Scribe Notes for *Algorithmic Number Theory*
Class 3—May 20, 1998

Scribes: Scott A. Guyer, Duxing Cai, and Degong Song

Abstract

Algebraic structures such as groups, rings, and fields are useful to the study of number theory. Both groups and rings are reviewed covering material from Sections 2.8.1 through 2.8.2 in [1]. The topic of fields is left for the next class meeting.

1 Groups

A *group* $(S, \circ)$ is a non-empty set S with an associative binary operation $\circ$ such that there is an identity, and inverses exist for every element in the set. Groups can be written additively or multiplicatively. Given a group G and two elements $a, b \in G$, notation for both additive and multiplicative groups are shown in the following table.

	Additive	Multiplicative
operation	$a + b$	$a \cdot b$
identity	0	1
inverse	$-a$	a^{-1}
powers	ka	a^k

Example 1.1 The integers modulo n, denoted $\mathbb{Z}/(n)$, represent a group under addition. In particular,

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

where $\overline{i}$ is the set of integers congruent to i modulo n.

If the group operation is commutative, we call that group *abelian*. Two important types of groups are vector spaces and cyclic groups.

1.1 Vector Spaces

A Euclidean space over the set of reals $\mathbb{R}$ is an example of a vector space that is a group. In particular, for the Cartesian space $\mathbb{E}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$, if we define the addition operation on $\mathbb{E}^3$ by

$$(a_1, a_2, a_3) + (b_1, b_2, b_3) \quad = \quad (a_1 + b_1, a_2 + b_2, a_3 + b_3),$$

then $(\mathbb{E}^3, +)$ forms a group.

1.2 Cyclic Groups

We say that a group G is *cyclic* if there exists an element $g \in G$ such that

$$G = \{g^k : k \in \mathbb{Z}\}.$$

There are two flavors of cyclic groups (and for groups in general), infinite and finite. Infinite cyclic groups are isomorphic (denoted by $\cong$, see Section 2.8.1 in [1] for a definition) to $(\mathbb{Z}, +)$ and have the property that $g^i \neq g^j$ for all integers $i \neq j$ and no positive power of g is equal to 1. In contrast, for every finite cyclic group, there exists a positive integer n such that $g^n = 1$ and $g^i \neq 1$ for $1 \leq i < n$. In this case, the group is isomorphic to $\mathbb{Z}/(n)$.

Example 1.2 The group $\mathbb{Z}/(5) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ is a finite cyclic group. It is easy to see that there is a single element that generates the group. Consider the element $\bar{2}$.

$$\begin{aligned} \bar{2} + \bar{2} &= \bar{4} \\ \bar{4} + \bar{2} &= \bar{1} \\ \bar{1} + \bar{2} &= \bar{3} \\ \bar{3} + \bar{2} &= \bar{0} \\ \bar{0} + \bar{2} &= \bar{2} \end{aligned}$$

and the cycle repeats.

1.3 Decomposition and Construction of Groups

Groups can be formed from other groups by taking subgroups, factor groups, or direct products.

1.3.1 Subgroups

Given a group G, a set $H \subseteq G$ is called a *subgroup* if H itself is a group (under the same operation as G).

Example 1.3 Consider $G = \mathbb{Z}/(12)$. Let $H = \{k\bar{3} : k \in \mathbb{Z}\}$. Then $H = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ is a subset of G. Furthermore, H is the cyclic group generated by $\bar{3}$ and so H is a subgroup of G.

1.3.2 Factor Group

Let G be an abelian group and H a subgroup of G. We define an equivalence relation on G with respect to H by: for all $g_1, g_2 \in G$,

$$g_1 \equiv g_2 \pmod{H}$$

if and only if $g_1 - g_2 \in H$. The equivalence classes induced by this relation are called *cosets* of H in G. The set composed of these equivalence classes is the *factor group* G/H. G/H is an additive group with cardinality $|G|/|H|$.

Example 1.4 Let $G = \mathbb{Z}/(12)$ and $H = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$. G/H is the factor group with elements

$$\begin{aligned} \bar{0} + H &= H \\ \bar{1} + H &= \{\bar{1}, \bar{4}, \bar{7}, \bar{10}\} \\ \bar{2} + H &= \{\bar{2}, \bar{5}, \bar{8}, \bar{11}\}. \end{aligned}$$

Also, note that $G/H \cong \mathbb{Z}/(3)$.

1.3.3 Direct Products

Given groups $G_1, G_2, \ldots, G_n$, we define their *direct product* by

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i, 1 \leq i \leq n\}.$$

Under the operation that is computed componentwise, $G_1, G_2, \ldots, G_n$ forms a group with identity $(e_1, e_2, \ldots, e_n)$ where e_i is the identity in group G_i.

Example 1.5 Let $G_1 = \mathbb{Z}/(4)$ and $G_2 = \mathbb{Z}/(3)$. Then the direct product $G_1 \times G_2$ is the group $\mathbb{Z}/(4) \times \mathbb{Z}/(3)$. Note that this direct product is isomorphic to $\mathbb{Z}/(12)$. This is illustrated by the isomorphism $\phi : \mathbb{Z}/(12) \longrightarrow \mathbb{Z}/(4) \times \mathbb{Z}/(3)$ which is defined by

$$\phi(\bar{a}) = (a \bmod 4, a \bmod 3).$$

The inverse of this isomorphism is

$$\phi^{-1}(\bar{c}, \bar{d}) = -3c + 4d \pmod{12}.$$

1.4 Fundamental Theorem of Finite Abelian Groups

The following theorem tells us that every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.

Theorem 1 *Suppose $n \geq 1$ and let*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

be the unique prime factorization of n. Then

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{e_1}) \times \mathbb{Z}/(p_2^{e_2}) \times \cdots \times \mathbb{Z}/(p_k^{e_k}).$$

Note, however, that we cannot decompose the direct product any further because in general, for $e > 1$,

$$\mathbb{Z}/(p^e) \ncong \underbrace{\mathbb{Z}/(p) \times \cdots \times \mathbb{Z}/(p)}_{e},$$

because $\mathbb{Z}/(p^e)$ is cyclic with order p^e while every element of the direct product has order p.

2 Rings

A *ring* is a non-empty set R with two binary operations $\cdot$ and $+$ where $(R, +)$ is an abelian group, $(R, \cdot)$ is a commutative *monoid* (a group without inverses). This is actually a commutative ring with unit element, but the name ring will suffice for the purposes of this course. Examples of rings include $\mathbb{Z}$, $\mathbb{Z}/(n)$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

2.1 Polynomial Rings

Given a ring R, let $R[X]$ be the set of all polynomials in X with coefficients from R. A typical element in this set has the form

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

where $a_n, a_{n-1}, \ldots, a_0 \in R$. Define operations $+$ and $\cdot$ on $R[X]$ in the usual way for polynomials. Then $R[x]$ forms a ring called a *polynomial ring.*

Example 2.1 Consider the polynomial ring $\mathbb{Q}[X]$. The polynomials $p(X) = 1/2X^2 + 5/7X - 2/3$ and $q(X) = 2X - 3$ are both elements of $\mathbb{Q}[X]$. The addition of $p(X)$ and $q(X)$ is

$$\begin{aligned} p(X) + q(X) &= (\frac{1}{2} + 0)X^2 + (\frac{5}{7} + 2)X + (-\frac{2}{3} - 3) \\ &= \frac{1}{2}X^2 + \frac{19}{7}X - \frac{11}{3}. \end{aligned}$$

The product $p(X)q(X)$ is

$$\begin{aligned} p(X)q(X) &= (X^3 + \frac{10}{7}X^2 - \frac{4}{3}X) + (-\frac{3}{2}X^2 - \frac{15}{7}X + 2) \\ &= X^3 - \frac{X^2}{14} - \frac{73X}{21} + 2. \end{aligned}$$

2.2 Quotient Rings

An *ideal* I in ring R is a non-empty subset of R such that I is a subgroup of $(R, +)$ and $RI \subseteq I$.

Example 2.2 Consider the ring $\mathbb{Q}[X]$. Let $I = \{g(X)p(X) : g(X) \in \mathbb{Q}[X]\}$ (where $p(X)$ is the same as in Example 2.1). Then I is an ideal of R. To see this, first consider the addition operation. Let $g_1(X), g_2(X) \in \mathbb{Q}[X]$, then

$$g_1(X)p(X) + g_2(X)p(X) = (g_1(X) + g_2(X))p(X),$$

since $g_1(X) + g_2(X) \in \mathbb{Q}[X]$. Hence, I is closed under addition. Finally, let $h(X) \in \mathbb{Q}[X]$. Then,

$$h(X)(g_1(X)p(X)) = (h(X)g_1(X))p(X),$$

since $h(X)g_1(X) \in \mathbb{Q}[X]$. This proves that $RI \subseteq I$. Hence, I is an ideal in $\mathbb{Q}[X]$.

Given an ideal I in a ring R, we can define the following equivalence relation. Let $a, b \in R$, then

$$a \equiv b \pmod{I}$$

if and only if $a - b \in I$. The set of equivalence classes induced is the *quotient ring* R/I. This is an equivalence relation that is compatible with multiplication. For example, if $a \equiv b \pmod{I}$ and $c \in R$, then $ca \equiv cb \pmod{I}$, since $a - b \in I$ implies $c(a-b) \in I$, which in turn implies $ca - cb \in I$.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, The MIT Press, Cambridge, Massachusetts, 1996.