω that are mapped to themselves when g is applied to them as an action.

Theorem 3.3.2: Orbit-Counting Lemma

The number of orbits of G on Ω is given by

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g).$$

Corollary 3.3.2: Jordan's Theorem

- Let G act transitively on the finite set Ω, where $|\Omega| > 1$. Then there is an element of G which fixes no point of Ω.
- Let H be a proper subgroup of a finite group G. Then

$$\bigcup_{g \in G} g^{-1}Hg \neq G.$$

Theorem 3.3.3: Sylow's Theorem

Let G be a group of order $n = p^a m$, where p is prime and $p \not| m$. Then

- G contains a subgroup of order p^a
- The number of subgroups of order p^a is congruent to 1 (mod p) and all these subgroups are conjugate
- Any subgroup of G of order p^k, $k \leq p$, is contained in a subgroup of order p^a

Theorem 3.3.4: Cauchy's Theorem

If a prime number p divides the order of a group G, then G contains an element of order p.

A grouo of p-power order, acting on a set of size divisible by p, has the property that the number of fixed points is divisible by p. Hence, if there is at least one fixed point, then there are at least p.

Theorem 3.3.5

Let G be a group of order $p^a m$, where p is prime not dividing m. Then, for $0 \leq i \leq a$,

- G contains a subgroup of order p^i
- if $i < m$, then any subgroup of order p^i is contained normally in a subgroup of order p^{i+1}.

Theorem 3.3.6

The center of a non-trivial p-group is non-trivial. Furthermore, if $|P| = p^a$, then P has a chain

$$P_0 < P_1 < \ldots < P_a = P$$

of subgroups, where $|P_i| = p^i$ and each is a normal subgroup of P. Moreover, $P_{i+1}/P_i \cong C_p$.

Lemma 3.3.1: Burnside's Lemma

The number of orbits is equal to the average number of fixed points. We can write this by

$$|G| \cdot (\text{number of orbits}) = \sum_{g \in G} |S^g|$$

Chapter 4

Module Theory

We will consider systems $AX = B$ where A, B have elements in a ring R, and looking for solutions $X = (x_1, \ldots, x_n)^t$ with entries in R.

4.1 Modules

The analogue for a ring R of a vector space over a field is called a module.

Definition 4.1.1: Module

Let R be a ring. An R-**module** V is an abelian group with a law of composition written $+$, and a scalar multiplication $R \times V \to V$, written $r, v \mapsto rv$, that satisfies:

$$\begin{aligned} 1v &= v \\ (rs)v &= r(sv) \\ (r+s)v &= rv + sv \\ r(v+v') &= rv + rv' \end{aligned}$$

for all $r, s \in R$ and $v, v' \in V$.

This is precisely the axioms for a vector space; but the elements of a ring do not need to be invertible.

Example 4.1.1: Free Modules

The modules R^n of R-vectors are a first example, called **free modules**. Then

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} \quad r \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ \vdots \\ ra_n \end{pmatrix}$$

An abelian group V can be made into a module over the integers in exactly one way, with

$$\begin{aligned} nv &= v + \ldots_n + v \\ (-n)v &= -(nv) \end{aligned}$$

and hence V is a $\mathbb{Z}$-module; this is the only way to do so. It also holds that any $\mathbb{Z}$-module has the structure of an abelian group, and hence abelian groups and $\mathbb{Z}$-modules are equivalent concepts.

Definition 4.1.2: Submodule

A **submodule** W of an R-module V is a non-empty subset that is closed under addition and scalar multiplication. Using the laws of composition on V, W is also a module.

Proposition 4.1.1

The submodules of the R-module R are the ideals of R.

Of course, we can define a homomorphism of R-modules in the same way one would expect:

Definition 4.1.3: Homomorphism of R-modules

A **homomorphism** $\varphi : V \to W$ of R-modules follows the laws of composition

$$\varphi(v + v') = \varphi(v) + \varphi(v')$$
$$\varphi(rv) = r\varphi(v)$$

If it is bijective, then it is an **isomorphism**. The **kernel** of a homomorphism $\varphi : V \to W$ is the set of elements $v \in V$ such that $\varphi(v) = 0$ *is a submodule of the domain* V, and the **image** of φ *is a submodule of the range* W.

Finally, we can extend the quotient construction to modules. Let W be a submodule of an R-module V. The quotient module $\overline{V} = V/W$ is the group of additive cosets $\overline{v} = v + W$, made into an R-module by the rule

$$r\overline{v} = \overline{rv}.$$

Theorem 4.1.1

Let W be a submodule of an R-module V.

- The set $\overline{V}$ of additive cosets of W in V is an R-module, and the canonical map from $V \to \overline{V}$ by $v \mapsto v + W$ is a surjective homomorphism of R-modules whose kernel is W.
- Let $f : V \to V'$ be a homomorphism of R-modules whose kernel K contains W. There is a unique homomorphism $\overline{f} : \overline{V} \to V'$ such that $f = \overline{f} \circ \pi$.
- Let $f : V \to V'$ be a surjective homomorphism of R-modules whose kernel is equal to W. Then $\overline{f}$ as defined above is an isomorphism (First Isomorphism Theorem)
- Let $f : V \to V'$ be a surjective homomorphism of R-modules with kernel W. There is a bijective correspondence between submodules of V' and those of V that contain W. Namely, if S' is a submodule of V', the corresponding submodule of V is $S = f^{-1}(S')$; and if S is a submodule of V that contains W, the corresponding submodule of V' is $S' = f(S)$. If the two are corresponding modules, then V/S is isomorphic to V'/S'

4.2 Free Modules

Definition 4.2.1: R-Matrix

Let R be a ring. An R**-matrix** is a matrix whose entries are in R. An **invertible** R**-matrix** is an R-matrix that has an inverse that is also an R-matrix. The $n \times n$ invertible R-matrices form a group called the **general linear group over** R:

$$GL_n(R) = \{n \times n \text{ invertible } R\text{-matrices}\}.$$

The **determinant** of an R-matrix $A = (a_{ij})$ is defined in the usual way

$$\det(A) = \sum_p \pm a_{1,p1} \dots a_{n,pn}.$$

or the sum over all permutations of the indices and the sign being the sign of the permutation. Of course, all the usual properties of determinants hold for R-matrices.

Lemma 4.2.1

Le R be a non-zero ring. Then a square R-matrix A is invertible if and only if it has either a left inverse or a right inverse, and only if its determinant is a unit of the ring. Furthermore, an invertible R-matrix is square.

Definition 4.2.2: Span

An ordered set $(v_1, \ldots, v_k)$ of elements of a module V is said to **generate** V or **span** V if every element v is a linear combination

$$v = r_1 v_1 + \ldots + r_k v_k$$

with coefficients in R. We call v_i **generators**. We say a module V is **finitely generated** if there exists a finite set of generators.

We say a set of elements $(v_1, \ldots, v_n)$ of a module V is **independent** if, whenever a linear combination $r_1 v_1 + \ldots + r_n v_n$ with $r_i \in R$ is zero, then all the coefficients r_i are zero. We say this is a basis if every v is a unique linear combination of those elements.

The standard multiplication works the same way; i.e.

$$BX = (v_1, \ldots, v_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = v_1 x_1 + \ldots + v_n x_n$$

which defines a homorphism of modules that we may denote by

$$R^n \to^B V.$$

The homomorphism is surjective iff B generates V, injective iff B is independent, and bijective iff B is a basis. In other words, V has a basis if and only if it is isomorphic to one of the free modules R^k, and if so, it is called a **free module** too. A module is free if and only if it has a basis.

Most modules have no basis! A free Z-module is also called a **free abelian group**; lattices in $\mathbb{R}^2$ are free abelian groups, while finite, non-zero abelian groups are not free.

Proposition 4.2.1

Let R be a non-zero ring. Then the matrix P of a change of basis in a free module is an invertible R-matrix. Furthermore, any two bases of the same free module over R have the same cardinality.

We call the number of elements for a free module V the **rank** of V. It is analogous to the dimension of a vector space. Likewise, every homomorphism f between two free modules is given by left multiplication by an R-matrix.

4.3 Generators and Relations

Definition 4.3.1: Presentations

Let an $m \times n$ R-matrix denoted by A be a homomorphism of R-modules

$$R^n \to^A R^m.$$

We can denote its image by AR^n. We say that the quotient module $V = R^m/AR^n$ is **presented** by the matrix A. Any isomorphism $\sigma : R^m/AR^n \to V$ is a **presentation** of a module V, of which A is a **presentation matrix** for V if there is such an isomorphism.

We use the canonical map $\pi : R^m \to V = R^m/AR^n$ to interpret the quotient module as follows:

Proposition 4.3.1

V is generated by a set of elements $B = (v_1, \ldots, v_m)$, the images of the standard basis elements of R^m. Furthermore, if Y is a column vector in R^m, the element BY of V is zero if and only if Y is a linear combination of the columns of A, with coefficients in R, if and only if there exists a column vector X with entries in R such that $Y = AX$.

If a module V is generated by a set $B = (v_1, \ldots, v_m)$, we call any element $Y \in R^m$ such that $BY = 0$ a **relation vector**, or simply a **relation** among the generators. A set S of relations is a **complete set** if every relation is a linear combination of S with coefficients in the ring.

Proposition 4.3.2: Theoretical Method of Finding a Presentation

First, choose a set of generators $B = (v_1, \ldots, v_m)$ for V. These generators give a surjective homomorphism $R^m \to V$ that sends a column vector Y to the linear combination $BY = v_1y_1 + \ldots + v_my_m$. Denote the kernel of the map by W. It is the **module of relations**; its elements are the relation vectors.

Repeat this procedure, choosing a set of generators $C = (w_1, \ldots, w_m)$ for W, and define a surjective map $R^n \to W$ using them. Here the generators w_j are elements of R^m, and thus column vectors. Assemble the coordinate vectors A_j of w_j into a matrix with A_i as column i. Then multiplication by A defines

$$R^n \to^A R^m$$

which sends $e_j \mapsto A_j = w_j$, as it is the composition of $R^n \to W$ with the inclusion $W \subset R^m$. By construction W is its image and we denote it by AR^n. Because the map $R^m \to V$ is surjective, by the First Isomorphism Theorem, V is isomorphic to $R^m/W = R^m/AR^n$. Hence V is presented by the matrix A.

In short the presentation matrix A for a module V is determined by the set of generators for V, and the set of generators for the module of relations W. Assuming the set of generators does not form a basis, the number of generators will be equal to the number of rows of A.

Note that this relies on the assumption that V has finite generators. We must also assume that W has a finite set of generators, which is slightly more problematic.

Proposition 4.3.3: Rules for manipulating A without changing isomorphism class

Let A be an $m \times n$ presentation matrix for a module V. The following matrices A' present the same module V:

- $A' = Q^{-1}A$, $Q \in GL_m(R)$
- $A' = AP$ with $P \in GL_n(R)$
- A' is obtained by deleting a column of zeroes
- if the j-th column of A is e_i, then removing row i and column j preserves the presentation

4.4 Noetherian Rings

Proposition 4.4.1

The following conditions on an R-module V are equivalent:

- Every submodule of V is finitely generated
- There is no infinite strictly increasing chain $W_1 < W_2 < \ldots$ of submodules of V.

Definition 4.4.1: Noetherian

A ring R is **noetherian** if every ideal of R is finitely generated.

Corollary 4.4.1

A ring is noetherian if and only if it satisfies the ascending chain condition; there is no infinite strictly increasing chain $I_1 < I_2 < \dots$ of ideals of R.

Principal ideal domains are noetherian because every ideal in such a ring is generated by one element.

Corollary 4.4.2

Let R be a noetherian ring. Every proper ideal I of R is contained in a maximal ideal.

Theorem 4.4.1: Submodules of Noetherian

Let R be a noetherian ring. Every submodule of a finitely generated R-module V is finitely generated.

Lemma 4.4.1

Let $\varphi : V \to V'$ be a homomorphism of R-modules.

- If V is finitely generated and φ is surjective, then V' is finitely generated.
- If the kernal and image of φ are finitely generated, then V is finitely generated.
- Let W be a submodule of an R-module V. If both W and $\overline{V} = V/W$ are finitely generated, then V is finitely generated. If V is finitely generated, so is $\overline{V}$.

Theorem 4.4.2: Hilbert Basis Theorem

Let R be a noetherian ring. The polynomial ring $R[x]$ is noetherian.

Proposition 4.4.2: Quotients of Noetherian

Let R be a noetherian ring, and let I be an ideal of R. Any ring that is isomorphic to the quotient ring $\overline{R} = R/I$ is noetherian.

Corollary 4.4.3

Let P be a polynomial ring in a finite number of variables over the integers/field. Any ring R that is isomorphic to the quotient ring P/I is noetherian.

Lemma 4.4.2

Let R be a ring, let I be an ideal of the polynomial ring $R[x]$. The set A whose elements are the leading coefficients of the nonzero polynomials in I, together with the zero element of R, is an ideal of R, the **ideal of leading coefficients**.

4.5 Structure of Abelian Groups

Definition 4.5.1: Direct Sum of Modules

Let $W_1, \ldots, W_k$ be submodules of an R-module V. Their sum is the submodule that they generate;

$$W_1 + \ldots + W_k = \{v \in V \mid v = w_1 + \ldots + w_k \quad w_i \in W_i\}$$

If $W_1 + \ldots + W_k = V$ AND they are independent ($w_1 + \ldots + w_k = 0 \iff w_i = 0$) then V is the direct sum of the submodules.

Similarly, $V = W_1 \bigoplus W_2 \iff W_1 + W_2 = V, \quad W_1 \cap W_2 = 0$.

Theorem 4.5.1: Structure Theorem for Abelian Groups

A finitely generated abelian group V is a direct sum of cyclic subgroups $C_{d_1}, \ldots, C_{d_k}$ and a free abelian group L:

$$V = C_{d_1} \bigoplus \ldots \bigoplus C_{d_k} \bigoplus L,$$

where the order d_i of C_{d_i} is greater than one, and $d_i \mid d_{i+1}$ for $i < k$.

Theorem 4.5.2: Structure Theorem (Alternate Form)

Every finite abelian group is a direct sum of cyclic groups of prime power orders.

Theorem 4.5.3: Uniqueness for Structure Theorem

Suppose that a finite abelian group V is a direct sum of cyclic groups of prime power orders $d_j = p_j^{r_k}$. The integers d_j are uniquely determined by the group V.

4.6 Analogues for Polynomial Rings and Linear Operators

Theorem 4.6.1

Let $R = F[t]$ be a polynomial ring in one variable over a field F and let A be an $m \times n$ R-matrix. There are products Q, P of elementary R-matrices such that

$$A' = Q^{-1}AP$$

is diagonal, each non-zero diagonal entry d_i of A' is a monic polynmial, and $d_1 \mid \ldots \mid d_k$.

Definition 4.6.1: Cyclic Modules

We define a **cyclic R-module** C, where R is any ring, to be a module that is generated by a single element v.

Then there is a surjective homomorphism $\varphi : R \to C$ defined by $r \mapsto rv$. The kernel of φ is a submodule of R, an ideal I. Therefore, C is isomorphic to the R-module R/I. When $R = F[t]$, the ideal I will be principal.

Theorem 4.6.2: Structure Theorem for Modules over Polynomial Rings

Let $R = F[t]$ be the ring of polynomials in one variable with coefficients in a field F. Let V be a finitely generated module over R. Then V is a direct sum of cyclic modules $C_1, C_2, \ldots, C_k$ and a free module L, where C_i is isomorphic to $R/(d_i)$, the elements $d_1, \ldots, d_k$ are monic polynomials of positive degree and satisfy both (but not simultaneously)

- $d_1 \mid d_2 \mid \ldots \mid d_k$
- Each d_i is a power of a monic irreducible polynomial