Algebra

Robert

June 2024

Abstract

This is a collection of notes for abstract algebra, but it could be interpreted as a textbook, as we include exercises. We will cover the theory of groups, rings, fields as well as modules.

The only prerequisite for this book is good mathematical maturity. It would help slightly if you have had linear algebra, as some of our examples depend on linear algebra.

Corrections and improvements are always appreciated. Please email me with any corrections.

Contents

Chapter 0

Preliminaries

We assume that the reader is already familiar with the basics of set theory and how to write proofs. More concretely, the reader should have a good grasp on functions and relations.

In this book, the naturals start from zero. That is, $\mathbb{N} = \{0, 1, 2, \dots\}$.

We first begin with an axiom. This will help us with proving the division algorithm (Theorem 0.0.2) and the fact that the GCD is a linear combination (Theorem 0.0.3).

Axiom 0.0.1 (Well-ordering for naturals)**.** Let $S \subseteq \mathbb{N}$ be a nonempty set of natural numbers. Then, S has a smallest element.

Theorem 0.0.2 (Division algorithm)**.** Let $n, m \in \mathbb{Z}$ and $m > 0$. Then, there exists unique $q, r \in \mathbb{Z}$, where $0 \leq r < m$ such that $n = qm + r$.

Proof. Let

$$S = \{ n - qm : q \in \mathbb{Z}, n - qm \geq 0 \}.$$

Then S is nonempty as $n \in S$, so it has a smallest element r. Clearly $r < m$, for if $r \geq m$ then it would not be the smallest. Then $n - r$ must divide m, so let q be an integer such that $qm = n - r$. For uniqueness, suppose q', r', where $0 \leq r' < m$ satisfies $n = q'm + r'$. Then, $qm + r = q'm + r'$, so $m(q - q') = r' - r$. Observe that $-m < r' - r < m$, so $q - q' = 0$, and thus $r = r'$ as well. □

In the proof above, q is called the *quotient* and r is called the *remainder*. If the remainder r is zero, then m is said to **divide** n, and we write $m \mid n$.

Theorem 0.0.3 (GCD is a linear combination)**.** Let $n, m \in \mathbb{Z}$ be nonzero integers. Then, there exists integers $s, t \in \mathbb{Z}$ such that $\gcd(n, m) = ns + mt$. Additionally, $\gcd(n, m)$ is the smallest positive integer of the form $ns + mt$.

Proof. Let

$$S = \{ na + mb : a, b \in \mathbb{Z}, na + mb > 0 \}.$$

Then S is nonempty, so it has a smallest element d, which is of the form $ns + mt$. We claim $d = \gcd(n, m)$. First, we show d divides both n and m. By Theorem 0.0.2, $n = qd + r$, where $0 \leq r < d$. If $r > 0$ then we have $r = n - qd = n - q(ns + mt) = n(1 - qs) - m(qt)$. So $r \in S$ but $r < d$, a contradiction. A similar argument holds for m, so d divides both n and m. Let d' divide both n and m too, we show d' divides d to establish that d is in fact the gcd. Let $n = d'h$, and $m = d'k$. Then $d = (d'h)s + (d'k)t = d'(hs + kt)$ as desired. □

We say that 2 numbers n, m are **coprime** if $\gcd(n, m) = 1$. One corollary of this theorem is so important it is singled out.

Corollary 0.0.4 (Bezout's lemma)**.** *If* $\gcd(n, m) = 1$*, then there exists integers* $s, t \in \mathbb{Z}$ *such that* $ns + mt = 1$*.*

These two theorems are rather important especially in the study of finite group theory. We will often invoke these without mention so make sure to keep them in mind.

Chapter 1

Groups

1.1 Groups

Before we give the definition of a group, the reader might appreciate some motivation behind what a group is trying to capture. The axioms of a group are in the sense, all that you need for the equation $ax = b$ to have a unique solution. Of course, the reader may also be motivated by other examples, such as the rotations and reflections of a square, or other sorts of symmetries.

Definition 1.1.1 (Group)**.** A group is a set G with a binary operation $\cdot : G \times G \to G$ such that

1. **(Associativity)** For all $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. **(Identity)** There exists $e \in G$ such that for all $g \in G$, $e \cdot g = g \cdot e = g$.
3. **(Inverses)** For all $g \in G$, there exists $h \in G$ such that $g \cdot h = h \cdot g = e$.

Note that the order of properties 2 and 3 do matter. We cannot write property 3 before property 2. A remark about how the identity and inverse is written is order.

To make notation clearer, we shall write gh for $g \cdot h$. We may sometimes use addition to denote the group operation as well, writing $g + h$. Additionally, because of associativity, we can drop any brackets. This means that there is no ambiguity about what xyz is. Recall that when adding numbers, $(2 + 3 + 4) + 5 = (2 + 3) + (4 + 5)$. Of course, it follows that you can drop the brackets for finitely many elements.

Exercise 1.1.2. Let G be a group. Prove that associativity holds for finitely many elements $x_1, \ldots, x_n \in G$. For example, $(xy)(zw) = x((yz)w)$.

Additionally, if we can commute elements under the group operation, the group is called Abelian.

Definition 1.1.3 (Abelian group)**.** Let G be a group. Then G is Abelian if for every $g, h \in G$, we have $gh = hg$.

We will immediately prove some properties about groups.

Theorem 1.1.4 (Basic properties of groups)**.** Let G be a group. Then, the following are true.

1. The identity of G is unique.
2. If $g \in G$ has an inverse h, then it is unique.

Proof. (1) Let $e, e' \in G$ and suppose both e, e' are identities. Keeping in mind that they satisfy the property of being an identity, we have,

$$e = ee' = e'e = e'.$$

(2) Suppose h, h' are both inverses of g. Again keeping in mind that h, h' both satisfy the properties of being an inverse for g.

$$h = h(h'g) = h(gh') = (hg)h' = h'.$$

□

Henceforth we shall talk about "the" identity of a group, and "the" inverse of an element. Additionally, if $g \in G$, then we shall denote the inverse of g by g^{-1}.

Let us now see some examples of groups.
Example 1.1.5. The integers form a group under usual addition. Clearly the identity is 0. Inverses are obvious. //
Example 1.1.6. The set of integers under usual multiplication is not a group. There is no multiplicative inverse for 2. //
Example 1.1.7. Let V be a vector space over $\mathbb{R}$. Then V is a group under vector addition. //
Example 1.1.8. Let $\mathbb{GL}_n(\mathbb{R})$ denote the set of $n \times n$ invertible matrices with real entries. Then this set is a group under the operation of matrix multiplication. //
Example 1.1.9. Let n be an integer. Let D_n be the set of symmetries of a regular n-sided polygon. **TODO: This example needs to be improved** //
Example 1.1.10. The real numbers form a group under usual addition. The real numbers without 0 form another group under usual multiplication. //

Note that the previous example illustrates an important point. *The same (similar) set can be a different group when the operation is replaced.* This tells us that to specify a group, we need both the set, as well as the group operation. However, if the operation does not matter, or it is clear from context, we shall simply say that G is a group.
Exercise 1.1.11. Verify that all of the above examples which are claimed to be groups are indeed groups.
Exercise 1.1.12. Groups can be finite or infinite in size. Identify which of the above groups are finite and which are not.
Exercise 1.1.13. Not every group is Abelian. Identify which of the groups above are abelian and which are not.

We state a few more properties of groups. While reading the proof, the reader should keep in the mind the proof strategies being deployed here.

Theorem 1.1.14. Let G be a group. Then, the following are true.

1. **(Generalized associativity)** For any $x_1, \ldots, x_n \in G$, the value of $x_1 \cdots x_n$ is independent of how it is bracketed.
2. If $g \in G$, then $\left(g^{-1}\right)^{-1} = g$.
3. **(Socks-shoes property)** If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.
4. **(Cancellation)** Let $g, h, h' \in G$. If $gh = gh'$ then $h = h'$. This is called left cancellation. Additionally, if $hg = h'g$, then $h = h'$. This is called right cancellation.

Proof. (1) is Exercise 1.1.2. If you could not do this, see [DF04, Prop 1, p. 19].

(2) Write

$$\left(g^{-1}\right)\left(g^{-1}\right)^{-1} = e = g^{-1}g.$$

Then the result follows by uniqueness of inverses.

(3)
$$(gh)^{-1}(gh) = e = h^{-1}h = h^{-1}(g^{-1}g)h = (h^{-1}g^{-1})(gh).$$

(4) Exercise for reader. □

To ensure that the reader is adequately familiar with the techniques of the proof above, we include the following simple exercises.
Exercise 1.1.15. Prove part (4) of Theorem 1.1.14.
Exercise 1.1.16. Prove Theorem 1.1.14 again using Theorem 1.1.14 part (4).

The next example is an important infinite family of finite groups.
Example 1.1.17. Let $\mathbb{Z}_n = \{0, \ldots, n-1\}$ be equipped with the operation of addition modulo n. That is, we define $+$ on $\mathbb{Z}_n$ to be given by $a + b = (a + b) \mod n$. This is called the *group of integers modulo* n, or alternatively *the cyclic group of order* n. We will soon see what this means. //
Exercise 1.1.18. Verify that $\mathbb{Z}_n$ with the operation as defined above is indeed a group.
Example 1.1.19. Let $U(n)$ denote the set of all nonnegative integers $k \leq n$ such that $\gcd(k, n) = 1$. Then $U(n)$ is a group under the operation of multiplication modulo n. That is, if $a, b \in U(n)$, $ab = a \cdot b \mod n$. //

The next example is also rather important.
Example 1.1.20 (Symmetric groups)**.** Let $S = \{1, \ldots, n\}$. Then consider the set of all permutations of S (bijective functions from S to S). We shall call this set S_n, which stands for *symmetric group on* n *things*. This set is a group under function composition. //
Exercise 1.1.21. Prove that S_n is a group under function composition.

We now introduce some notation. Let G be a group and $g \in G$. We shall write
$$g^n = \underbrace{gg \cdots g}_{n \text{ times}}$$
to mean g multiplied by itself n times.

1.1.1 Problems

Problem 1.1.1. Let G be a group. Prove that if for every $g \in G$, we have $g^2 = e$, then G is Abelian.

1.2 Subgroups

We can essentially understand a subgroup as a smaller group that's contained within a group.

Definition 1.2.1 (Subgroup). Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G if the following properties hold.

1. The identity of G is in H.
2. For all $x, y \in H$, $xy \in H$.
3. For all $x \in H$, $x^{-1} \in H$.

This tells us that if we restrict the operation of G to H, then H is still a group. If H is a *proper* subgroup of G, it means that H is a proper subset of G.

Theorem 1.2.2 (Subgroup tests). Let G be a group and $H \subseteq G$. Then, the following are equivalent.

1. H is a subgroup of G.
2. H is nonempty, and for all $x, y \in H$, we have $xy^{-1} \in H$.

Proof. We will not insult the reader's intelligence by providing a proof. □

Exercise 1.2.3. Prove Theorem 1.2.2.

1.2.1 Problems

Problem 1.2.1. Prove that no group is the union of 2 proper subgroups. (No cheating and looking this up)

1.3 Cyclic groups

Definition 1.3.1 (Cyclic group). Let x be anything.

Chapter 2

Rings

TBD

Chapter 3

Field Extensions and Splitting Fields

3.1 Extension fields

Given a polynomial, is it possible to find a field in which that polynomial has a root? For example, consider the polynomial $x^2 + 1$.

Definition 3.1.1. Let F be a field. If $E \supseteq F$ is a field and the operations of E restricted to F are the same as the operations of F, then E is an **extension field** of F.

If E is an extension field of F, we can say that E is an extension of F, or E extends F. Note the abuse of notation here again: F may not actually be a subset of E, but if it is isomorphic to a subfield of E it is good enough.

Example 3.1.2. $\mathbb{C}$ is clearly an extension field of $\mathbb{R}$. Additionally, $\mathbb{R}$ is an extension field of $\mathbb{Q}$. //

Example 3.1.3. Let F be a field and let $p \in F[x]$ be irreducible over F. Then, $F[x]/\langle p \rangle$ is an extension field of F. Notice that we can embed F as a subfield of $F/\langle p \rangle$ by the map

$$x \mapsto x + \langle p \rangle.$$

It is not too hard to see that this map is an isomorphism onto its image. We will use this example to motivate the following theorem. //

Theorem 3.1.4 (Existence of Extension Fields)**.** Let F be a field and let $f \in F[x]$ be a nonconstant polynomial. Then there exists an extension field E of F such that f has a root in E.

Proof. Let $p(x)$ be an irreducible factor of f. This exists as $F[x]$ is a UFD. It suffices to produce an extension field of F where p has a root in. Let $E = F[x]/\langle p \rangle$. Then F embeds into E. Now, we see that $x + \langle p \rangle$ is a root of p in E. Write $p(x) = \sum_{i=0}^{n} a_i x^i$, then

$$p(x + \langle p \rangle) = \sum_{i=0}^{n} a_i (x + \langle p \rangle)^i = \left(\sum_{i=0}^{n} a_i x^i \right) + \langle p \rangle = \langle p \rangle.$$

□

Note that if D is an integral domain and $p \in D[x]$, then there is an extension field of $Q(D)$ that contains a root of p. This means that there is an extension field that contains D. This need not be true if D is not an integral domain.

Example 3.1.5. Let $f(x) = 2x + 1$ in $\mathbb{Z}_4[x]$. Then given any ring $R \supseteq \mathbb{Z}_4$, f has no roots in R. //

3.2 Splitting Fields

Definition 3.2.1. Let F be a field, and let E be an extension of F. Then we *define* $F(a_1, \ldots, a_n)$ to be the *smallest* subfield of E that contains F and $\{a_1, \ldots, a_n\}$.

It immediately follows that $F(a_1, \ldots, a_n)$ is the intersection of all subfields of E that contain F and $\{a_1, \ldots, a_n\}$. We warn the reader that it is important that we have an extension field to talk about. For example, it is nonsensical to write something like $\mathbb{Q}(\text{apple})$ when we don't have any field that contains apple in it.

Definition 3.2.2 (Polynomial splitting)**.** Let F be a field and let E be an extension of F. Let $f \in F[x]$. Then f **splits** in E if it can be factorized into linear factors, i.e. we have $a \in F$, $a_i \in E$ such that

$$f(x) = a(x - a_1) \cdots (x - a_n).$$

We say that E is a **splitting field for** f if $E = F(a_1, \ldots, a_n)$.

In other words, E is a splitting field for f it is the smallest field that contains F and all roots of f. We remark that whether a polynomial splits depends on which field the polynomial comes from.

Example 3.2.3. Let $f(x) = x^2 + 1$ in $\mathbb{Q}[x]$. Then $\mathbb{C}$ is *not* a splitting field of f over $\mathbb{Q}$, since we can find a smaller field that still contains roots of f, namely, $\mathbb{Q}[x]/\langle f \rangle$. //

It would be pretty stupid if splitting fields did not exist. Luckily they do.

Theorem 3.2.4 (Splitting fields exist)**.** Let F be a field and $f \in F[x]$ be nonconstant. Then there is a splitting field of f over F.

The proof of the theorem is simple: induction on $\deg f$ and use Theorem 3.1.4.

Proof. We go by induction[1] on $\deg f$. If $\deg f = 1$ it is trivial: $f(x) = (x - a)$ for some $a \in F$. Now suppose the theorem is true for all polynomials of degree less than $\deg f$ and all fields. By Theorem 3.1.4, there is an extension field $E \supseteq F$ such that f has a root in E. Let this root be a_1. Then we factorize f over E, so write $f(x) = (x - a_1)g(x)$, where $g(x) \in E[x]$. Thus there is a splitting field $K \supseteq E$ of g over E. K has all roots of g, say they are $a_2, \ldots, a_n$. Since $E \supseteq F$, K contains a_1, F and $a_2, \ldots, a_n$. So we can take the splitting field to be $F(a_1, \ldots, a_n)$. □

Now we can finally give some examples of splitting fields.

Example 3.2.5. Let $f(x) = x^2 + 1$, but this time considered as an element of $\mathbb{R}[x]$. Then $\mathbb{C}$ is a splitting field of f over $\mathbb{R}$. Notice that $\mathbb{R}[x]/\langle f \rangle$ also is a splitting field of f. Are these the same splitting field? We will answer this soon. //

[1] Note that strong induction is used here, since $\deg g$ may not necessarily be $\deg f - 1$. If I am wrong, please correct me.

Bibliography

[DF04] David Steven Dummit and Richard M. Foote. *Abstract algebra*. 3rd ed. Hoboken, NJ: Wiley, 2004. ISBN: 9780471433347.

[Gal20] Joseph A. Gallian. *Contemporary abstract algebra*. Tenth edition. Boca Raton: Chapman & Hall/CRC, 2020. ISBN: 9781003142331.