Algebra: An Appendix to Stein's *Number Theory*

Peter Hawthorne

December 12, 2002

Contents

This appendix provides an overview of the abstract algebra that is assumed throughout this book. We first lay out the basic structures and definitions, such as groups and rings, then consider several fundamental examples in greater depth, and finally examine how algebra is used in each section of the book.

1 Basic Structures

1.1 Groups

We can think of algebra as abstracting its concepts from basic arithmetic and providing a generalization of the objects of elementary number theory. Numbers are abstracted to general sets, and addition and multiplication to binary operations in general. The simplest and most basic example of this abstraction is the group, which consists of a set with a single operation[1]. Examples of groups with which we are already familiar are $\mathbb{Z}$ under addition, or the nonzero elements of $\mathbb{Q}$ under mulitplication. The precise definition of a group adds certain axioms:

Definition 1.1 (Group). A group is a pair $(G, \circ)$ where G is a non-empty set and $\circ$ a binary operation on the set such that:
i) The operation is associative.
ii) The operation has an identity element.
iii) Every element of G has an inverse under $\circ$.

We see that $\mathbb{Q}$ under multiplication cannot be a group, because 0 has no inverse. Other examples of groups which are encountered in this book are $\frac{\mathbb{Z}}{n\mathbb{Z}}$ under addition, and $\mathrm{GL}_2(\mathbb{Z})$, the group of invertible 2×2 matrices, under mulitplication.

A group G is called *abelian* if its operation is commutative. That is, if $ab = ba$ for every $a, b \in G$.

A group G is a *cyclic* group if there is an element $x \in G$ such that for some $m \in \mathbb{Z}$, we have $x^m = 1$ and $G = \{1, x, \ldots, x^{m-1}\}$, with $x, \ldots, x^{m-1}$ distinct.

We say the *order* of a group G is the number of elements it contains. The *order* of an element x of G is the smallest m such that $x^m = 1$. It is possible in infinite groups that the order of an element will be infinity.

One basic fact about groups is the following proposition:

[1] this is sometimes known as a *rule of composition*

Proposition 1.2 (Cancellation Law). *Let a, b, c, be elements of a group G. If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.*

Proof. : Multiply both sides of $ab = ac$ by a^{-1} on the left:
$b = a^{-1}ab = a^{-1}ac = c$. □

One natural question is whether it is possible to extract any smaller groups from a given group G. Indeed it is. For example, the even integers under addition satisfy all of the group axioms and are a subset of (Z). Such a subset is known as a subgroup:

Definition 1.3 (Subgroup). Let H be a subset of G. Then H is a subgroup if:
i) For any $a, b \in H, ab \in H$.
ii) The identity of G is in H.
iii) For any $a \in H, a^{-1} \in H$.

Note that this is equivalent to the condition that if $H \subseteq G$, then H is a subgroup of G if and only if for all $h_1, h_2 \in H, h_1 h_2^{-1} \in H$.

To see the ubiquity of the group structure, note the following:

Fact 1.4. *Every set can be endowed with a group structure.*

The implication of this for number theory is that we have to be somewhat judgemental about group structures on sets we encounter. We will always be able to find something, but the goal, of course, is to find a natural structure which will give us some insight into what we are interested in.

1.2 Rings

Rings are another of the basic structure studied in algebra. Conceptually, they should be thought of as abstractions of the integers, in that they have two operations, which are modeled on addition and multiplication. A related structure is the field, which has the extra stipulation that all elements have mulitplicative inverses. For example, $\mathbb{Z}$ is a ring but not a field, while $\mathbb{Q}$ is both.

Definition 1.5. A ring is a triple $(R, +, \times)$ where R is a set, and $+$ and $\times$ are binary operations on the set such that:
i) R under $+$ is an abelian group. We denote the identity by 0.
ii) The operation $\times$ is associative and has an identity. We denote this by 1.
iii) $\forall\, a, b, c, \in R$, we have $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$.
For fields, add the axiom that $\forall\, r \in R \exists\, r^{-1} \in R$ such that $r^{-1}r = 1$ and $rr^{-1} = 1$ (i.e. the existence of multiplicative inverses).

Just as with groups, we can define *subrings* of R. A subring is a subgroup with the added stipulations that it is closed under multiplication and contains the element 1.

As a word of warning, when we use the word ring here, we are referring to *commutative rings*, in which the multiplicative law is commutative. There are non-commutative rings, but none are considered in the text, so we will not concern ourselves with them here.

1.3 Ideals

An ideal I is a subset of a ring R which is of special importance in number theory. There are many results in the text which are possible without ideals, but which are made much easier and clearer with them. The different proofs of quadratic reciprcity offer an example of this. Ideals arose in number theory as part of Dedekind's attempts to prove Fermat's Last Theorem. They were an attempt to idealize the numbers he was dealing with (quadratic fields) to ensure unique factorization.

Definition 1.6. An ideal I of a ring R is a subset of R such that:
i) I is a subgroup of the additive group of R.
ii) If $a \in I$ and $r \in R$, then $ra \in I$.

Ideals can also be defined as

The clearest way to think about ideals is as lattices. For example, imagine the ring $\mathbb{Z} \times \mathbb{Z}$ as embedded in $\mathbb{C}^2$ (which gives it a multiplicative structure). The ideal generated by the elements (2,0) and (0,2) is all points of the form $(2m, 2n)$ where $m, n \in \mathbb{Z}$.

1.4 Cosets and Quotients

Using a particular relation between a group G and a subgroup H, we can construct another group G/H. The group $\mathbb{Z}/n\mathbb{Z}$ is an example of such a group, as we shall see.

Definition 1.7 (Cosets). Given a group G, a subgroup H of G, and an element $g \in G$, we call the set $gH = \{gh : h \in H\}$ a *left coset of H in G*. We define Hg, the *right cosets*, similarly. Note that for G an abelian group, the right and left cosets will be the same.

The cosets of H in G form a disjoint partition of G. Furthermore, each coset has the same order. Letting each coset define an equivalence class, we are able to construct another group structure from G and H, the quotient group.

Definition 1.8 (Quotient Group). Let G be an abelian group, and H a subgroup of G. We define the *quotient group* of G by H as $\overline{G} = G/H = \{\overline{g_1}, \ldots, \overline{g_n}\}$, where $\overline{g_i}$ denotes $g_i H$. Put another way, G/H is the set of cosets of H in G. The group operation is coset multiplication: $(\overline{g_i}\overline{g_j} = \overline{g_i g j}$.

Note that it is not always stipulated that G be abelian, but if it is not, we must also require that H satisfy a particular property, namely that $gH = Hg$ for any g. If this property is satisfied, H is said to be a *normal* subgroup.

As an example, consider $G = \mathbb{Z}, H = 2\mathbb{Z}$. That is, $G = \{\ldots, -2, -1, 0, 1, 2, \ldots\}, H = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. The two cosets of H in G are $\overline{0} = 0H = H$ and $\overline{1} = 1H = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$ (recall that the group operation is addition). The group $\mathbb{Z}/2\mathbb{Z}$, then, is the group of order 2 {0,1}.

1.5 Group Actions

The examples of groups that we have seen so far have been very closely related to number theory. They are the sort of groups that number theorists use all the time, and form the grounding of the field. Here, we go on a brief digression, so as to make the following concept more intuitive, and look at groups of rotations.

Let r_θ be a rotation of the plane by θ radians. Consider the set $\{r_0, r_{2\pi/n}, r_{2(2\pi/n)}, \ldots, r_{(n-1)2\pi/n}\}$. Now, if we define an operation by composition of rotations: $r_\theta r_\phi = r_{\theta+\phi}$, we can form a group. Note that the group is a cyclic group of order n. Denote this group by R_n. Now, consider the set S of vertices of a regular n-gon with center at the origin. We can apply each element of R_n to S, sending an element $s \in S$ to another point on the n-gon. This is known as the *action* of R_n on S. It can be generalized so that given any set S and group G, we may define an action of G on S.

Definition 1.9 (Group Action). Given a group G and a set S, the *action* of G on S is a map $G \times S \longrightarrow S, (g, s) \mapsto gs$. The map must be such that, for all $s \in S$, and $g_1, g_2 \in G$:
i) For 1 the identity element of G, $1s = s$.
ii) $(g_1 g_2)s = g_1(g_2 s)$.

In the text, group actions play a central role in chapter 12 as the action of $\mathrm{SL}_2(\mathbb{Z})$ on the complex plane. The properties of this action are explored below in section 2.1 and 3.NUM. A deeper study of actions in algebra leads to actions of a group on itself, actions of a group on cosets, and many other interesting topics. These are certainly of relevance in higher number theory, but are beyond the scope of this text.

1.6 Free Groups and the Structure Theorem

discussion of free groups

There is an important result which follows from the study of free groups and modules, which are essentially vector spaces over a ring, rather than a field. Recalling the definition of a direct sum from linear algebra, we have the following statement of the theorem.

Theorem 1.10 (Structure Theorem for abelian groups). *If G is a finitely generated abelian group, then we have $G \simeq C_{d_1} \oplus \cdots C_{d_m} \oplus L$, where C_n is the cyclic group of order n and L is a free abelian group.*

The proof of this theorem is beyond the scope of this appendix. We will offer the following equivalent statement, however, which puts the theorem in more familiar terms:

Theorem 1.11. *If G is a finitely generated abelian group, then $G \simeq \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_m \times \mathbb{Z}^t$.*

1.7 Polynomial Fields

2 Fundamental examples

In this section, we examine a few of the most important examples of groups, rings, and fields which are encountered in the text, and explore a few of their interesting properties. It is hoped that this will help to give the reader a feel for the objects, which is one of the primary aims of both algebra and number theory.

2.1 The Group $\mathrm{SL}_2(\mathbb{Z})$

The first of the groups we will look at is quite useful in algebra, and very relevant to number theory. Now, although the following defintions apply to any ring R, we will restrict our attention to $\mathbb{Z}$ and $\mathbb{Z}/n$.

Let $\mathrm{GL}_2(R)$ denote the set of 2×2 matrices of R so that the determinant is invertible under multiplication in R. That this set forms a group under matrix multiplication is left as an exercise. We denote be $\mathrm{SL}_2(R)$ the set of invertible matrices with determinant 1. In the text, we are concerned mainly with $\mathrm{SL}_2(\mathbb{Z})$.

To give the reader a flavor for these groups, we present a few introductory results:

Theorem 2.1. *For any n, the map given by reduction of the matrix entries of an element of $SL_2(\mathbb{Z})$ gives a surjective group homomorphism $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z})$.*

Proof. proof here □

The following proposition characterizes the order of several linear groups. The proof is left to the reader.

Proposition 2.2. *i) The order of* $\mathrm{GL}_2(\mathbb{Z}/p)$ *is* $(p^2-1)(p^2-n)$.
ii) The order of $\mathrm{SL}_2(\mathbb{Z}/p)$ *is* $p(p^2-1)$.
iii) The order of $\mathrm{SL}_2(\mathbb{Z}/n)$ *is* $n^3 \prod_{p|n}(1-p^{-2})$.

The linear groups can be used to provide an action on $\mathbb{C}$, the complex plane.

2.2 Quadratic Fields

3 Algebra in This Book

3.1 Chapter 3

One of the most basic rings, $\mathbb{Z}/n$, is introduced in this chapter. It is noted that since $\mathbb{Z}/n$ is the quotient of the ring $\mathbb{Z}$ with an ideal $n\mathbb{Z}$, there is an induced ring structure on $\mathbb{Z}/n$. The proof that this holds in general is presented here:

Theorem 3.1. *PROOF from Artin.*

3.2 Chapter 4

3.3 Chapter 5

This aim of this chapter is to show that the group $(\mathbb{Z}/p)^\times$ is cyclic. Clearly, one must understand the basic notion of a cyclic group, which was presented in section 1 above. The proof relys on the following equivalent definition of the order of an element: $x \in G$ has *order* m if the subgroup generated by x has order m. If H is a subgroup of G, and $|H| = |G|$, then $H = G$. Now, since we know $(\mathbb{Z}/p)^\times$ has order $p-1$, we need only show that it contains an element of order $p-1$. The chapter proceeds with this goal.

3.4 Chapter 6

The last section of chapter 6 contains a proof of qudratic reciprocity which is very rich in algebraic content. First, we introduce the complex field. Recall that a field is a ring with multiplicative inverses.

3.4.1 n^{th} Roots of Unity

One group that arises in this section is the group of complex roots of unity, which are defined in Definition 6.4.1. We observe here that under complex mulitiplication, the n^{th} roots of unity form a group of order n, with identity $1 + 0i$. If n is prime, then the group is cyclic, generated by $e^{2\pi i/n}$.

3.4.2 Proposition 6.2.5 and Homomorphisms

This proposition relies on an aspect of algebra that we haven't used to this point - homomorphisms. Morphisms, of which homomorphisms are one type, are maps between one algebraic structure and another. There are morphisms from groups to groups, and rings to rings.

Definition 3.2. Let G and H be groups. A *group homomorphism* is a map $\varphi : G \longrightarrow H$ such that for any $a, b \in G, \varphi(ab) = \varphi(a)\varphi(b)$.

The general fact stated, that

3.5 Chapter 7

The dominant algebraic structure in this chapter is the *real quadratic field*, $\mathbb{Q}(\sqrt{d})$.

3.6 Chapter 8

3.7 Chapter 9

There are a few definitions we need to lay the groundwork:

Definition 3.3. An ideal I is called *principal* when it has only one generator.

Definition 3.4 (Principal Ideal Domain). A ring R is called a *principal ideal domain* when every ideal I of R is principal.

Definition 3.5. A nonzero ring R is called an *integral domain* when it has no zero divisors. That is, if $ab = 0$, either $a = 0$ or $b = 0$.

Definition 3.6. An integral domain R is a *Euclidean domain* when there exists a function $\delta : R \longrightarrow \{0, 1, 2, \ldots\}$ such that if $a, b \in R$, and $a \neq 0$, then $\exists q, r \in R$ so that $b = aq + r$, and either $r = 0$ or $\delta(r) < \delta(a)$. The function δ can be thought of as a norm on R. The condition that must hold is the division algorithm.

It is not the case that every ring encountered in this text is an integral domain:

Proposition 3.7. *The ring $\mathbb{Z}/n$ is an integral domain if and only if n is prime.*

Proof. need proof? □

We have the following result relating the foregoing definitions:

Theorem 3.8. *Every Euclidean domain is a principal ideal domain.*

Proof. Let R be a Euclidean domain, and let I be an ideal in R. If I is the zero ideal, then $I = 0R$, so consider $I \neq \{0\}$. Choose $b \in I \setminus \{0\}$ with $\delta(b)$ minimal. Now, since $b \in I$, it is clear that $bR \subseteq I$. Now take $a \in I$. Then we have $q, r \in R$ as in the definition of a Euclidean domain. So $r = a - bq$ so that $r \in I$. By the choice of b we cannot have $r \neq 0$ and $\delta(r) < \delta(b)$. So, $r = 0$ and $a = bq \in bR$. □

3.8 Chapter 10

3.9 Chapter 11

3.10 Chapter 12

3.11 Chapter 13