

Notes for CS203

Contents

Contents	i
1 Groups	1
1.1 Introduction	2
1.2 Subgroups and Group Morphisms	4
1.3 Effect of ψ on G - Quotienting	5
1.4 Finite Groups	7
2 Rings	9
2.1 Introduction	9
2.2 Units in Rings	10
2.3 Defining primes in R	11
2.4 Solutions of $y^3 = x^2 + 2$	11
2.5 Ideals	12
2.6 Ring Properties, Morphisms and Quotienting	14
3 Fields	19
3.1 Introduction	19
3.2 Finite Fields	20

Chapter 1

Groups

You also get dramatic advances when you spot that you can leave out part of the problem. Algebra, for instance (and hence the whole of computer programming), derives from the realisation that you can leave out all the messy, intractable numbers.

Douglas Adams (The Salmon of Doubt: Hitchhiking the Galaxy One Last Time, 2002)

The term Group was first used by Galois ¹ in his quest of solutions of roots of polynomial equations of degrees higher than four. The development of group theory has three main roots, the theory of algebraic equations, geometry and number theory. Today, group theory and abstract algebra in general sees many uses in the field computer science, from cryptography and coding theory, down to finding computationally faster methods to multiply integers.

¹Galois was a brilliant mathematician, but he unfortunately was killed in a duel when he was just 20, which might have had been motivated by a conflict arising from a romantic entanglement, or his political involvements.

1.1 Introduction

Definition 1. Let G be a set. Let $\circ : G \times G \rightarrow G$ be a map that satisfies the following properties:

- *Closure:* For all $a, b \in G$, we have $a \circ b \in G$.
- *Associativity:* For all $a, b, c \in G$, we have $(a \circ b) \circ c = a \circ (b \circ c)$
- *Identity:* There exists an element in G , say e that satisfies $a \circ e = e \circ a = a$, for all $a \in G$.
- *Inverse:* For every element $a \in G$, there exists a unique element b that satisfies $a \circ b = b \circ a = e$, where e is the identity, as described above.

Such a set G , if the operation satisfies the above properties, is called a group under \circ . Note that the third condition forces the identity to be unique. The proof for this is trivial, and has been left as an exercise.² If this were not the case, the fourth condition would not have made sense.

Put in words, a group is a set, along with a binary operation that is closed under the operation, the operation is associative in the elements of the set, there exists an identity for the operation in the set, and all elements of the set have an inverse.

Further, if the elements satisfy the property that for all $a, b \in G$, $a \circ b = b \circ a$, then the group is called an **abelian** group, or a commutative group. If not, then the group is called **non-abelian**, or non commutative.

A number of examples and counterexamples are presented below to reinforce the concept of the group, and to set up notation for the rest of this text.

Examples

- *Example 1:* \mathbb{Z} , the set of all integers, is a group under the addition operation. It is easy to see that all the group properties are satisfied by addition, with 0 being the identity, and the inverse of any number a being $-a$. It is also easy to see that this group is abelian. Further, the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all similarly sets under addition (the set of rationals, reals, and complex numbers respectively).
Note however, that \mathbb{N} , the set of natural numbers is NOT a group, since no element except the identity 0 has an inverse.

²Hint: Attempt a proof by contradiction

- *Example 2:* Similarly, the set of all $n \times m$ matrices with entries from \mathbb{Z} , under the operation of matrix addition is an abelian group.
- *Example 3:* The set of all non-zero rational numbers, \mathbb{Q}^* is an abelian group under the operation of multiplication, with identity 1. Note however, that the set \mathbb{Z}^* is not a group, since integers do not have integer multiplicative inverses. Also, we require that our set contains all rationals EXCEPT 0, since 0 cannot have a multiplicative inverse.
- *Example 4:* The set of all invertible $n \times n$ matrices with entries in \mathbb{Q} is a group under the operation of matrix multiplication. The $n \times n$ identity matrix I acts as the identity element. Further, since the product of invertible matrices is invertible, the operation is closed. This group is non-abelian.
- *Example 5:* Let $S_n = \{f | f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}\}$, such that every f is a permutation. S_n is a group under the operation of composition.
- *Example 6:* Define $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. This set is an abelian group under the operation $+$ (mod n).
- *Example 7:* Define $\mathbb{Z}_n^* = \{1, \dots, n-1\}$. This set is an abelian group under the operation $*$ (mod n), when n is prime. Note that this is not the case when n is composite. For example, in \mathbb{Z}_6^* , $2 * 3 \equiv 0 \pmod{6}$, which is not in the set, that is, closure is violated.
- *Example 8:* For composite numbers, we redefine $\mathbb{Z}_n^* = \{m | 1 \leq m \leq n, \gcd(m, n) = 1\}$. Under this definition, \mathbb{Z}_n^* is an abelian group under modular multiplication for all n .
- *Example 9:* The set of complex n^{th} roots of unity for any n is an abelian group under multiplication.
- *Example 10:* Consider the curve $y^2 = x^3 - x$. Let the set E be the set $\{\text{All points on the curve}\} \cup \{\infty\}$. For any $p, q \in E$, define $p+q$ as first joining p and q by a line, getting the unique point of intersection of the line with the curve itself, and then taking its mirror with respect to the x axis. E is then a group under the above operation.

Now that a large number of examples have been presented, the reader should have a basic intuitive idea of a group. In the next sections, we study the structure of groups, and mapping between groups.

1.2 Subgroups and Group Morphisms

Definition 2. Let G be a group. A set $H \subseteq G$ is a **subgroup** of G if H is a group under the same operation.

More verbosely, H is a subgroup of G if it is a subset of G , and the following three properties hold.

- $e \in H$, where e is the identity element of G .
- If $a, b \in H$, then $a \circ b \in H$, where \circ is the operation under which G is a group.
- If $a \in H$, and $a \circ b = e$ in G , then $b \in H$. In other words, if an element is in a subgroup, so is its inverse.

Some examples of subgroups are:

- *Example 1:* The set \mathbb{Z} under addition is a subgroup of \mathbb{Q} , which itself is a subgroup of \mathbb{R} , which further is a subgroup of \mathbb{C} .
- *Example 2:* For any group G , G is a subgroup of itself. G is called the improper subgroup of G .
- *Example 3:* For any group G , the set consisting of only the identity element is a subgroup. This is called the trivial subgroup of G . All other subgroups are called non-trivial.
- *Example 4:* Let G be the group of all $n \times n$ invertible matrices under multiplication. Consider the subset of all matrices that have determinant 1. This forms a subgroup of G . Similarly, the subset of all matrices that have determinant ± 1 also form a subgroup of G . Both of these subgroups are proper and non-trivial.

Definition 3. Let G and H be groups under the operations $+$ and \oplus respectively. Let $\psi : G \rightarrow H$. Mapping ψ is a **homomorphism** if for all $a, b \in G$, we have $\psi(a + b) = \psi(a) \oplus \psi(b)$. Further, if ψ is also one-one and onto, then ψ is called an **isomorphism**. In this case, we generally write $G \cong H$.

For example, consider the group \mathbb{Z} of integers under addition, and the group \mathbb{Q}^* of non zero rationals under multiplication. Let the map $\psi : \mathbb{Z} \rightarrow \mathbb{Q}^*$, $\psi(n) = 2^n$. ψ is a homomorphism, as for all $a, b \in \mathbb{Z}$, $2^{a+b} = 2^a \times 2^b$.

Let ψ be a homomorphism from G to H .

Lemma 1. Let $\widehat{H} = \{b | \psi(a) = b, a \in G\}$. \widehat{H} is a subgroup of H .

Proof. If $b, c \in H$, then we have $x, y \in G$ such that $\psi(x) = b, \psi(y) = c$. Then $\psi(x + y) = b \oplus c$ by property of homomorphisms. \widehat{H} is thus closed. Associativity is inherited from H . Homomorphisms necessarily map identities to identities. This can trivially be checked by noting that $\psi(e_g + e_g) = \psi(e_g) = \psi(e_g) \oplus \psi(e_g)$ where e_g is the identity of G . This gives us existence of identity in \widehat{H} . Finally, if $\psi(x) = a$, then the image of the inverse of x is the inverse of a . This can be derived again by using the fact that identities are mapped to identities. \square

If ψ is a one-one map, then clearly ψ gives an isomorphism between G and \widehat{H} . If not, then consider the set $\widehat{G} = \{a | a \in G, \psi(a) = e_h\}$, where e_h is the identity of H .

Lemma 2. \widehat{G} is a subgroup of G .

Proof. Closure holds since if for $a, b \in \widehat{G}$ we have $\psi(a) = \psi(b) = e_h$, then $\psi(a + b) = \psi(a) + \psi(b) = e_h + e_h = e_h$. Associativity is inherited from G . Identity exists because homomorphisms map identities to identities. Finally for any $a \in \widehat{G}$, we have that the image of the inverse of a is the inverse of the image of a , or the inverse of e_h , which is e_h itself. \square

This subgroup is called the **kernel** of ψ .

1.3 Effect of ψ on G - Quotienting

For each b in \widehat{H} , let by $[b] = \{a | a \in G, \psi(a) = b\}$. In this notation, the kernel of ψ is clearly represented by $[e_h]$.

Lemma 3. For each $b \in \widehat{H}$, we have $[b] = a + \widehat{G}$ for some $a \in G$. Here, $a + \widehat{G}$ refers to the set of all elements that we get by adding a to each element of \widehat{G} , or more formally $a + \widehat{G} = \{b | b = a + g, g \in \widehat{G}\}$.

Proof. Let $\psi(a_1) = \psi(a_2) = b$. This gives us that $\psi(a_1 - a_2) = 0 \Rightarrow a_1 - a_2 \in \widehat{G}$, where $-a_2$ refers to the inverse of a_2 in G . This gives us $a_1 \in a_2 + \widehat{G}$. But a_1 was picked arbitrarily. We can repeat the above argument with any element from $[b]$ in place of a_1 , and we always get, for all elements a , $a \in a_2 + \widehat{G}$. This completes the proof. \square

Further, also note that for every element a that belongs to $a_2 + \widehat{G}$, we have $\psi(a) = \psi(a_2) + \psi(g)$ for some $g \in \widehat{G}$. Every element of $a_2 + \widehat{G}$ maps

to b under ψ . Thus, the elements of G are partitioned, and each can be recognized by an element of \widehat{H} (for every element $b \in \widehat{H}$, the corresponding partition is $[b]$) or by a single element of each partition (implicitly adding G will give the whole class). The above gives us an equivalence relationship, with $a_1 R a_2 \Leftrightarrow \psi(a_1) = \psi(a_2)$.

Define operator \boxplus be defined as $[b_1] \boxplus [b_2] = [b_1 \oplus b_2]$.

Define $G/\widehat{G} = \{[b_i] | b_i \in \widehat{H}\}$.

Lemma 4. G/\widehat{G} is a group under \boxplus .

Proof. Closure is clear from the definition of \boxplus . For associativity, we have

$$\begin{aligned} ([a] \boxplus [b]) \boxplus [c] &= [a \oplus b] \boxplus [c] \\ &= [(a \oplus b) \oplus c] \\ &= [a \oplus (b \oplus c)] \\ &= [a] \boxplus [b \oplus c] \\ &= [a] \boxplus ([b] \boxplus [c]) \end{aligned}$$

$[e_h]$ clearly acts as the identity. Further, for any $[a]$, the inverse of $[a]$ is simply $[b]$ such that b is the inverse of a in H . This follows since $[a] \boxplus [b] = [a \oplus b] = [e_h]$. \square

It is quite obvious that G/\widehat{G} and H are isomorphic, with the map being one that sends $[b] \rightarrow b$.

The above formulation is known as the the **First Isomorphism Theorem**.

We now Quotient G with other subgroups and study the resulting structure.

Let G be an abelian group, and \widehat{G} be a subgroup of G .

For any $a \in G$, define $[a] = \{b | b \in G, b - a \in \widehat{G}\}$. For any $a_1, a_2 \in G$, either $[a_1] = [a_2]$ or $[a_1] \cap [a_2] = \phi$. Define $G/\widehat{G} = \{[a] | a \in G\}$. Define $[a_1] \boxplus [a_2] = [a_1 + a_2]$. G/\widehat{G} is a group under \boxplus . It is called the quotient group of \widehat{G} .

The element $a \in G$ is called the representative element of $[a]$ in the quotient group. The representative element is clearly not unique.

Examples

- *Example 1:* Consider the group \mathbb{Z} , and its subgroup $n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z} = \{[m]\}$, ie all numbers that are congruent to m modulo n . The most natural representative set is $0, 1, \dots, n-1$.
- *Example 2:* Consider the group \mathbb{Q}^* under multiplication and its subgroup $G = \{2^n | n \in \mathbb{Z}\}$. $\mathbb{Q}^*/G = \{[\alpha]\}$, where the representative set can be $\{\frac{n}{m}, n, m \in \mathbb{Z}, m \neq 0, m, n \text{ odd}\}$.
- *Example 3:* Consider the group of all $n \times n$ matrices under addition, and its subgroup, the set of all $n \times n$ upper triangular matrices. The quotient group of this subgroup can be represented by the set of all lower triangular matrices, with zero in their diagonals.
- *Example 4:* Consider the group \mathbb{Z}_6 , and its subgroup $G = \{0, 3\}$. $\mathbb{Z}_6/G = [m]$, where the representative set can be $0, 1, 2$. Note that this quotient group is isomorphic to \mathbb{Z}_3 .
- *Example 5:* Let the group be all two dimensional vectors over \mathbb{R} , with addition as the group operation. Let the subgroup be any line through the origin. The quotient group is the set $\{[\alpha, \beta]\}$ where a possible representative element can be the intersection of the new line with the x axis.

From this point onwards, we drop the unwieldy notation of using different symbols for representing group actions of various groups. All groups will generally be represented by G or H , with operation $+$. The context should make clear what group the operation is being performed on. Further, the identity element will be represented by 0 , and the inverse of an element a by $-a$.

1.4 Finite Groups

The **order** of a group is its cardinality, i.e the number of elements in its set. We represent the order of a group G by $|G|$, or $\text{ord}(G)$.

Theorem 1. *Let H be a subgroup of an abelian group G , with $\text{ord}(G) = l$. Then, $\text{ord}(H) | l$, and in particular, $l = \text{ord}(H) \times \text{ord}(G/H)$.*

Proof. H divides G into equivalence classes as discussed above, all of size $|H|$. This implies both that $\text{ord}(H) \mid \text{ord}(G)$ and that $\text{ord}(G) = \text{ord}(H) \times \text{ord}(G/H)$ \square

Similar to how the order for the group was defined, we can also define the order of an element $a \in G$ as follows:

For any $a \in G$, let $H_a = \{k \times a \mid k \in \mathbb{Z}\}$ where $k \times a$ denotes the addition of a to itself k times. Then, $\text{ord}(a) = \text{ord}(H_a)$. H_a is then a subgroup, and it is easy to see that it is isomorphic to $\mathbb{Z}_{\text{ord}(a)}$

H_a is more commonly denoted as $\langle a \rangle$. a is called a **generator** if $\langle a \rangle = G$.

Definition 4. Let G be a commutative group, and $a_1, a_2, \dots, a_k \in G$. This set is called a generator set if for all $b \in G$, we have $b = \sum_{i=1}^k k_i \times a_i$. Such a group is called finitely generated, and the set a_1, \dots, a_k is called the generator set.

We now give, without proof, a very powerful theorem about finite groups.

Theorem 2. *Structure Theorem for Finite Abelian Groups:* Let G be a finite abelian group of order l . Then, $G \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \dots \times \mathbb{Z}_{p_k^{e_k}}$ where p_i are primes, and e_i are integers such that $\prod p_i^{e_i} = l$.

Chapter 2

Rings

Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.

G. H. Hardy (A
Mathematician's Apology,
1940)

2.1 Introduction

Definition 5. $(R, +, *)$ is a ring if:

- R is a commutative group under $+$.
- R is closed under $*$, associative and has identity.
- For all $a, b, c \in R$ $a*(b+c) = a*b+a*c$ and similarly $(b+c)*a = b*a+c*a$

If $*$ is commutative, R is called a **commutative ring**.

Definition 6. $(F, +, *)$ is a field if:

- F is a commutative group under $+$.
- $F^* = F \setminus \{0\}$ is a commutative group under $*$.

- *Distributivity property holds.*

Fields will be studied more in detail in the subsequent chapter.

Examples

- *Example 1:* \mathbb{Z} is a commutative ring.
- *Example 2:* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.
- *Example 3:* \mathbb{Z}_n is a ring.
- *Example 4:* \mathbb{Z}_p is a field, when p is prime.
- *Example 5:* $n \times n$ matrices from \mathbb{Q} is a ring.
- *Example 6:* For any field F , vectors in F^n form a commutative ring, under componentwise operations.
- *Example 7:* $R[x]$, the set of all polynomials in x with coefficients from a ring R , is a ring under polynomial addition and multiplication. This can be extended to multivariate polynomials over R .
- *Example 8:* Let \mathcal{F} be the set of all continuous maps from $\mathbb{R} \rightarrow \mathbb{R}$. \mathcal{F} is a commutative ring, under the operations $+, *$ defined as $(f+g)(x) = f(x) + g(x)$ and $(f*g)(x) = f(x)*g(x)$ for all f, g .

2.2 Units in Rings

Note that from this point onwards, for ring elements a, b , we will use ab as shorthand for $a * b$.

Definition 7. Let R be a commutative ring. $a \in R$ is a unit if there exists an element b in R such that $ab = 1$.

Examples

Some very trivial examples of units are ± 1 in \mathbb{Z} and \mathbb{Z}^* in \mathbb{Z}_n .

A more interesting example follows. Consider $\mathbb{Z}[\sqrt{2}]$, which are the set of all polynomials, with $\sqrt{2}$ substituted for x . Elements of this ring are of the form $a_0 + a_1\sqrt{2} + \dots + a_i\sqrt{2}^i$ which can be easily generalized as $\{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\}$. For some $a + \sqrt{2}b$ to be a unit, we require $(a + \sqrt{2}b)(c + \sqrt{2}d) = 1$ for some c, d . This gives us $ac + 2bd + \sqrt{2}(ad + bc) = 1 \Rightarrow ad = -bc \Rightarrow d = -\frac{bc}{a}$

Substituting this back gives us $a^2 - 2b^2 = \frac{a}{c}$. Since a, b, c, d are integers, the above can only hold when $a = \alpha c$ and $b = -\alpha d$ for some α . This finally gives us $1 = (\alpha c - \sqrt{2}\alpha d)(c + \sqrt{2}d) \Rightarrow \alpha(c^2 - 2d^2) = 1 \Rightarrow \alpha = \pm 1, (c^2 - 2d^2) = \pm 1$. The solutions to the above equation give us all units, and it can be shown that the only possible units are the powers of $(1 + \sqrt{2})$.

2.3 Defining primes in R

We now try and define primes in rings.

The first definition we can try is that $a \in R$ is prime if whenever $a = bc$, then either b or c are units. This definition is clearly just an extension of the definition of primes over integers, but is not very adequate, since some rings, like \mathbb{Z}_n have no primes under this definition, except the units.

Definition 2: $a \in R$ is prime if whenever a divides bc , it either divides b or c . Consider \mathbb{Z}_6 . 2 can be written as $2 = 2 * 4, 2 * 1, 4 * 5$, and it is easily checked that 2 always divides one of the elements of the product. Thus, 2 is a prime under this definition.

$a \in R$ is defined as **irreducible** if whenever $a = bc$, either b or c is a unit, and a is not.

2.4 Solutions of $y^3 = x^2 + 2$

We now use the tools developed so far to try and find the solutions of this equation. The proof here is just a rough sketch, and the details can be easily filled out.

We can factorize $x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$. Consider $\mathbb{Z}[i\sqrt{2}]$, which has elements of the form $\{a + i\sqrt{2}b | a, b \in \mathbb{Z}\}$. If we assume that $y, (x + i\sqrt{2}), (x - i\sqrt{2})$ are all irreducible, then there cannot be any solutions. Thus y needs to be reducible.

Starting with the assumption that $y = (a + i\sqrt{2}b)(c + i\sqrt{2}d)$ gives us that y needs to be of the form $y = (m + i\sqrt{2}n)(m - i\sqrt{2}n)$ for some m, n . These are called conjugates of each other.

We have $(m - i\sqrt{2}n)^3(m + i\sqrt{2}n)^3 = (x + i\sqrt{2})(x - i\sqrt{2})$. Whatever we equate for $(x + i\sqrt{2})$, we need to assign to $(x - i\sqrt{2})$ its conjugate. This gives us two cases, $(x + i\sqrt{2}) = (m + i\sqrt{2}n)^3$ and $(x + i\sqrt{2}) = (m + i\sqrt{2}n)^2(m - i\sqrt{2}n)$. The remaining two cases are similar to these, and are ignored here.

Case I: gives us $(x + i\sqrt{2}) = (m + i\sqrt{2}n)^3 = m^3 - 6n^2m + (3m^2n - 2n^3)i\sqrt{2}$ which further gives us $x = m^3 - 6n^2m$ and $1 = 3m^2n - 2n^3 = 1$. Applying

the constraint that m, n are integers, we get $n = 1$ and $a = \pm 1$ and thus $x = \pm 5$.

Case II: gives us $x = m(m^2 + 2n^2)$ and $1 = n(m^2 + 2n^2)$. The integer solutions again give us $n = \pm 1$ which then gives $m^2 + 2 = \pm 1$, which has no solutions.

This shows that solution to the equation include $x = \pm 5, y = 3$.

2.5 Ideals

In this section, a number of lemma and definition are presented.

Consider the ring $\mathbb{Z}[i\sqrt{5}]$. In this ring, $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$. $3, (2 + i\sqrt{5}), (2 - i\sqrt{5})$ are all irreducible, therefore, we cannot cancel anything on either side. $\mathbb{Z}[i\sqrt{5}]$ is said to not admit unique factorization.

Division in Rings

Ring elements satisfy the following two properties:

- For all $a, b, c \in R$ if $a|b$ and $a|c$ then $a|bc$.
- If $a|b$ then $a|bc$.

Ideal Numbers and Ideals

Attempts to fix the problem of Unique Factorizing led to the development of ideal numbers, which generalized to ideals.

We represent elements $a \in Ra$ by all b such that $a|b$. Let all the b for a given a be represented by (a) .

Lemma 5. *If $(a) = (c)$ then $a = c \times u$ for some unit u .*

Definition 8. *$I \subseteq R$ is an ideal if the following hold:*

- $(I, +)$ is a subgroup of $(R, +)$.
- For all $a \in I$ and $b \in R$, $ab \in I$.

In the ring $\mathbb{Z}[i\sqrt{5}]$, some ideals are $(3), (2 + i\sqrt{5}), (2 - i\sqrt{5})$. Further, consider $(3, 2 + i\sqrt{5}) = \{3a + (2 + i\sqrt{5})b | a, b \in R\}$. The fact that this is an ideal is quite clear.

Given ideal I of a ring, and a subset S of I , $S \subseteq I$, I is generated by S , if for every $a \in I$, $a = \sum \alpha_i \beta_i$, for $\alpha_i \in R$ and $\beta_i \in S$. Elements of S are called generators of I . S can be either finite or infinite.

Ideal I is called a **principal ideal** if it can be generated by a single element.

Let I_1, I_2 be ideals of R . Then $I_1 * I_2 = \{\Sigma a_i b_i | a_i \in I_1, b_i \in I_2\}$

Lemma 6. $I_1 * I_2$ is an ideal.

Proof. If $c \in I_1 * I_2$ and $\alpha \in R$, then $\alpha c = \alpha \Sigma a_i b_i = \Sigma (\alpha a_i) b_i$. \square

Definition 9. Ideal I is called **prime** if for every I_1, I_2 , $I = I_1 * I_2 \Rightarrow I_1 = (1)$ or $I_2 = (1)$.

Lemma 7. For any ideal I , $I * (1) = I$.

Proof. $a \in I \Rightarrow a = a \times 1 \in I * (1)$
 $a \in I * (1) \Rightarrow a = \Sigma a_i b_i$. $a_i \in I, b_i \in R$ by properties of ideals. This implies $a_i b_i \in I \Rightarrow \Sigma a_i b_i \in I$. \square

Examples in $\mathbb{Z}[i\sqrt{5}]$

In $\mathbb{Z}[i\sqrt{5}]$, $(3) = (3, 2 + i\sqrt{5}) * (3, 2 - i\sqrt{5})$.

Proof. First we need to show that $3 \in (3, 2 + i\sqrt{5}) * (3, 2 - i\sqrt{5})$. Consider $3 * (2 - i\sqrt{5}), 3 * (2 + i\sqrt{5}), -(2 - i\sqrt{5}) * (2 + i\sqrt{5})$ all that belong to $(3, 2 - i\sqrt{5}) * (3, 2 + i\sqrt{5})$. Their sum is 3.

Second, consider an element of $(3, 2 - i\sqrt{5}) * (3, 2 + i\sqrt{5})$, $(3a + (2 + i\sqrt{5})b) * (3c + (2 - i\sqrt{5})d) = 9ac + 9bd + 3a(2 - i\sqrt{5}) + 3c(2 + i\sqrt{5}) \in (3)$. \square

Similarly, in $\mathbb{Z}[i\sqrt{5}]$, $(2 + i\sqrt{5}) = (3, 2 + i\sqrt{5}) * (3, 2 + i\sqrt{5})$ and $(2 - i\sqrt{5}) = (3, 2 - i\sqrt{5}) * (3, 2 - i\sqrt{5})$.

Examples of Ideals in other Rings

- *Example 1:* In \mathbb{Z} , $(2), (3) \dots$ are the principal ideals. There are no other ideals, since for any $a, b \in \mathbb{Z}$, we have $(a, b) = (gcd(a, b))$. This is given by the fact that the gcd of any two numbers is an integer linear combination of the numbers.
- *Example 2:* In \mathbb{Z}_n , $(m) = \mathbb{Z}_n$ if $gcd(m, n) = 1$. In \mathbb{Z}_6 , $(2) = \{0, 2, 4\}$, $(3) = \{0, 3\}$
- *Example 3:* In $\mathbb{Z}[x]$, the ideal $(p(x))$ for any polynomial $p(x)$ is just all its multiples.
- *Example 4:* In $\mathbb{Z}[x, y]$, consider the ideal (x, y) . It consists of all polynomials that have 0 as the constant term.

- *Example 5:* Consider the polynomial generated by (x, y) in $\mathbb{Q}[x, y]$. This ideal has the property that the only ideal larger than it is (1) .

Proof. Consider an ideal I such that $(x, y) \subsetneq I$. Then $p(x, y) = c + q(x, y)$ such that $q(x, y) \in (x, y), c \neq 0$. This gives us $c = p(x, y) - q(x, y) \in I \Rightarrow 1 \in I \Rightarrow I = (1)$. \square

Definition 10. Ideal I is **maximal** if (1) is the only ideal larger than I .

- *Example 6:* Consider the ring C_x , the set of all continuous functions from $\mathbb{R} \rightarrow \mathbb{R}$. $I = \{f \in C_x, f(0) = 0\}$.

2.6 Ring Properties, Morphisms and Quotienting

Definition 11. Ring R is called a **Dedekind Domain** if

- R is an integral domain. (If $a * b = 0$ then $a = 0$ or $b = 0$)
- R is integrally closed.
- All prime ideals of R are maximal.
- All ideals of R are finitely generated

Theorem 3. If R is a Dedekind Domain, then every ideal I of R can be uniquely written as a product of prime factors.

Definition 12. Let R_1 and R_2 be two rings. Function $\phi : R_1 \rightarrow R_2$ is a ring homomorphism if

- For all $a, b \in R_1, \phi(a + b) = \phi(a) + \phi(b)$
- For all $a, b \in R_1, \phi(a * b) = \phi(a) * \phi(b)$

The above two properties lead to the following:

$$\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0) \Rightarrow \phi(0) = 0.$$

$\phi(1) = \phi(1 * 1) = \phi(1) * \phi(1) \Rightarrow \phi(1) * (\phi(1) - 1) = 0$. This implies that $\phi(1) = 1$ or $\phi(1) = 0$. If $\phi(1) = 0$ then $\phi(a) = \phi(1 * a) = \phi(1) * \phi(a) = 0, \forall a$.

Definition 13. The kernel of ϕ is $A \subseteq R$ such that $\phi(a) = 0$ for all $a \in A$. It is represented as $\ker(\phi)$.

$\ker(\phi)$ is an additive subgroup of R . Further, if $a \in \ker(\phi)$ then we have $\phi(a * b) = \phi(a) * \phi(b) = 0 * \phi(b) = 0 \Rightarrow \ker(\phi)$ is an ideal of the ring.

We can further define equivalence classes in R , induced by ϕ , as we did for groups. The classes are represented by $\ker(\phi), \ker(\phi) + a_1, \ker(\phi) + a_2 \dots$ for elements $a_1, a_2 \notin \ker(\phi)$.

In general, for an ideal A , we have $R/A = \{A, a_1 + A, a_2 + A, \dots\}$.

Lemma 8. R/A is a ring where $(a_1 + A) + (a_2 + A) = (a_1 + a_2) + A$ and $(a_1 + A) * (a_2 + A) = (a_1 * a_2) + A$.

Proof. R/A is a commutative group under $+$, because both R and A are commutative groups under addition. Further considering multiplication, $(a_1 + \alpha_1) * (a_2 + \alpha_2) = a_1 * a_2 + a_1 * \alpha_2 + \alpha_1 * \alpha_2 + a_2 + \alpha_1$. We have $a_1 * \alpha_2, a_2 + \alpha_1, \alpha_1 + \alpha_2 \in A$ which means $(a_1 + \alpha_1) * (a_2 + \alpha_2) \in (a_1 + a_2) + A$ independent of the representative element. Finally, distributivity is clear from the distributive property of R . \square

Based on whether we quotient by a maximal ideal, prime ideal or principal ideal, R/A has different properties.

Quotienting by maximal ideals

Lemma 9. When I is a maximal ideal, R/I is a field.

Proof. Let $a + I \in R/I, a \neq 0$. Further, let $0 = I, 1 = 1 + I$. We need to find the inverse of R/I . Define $J = (a, I)$, the ideal containing both a and I . $I \subsetneq J$ since $a \notin I$. Since I is maximal, $J = (1)$. The elements of J are $a * b + \alpha$ for $b \in R, \alpha \in I$. Since $1 \in J, 1 = a * b + \alpha$. In R/I we get $(a + I) * (b + I) = (a * b) + I = 1 + I \Rightarrow (a + I)^{-1} = (b + I)$. \square

Defining real numbers using maximal ideals

We now define real numbers using quotienting using maximal ideals.

Definition 14. $(a_0, a_1, a_2, \dots), a_i \in R$ is a **Cauchy Sequence** if for all $\epsilon > 0, \epsilon \in \mathbb{Q}, \exists m > 0, m \in \mathbb{Z}$ such that for all $n \geq m, n \in \mathbb{Z}, |a_n - a_m| < \epsilon$.

For example, $\{\frac{3}{1}, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \frac{31415}{10000}, \dots\}$ is a cauchy sequence that converges to π .

Theorem 4. Let \mathcal{R} denote the set of all cauchy sequences. \mathcal{R} is a ring under componentwise addition and multiplication.

Proof. Associativity and identity are borrowed from the ring of real numbers. We need to show closure.

Let $S_1 = (a_0, a_1, a_2, \dots)$ and $S_2 = (b_0, b_1, b_2, \dots)$. Fix an $\epsilon > 0$. Let $m_1 \in \mathbb{Z}$ such that $|a_n - a_{m_1}| < \frac{\epsilon}{4} \forall n \geq m_1$. Similarly $m_2 \in \mathbb{Z}$ such that $|b_n - b_{m_2}| < \frac{\epsilon}{4} \forall n \geq m_2$. Let $m = \max\{m_1, m_2\}$.

We have $|a_n + b_n - a_m - b_m| \leq |a_n - a_m| + |b_n - b_m|, \forall n > m$. Further, $|a_n - a_m| + |b_n - b_m| \leq |a_n - a_{m_1}| + |a_{m_1} - a_m| + |b_n - b_{m_2}| + |b_{m_2} - b_m| \leq \frac{\epsilon}{4} + \frac{\epsilon}{4} + \frac{\epsilon}{4} + \frac{\epsilon}{4} \leq \epsilon$. Therefore, $S_1 + S_2$ is cauchy.

Similarly, by picking the right m , we can prove that $S_1 * S_2$ is also cauchy. This has been left as an exercise. \square

Let I be the set of all cauchy sequences converging to 0.

Theorem 5. I is a maximal ideal of \mathcal{R} .

Proof. I is clearly a commutative group under addition. Further, for any $S \in I, S' \in \mathcal{R}, S * S'$ clearly converges to 0.

Let $S' = (b_0, b_1, \dots) \in \mathcal{R}$ such that $S' \notin I$. Since $S' \notin I$, there exists $\delta > 0$ such that for all $n \geq n_0$ for some n_0 we have $|b_n| > \delta$. Let J be the ideal containing I and S' and $k = \max\{|b_i|, 0 \leq i \leq n_0\}$. Let t be the cauchy sequence with $k + \delta$ as the first n_0 elements, and 0 as the rest of the elements. $t \in I \Rightarrow S' + t \in J$. All elements of $S' + t = (c_0, c_1, \dots)$ are atleast as big as δ in magnitude. Define $t' = (\frac{1}{c_0}, \frac{1}{c_1}, \dots)$. t' is cauchy, since $|\frac{1}{c_n} - \frac{1}{c_m}| = \frac{|c_m - c_n|}{|c_m c_n|} \leq \frac{|c_n - c_m|}{\delta^2} \leq \frac{\epsilon}{\delta^2}$, since $S' + t$ is cauchy.

Therefore, we have $t' \in \mathcal{R}$ and thus $t' * (S' + t) \in J \Rightarrow (1, 1, \dots) \in J \Rightarrow J = \mathcal{R}$. \square

$\mathbb{R} = \mathcal{R}/I$ is thus a field, and it is exactly the field of real numbers. This is because, there is exactly one sequence in it converging to every real number.

The above exercise can be repeated with different valuations to get fields such as the the field of p-adics.

Other Examples of Ring Quotienting

- *Example 1:* Consider the ring $\mathbb{Z}[i\sqrt{5}]$ and the ideal $(3, 2 + i\sqrt{5})$. The ring is a dedekind domain, therefore $(3, 2 + i\sqrt{5})$, which is prime, is also maximal. An arbitrary element of the ring is $a + i\sqrt{5}b = (a - 2b) + (2 + i\sqrt{5})b$. $a - 2b$ is an integer, and thus can be written as $\gamma + 3c$ where γ is either 0, 1 or 2. Thus, an arbitrary element is of the form $\gamma + 3c + (2 + i\sqrt{5})b$. When quotienting with $(3, 2 + i\sqrt{5})$, everything except γ is absorbed away. Therefore, $\mathbb{Z}[i\sqrt{5}]/(3, 2 + i\sqrt{5}) \cong \mathbb{Z}_3$.

- *Example 2:* Consider the ring \mathbb{Z} and ideal (m) . Then $\mathbb{Z}/(m) \cong \mathbb{Z}_m$. If we consider (p) such that p is prime, then (p) is maximal, the proof of which follows from the fact that the *gcd* of any two numbers is their integer linear combination. This gives us the fact that $\mathbb{Z}/(p)$ is a field, and is denoted by \mathbb{F}_p .
- *Example 3:* $F[x]$ where F is a ring. All ideals can be shown to be principal. Consider a polynomial $q(x)$. $F[x]/(q(x))$ is the ring of all polynomials of degree less than the degree of $q(x)$, with operations done modulo $q(x)$. If $q(x)$ is irreducible, then $(q(x))$ is maximal and the quotient ring is a field.

In particular, if $F[x]$ is $\mathbb{R}[x]$ and $q(x) = x^2 + 1$, then the quotient field is isomorphic to \mathbb{C} .

- *Example 4:* Take $F[x, y]/(x^2 + y^2 + 1)$. $(x^2 + y^2 + 1)$ is a principal ideal. Consider two elements that belong to the same class, q_1, q_2 . $q_1 - q_2 \in (x^2 + y^2 + 1) \Rightarrow q_1 - q_2 = (x^2 + y^2 + 1) * p(x, y)$ for some polynomial p . This implies that q_1, q_2 take on the same values on the circle $x^2 + y^2 + 1$. Put another way, the quotient group captures polynomials that are the same over the given curve, here the circle.

Prime and Irreducible Ideals

Definition 15. Ideal I of ring R is **prime** if for every $a, b \in R$, if $a * b \in I$, then $a \in I$ or $b \in I$.

Definition 16. Ideal I of ring R is **irreducible** if for every pair of ideals I_1, I_2 of R , if $I = I_1 * I_2$ then either $I_1 = (1)$ or $I_2 = (1)$.

Lemma 10. Let R be a ring, and I a prime ideal. Then R/I is an integral domain.

Proof. Let $a + I, b + I \in R/I$ such that $(a + I) * (b + I) = I \Rightarrow ab + I = I \Rightarrow ab \in I$. This implies that either a or b is in I , which means one of $(a + I), (b + I)$ is zero. \square

Chapter 3

Fields

Algebra is generous; she often
gives more than is asked of her.

Jean d'Alembert

This chapter first lists a few general properties of fields, followed by a discussion of finite fields in particular.

3.1 Introduction

Theorem 6. *A field has no ideals except (0) and (1) .*

Theorem 7. *If ϕ is a homomorphism between two fields, then it is either trivial or one-one.*

Both of the above theorems have very simple proofs that have been left as exercises.

Theorem 8. *Let $p(x)$ be a polynomial over a field F with degree d . Then $p(x)$ has at most d roots in F .*

Proof. Proof by strong induction.

Inductive Hypothesis: A polynomial of degree d over a field has at most d roots.

Base Case: For $d = 1$, $p(x) = ax + b \Rightarrow x = -\frac{b}{a}$.

Inductive Step: Let the inductive hypothesis hold for all numbers from 1 to $d - 1$. Let α be a root of $p(x)$, $\alpha \in F$. $p(x) = p(x) - p(\alpha) = \sum_i a_i x^i - \sum_i a_i \alpha^i = (x - \alpha) \sum_i a_i \frac{x^i - \alpha^i}{x - \alpha} = (x - \alpha)p'(x)$, where $p'(x)$ has degree $d - 1$. By induction, $p'(x)$ has at most $d - 1$ roots, and $p(x)$ has d roots. Further, any

$\beta \neq \alpha$ that is not a root of $p'(x)$ cannot be a root of $p(x)$ since fields are integral domains. Thus a degree d polynomial has at most d roots. \square

Definition 17. A field F where every polynomial of degree d has exactly d roots is called an **algebraically closed field**.

Definition 18. Let F be a field. The characteristic of F is the smallest integer n such that $\underbrace{1 + \cdots + 1}_{n \text{ summands}} = 0$.

Lemma 11. The characteristic of a field is either 0 or prime.

Proof. Suppose $\text{char}(F) = n$, and $n = ab$. Then $\underbrace{1 + \cdots + 1}_{n \text{ summands}} = 0$. This implies $\underbrace{1 + \cdots + 1}_{a \text{ summands}} * \underbrace{1 + \cdots + 1}_{b \text{ summands}} = 0$. Since fields are integral domains, one of the terms needs to be zero, which contradicts the fact that n is the smallest integer for which the property holds. \square

For example, consider the field \mathbb{Z}_p where p is prime. This is a field of characteristic p , and is usually denoted by \mathbf{F}_p . Further, consider an irreducible of degree d in \mathbf{F}_p , $q(x)$. $\mathbf{F}_p[x]/(q(x))$ is a field of polynomials with elements in \mathbf{F}_p . This field has characteristic p too, and is denoted by \mathbf{F}_{p^d} .

3.2 Finite Fields

Theorem 9. Let \mathbf{F} be a finite field, with characteristic p . \mathbf{F} is then isomorphic to $\mathbf{F}_p[x]/(q(x))$ where $q(x)$ is an irreducible polynomial over \mathbf{F}_p .

Theorem 10. For every prime p and $d \geq 1$, there exists an irreducible of degree d .

Corollary 1. For every prime p and $d \geq 1$, there exists a unique finite field of size p^d which is denoted by \mathbf{F}_{p^d} .

Theorem 11. Let \mathbf{F} be a finite field. Then $\mathbf{F}^* = \mathbf{F} \setminus \{0\}$ is a cyclic group.

Proof. \mathbf{F}^* is finite, and commutative. From Structure Theorem we get that $\mathbf{F} \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \cdots \mathbb{Z}_{p_n^{e_n}}$

Assume $p_1 = p_2$. Consider $\gamma = (p_1^{e_1-1}\alpha, p_2^{e_2-1}\beta, 0, \dots, 0)$, $\alpha, \beta \in \mathbb{Z}_{p_1}$. There are p_1^2 such elements, and all of them are unique in \mathbf{F}^* . Further, for each γ , we get $\underbrace{\gamma + \cdots + \gamma}_{p_1 \text{ times}} = (0, 0, \dots, 0)$. Let $\hat{\gamma} \in \mathbf{F}^*$ correspond to γ .

We have $\widehat{\gamma}^{p_1} = 1$ for each γ . This gives us p_1^2 solutions to the polynomial $x^{p_1} - 1 = 0$. This contradicts Theorem 8. Therefore we have $p_i \neq p_j$ whenever $i \neq j$.

Consider $\delta = (1, 1, \dots, 1) \in \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \dots \mathbb{Z}_{p_n^{e_n}}$. δ has order that is divisible by $p_i^{e_i}$ for all i . Since all $p_i^{e_i}$ are relatively prime, δ is divisible by the product. Therefore $\text{ord}(\delta) \geq |\mathbf{F}^*| \Rightarrow \delta = |\mathbf{F}^*|$. Thus we can just find the element in \mathbf{F}^* that corresponds to $(1, 1, \dots, 1)$ and this acts as the required generator. \square