MATH 1530: Abstract Algebra

Spring 2017

Notes for Abstract Algebra: Part II

Nicholas Tomlin

Contents

1 Applications of group theory

In the past, mathematicians studied extrinsic properties of groups rather than intrinsic properties. As we'll see in the following theorem, every finite group can be "embedded" as an isomorphism to some subgroup of the symmetric group S_n. Today, we focus less on the properties of S_n and more on the properties of groups at a general level.

Theorem 1.0.1: Cayley's Theorem
Every finite group G is isomorphic to a subgroup of S_n for some $n \in \mathbb{Z}$. In fact, we may take $n = |G|$.

Proof. Consider the action of left multiplication of the group G on the set G. I.e., $g \cdot x = gx$, which is a product in G. Thus we have the permutation representation $\varphi : G \to S_G \cong S_n$. As an exercise: check that φ is injective. □

Definition 1.0.2: *A **representation** of a group G is a homomorphism $\varphi : G \to \mathrm{GL}(V)$, which is an invertible linear transformation of a vector space V.*

2 Introduction to rings

We're all familiar with some examples of rings. For example, the real numbers, the complex numbers, etc. all have addition and multiplication which are compatible via the distributive law. Now, we'll formally define it:

Definition 2.0.1: *A **ring** is a set R together with binary operations $+$ and $\times$ such that the following ring axioms hold:*
(1) $(R, +)$ is an abelian group.
(2) $\times$ is associative.
(3) $\times$ distributes over $+$, i.e., for all $a, b, c \in R$, then we write $(a+b)\times c = a\times c+b\times c$ and also $c \times (a + b) = c \times a + c \times b$.
(4) We say R has a (multiplicative) identity if there exists $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.
*Further, we say R is **commutative** if $\times$ is commutative.*

Theorem 2.0.2
Let R be a ring. Then $a \times 0 = 0 \times a = a$ for all $a \in R$.

Proof. We can write the following derivation:

$$\begin{aligned} a \times 0 &= a \times (0 + 0) \\ &= a \times 0 + a \times 0 \\ 0 &= a \times 0 \end{aligned}$$

where the last step follows from subtracting $a \times 0$ from both sides of the equation. □

Theorem 2.0.3
Let R be a ring. Then $(-a) \times b = a \times (-b) = -ab$ for all $a, b \in R$.

Theorem 2.0.4
Let R be a ring. The multiplicative identity $1 \in R$ is unique if it exists. Further, $(-1) \times a = -a$.

Proof. If $1 \in R$ and $1' \in R$ are multiplicative identities, then $1 = 1 \times 1' = 1'$ as desired. Then, note that $0 = 0 \times a = (1 + (-1)) \times a = 1 \times a + (-1) \times a = a + (-1) \times a$, so therefore $(-1) \times a = -a$ is the additive inverse. □

2.1 Examples of rings

Many of the groups we have discussed previously can also be considered rings with the usual definition of addition and multiplication: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, and $\mathbb{Z}/n\mathbb{Z}$ are all examples of this. The group $2\mathbb{Z}$ may also be considered a ring; however, it's notable that $2\mathbb{Z}$ has no multiplicative inverse. (This does not violate the ring axioms.)

Definition 2.1.1: *Given a ring R, a **subring** is a subset $S \subseteq R$ such that $+$ and $\times$ are closed with respect to S and $(S, +, \times)$ is also a ring.*

Example 1: Given a ring R, let $\text{Mat}_{n \times n}(R)$ be the ring of $n \times n$ matrices with entries in R. This is a good example of a (typically) noncommutative ring.

2.1.1 Polynomial rings

Definition 2.1.2: *Given any ring R, define $R[x]$ to be the **polynomial ring** with coefficients in R. Formally:*

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 : a_i \in R_i, n \geq 0\}$$

*where we call a_n the **leading coefficient** and n is the **degree**.*

Addition on the polynomial ring is defined component-wise as follows:

$$(a_0 + a_1x + \cdots) + (b_0 + b_1x + \cdots) = (a_0 + b_0) + (a_1 + b_1)x + \cdots$$

Meanwhile, multiplication is defined via distribution. So each term of one polynomial is multiplied by each term of the other, and then all terms are summed:

$$(a_0 + a_1x + \cdots) \times (b_0 + b_1x + \cdots) = (a_0b_0) + (a_0b_1 + a_1b_0)x + \cdots$$

We can extend this to multivariable polynomial rings via induction. Indeed, we'll write $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ to define polynomial rings with an arbitrary number of variables.

2.1.2 Trivial rings

Given any abelian group $(R, +)$, define $\times$ on R by $a \times b = 0$ for all $a, b \in R$. If $(R, +) = \{0\}$, then we have the zero ring. This is the unique ring with an identity $1 = 0$. This is also the only ring which is a group under multiplication. (Some other rings can be made into multiplicative groups by deleting the additive identity, e.g., $\mathbb{R}$.)

2.1.3 Group rings

Definition 2.1.3: *Let G be a group[a] and R be a ring. The* ***group ring***

$$RG = \{r_1g_1 + \cdots r_kg_k : r_i \in R, g_i \in G\}$$

uses the definition of a "formal sum," which will be explained briefly.

[a] Dummit and Foote requires that $|G|$ be finite, but this is not strictly necessary.

As before, addition behaves component-wise:

$$(r_1g_1 + \cdots + r_kg_k) + (r_1'g_1 + \cdots + r_k'g_k) = (r_1 + r_1')g_1 + \cdots + (r_k + r_k')g_k$$

Multiplication may be defined by setting $(rg) \cdot (r'g') = (rr')(gg')$ and extending this definition via addition.

Definition 2.1.4: *A* ***formal sum*** *of elements of G with coefficients in R is a map of sets $f : G \to R$ such that $f(g) = 0$ for all but finitely many $g \in G$.*

Example 2: The formal sum of elements in $\mathbb{N} = \{0, 1, 2, \ldots\}$ with $\mathbb{R}$ coefficients are naturally in bijection with $\mathbb{R}[x]$, which is the set of polynomials with real-valued coefficients.

Given a ring R, we might also consider the Laurent polynomial ring $R[x^{\pm}] = \{a_mx^m + \cdots + a_nx^n : m \leq n\}$ where $m, n \in \mathbb{Z}$. For example, the element $x^{-2} + 3x^{-1} + 5x^7 \in \mathbb{R}[x^{\pm}]$ is a member of the Laurent polynomial ring with real coefficients. Then $\mathbb{R}[x^{\pm}] \cong \mathbb{R}\mathbb{Z}$, which is the group ring. For example, $(x^{-2}) \cdot (x^3 + x^5) = x + x^3$.

2.2 The structure of rings

But what does it mean to say that $\mathbb{R}[x^{\pm}]$ is isomorphic to $\mathbb{R}\mathbb{Z}$? Even though we have defined isomorphism between groups, we need to re-define the concept of isomorphism for rings. We can do so with the following definition:

Definition 2.2.1: *An **isomorphism** $\varphi : R \to S$ **of rings** is a bijection φ such that:*

$$\varphi(r + r') = \varphi(r) + \varphi(r')$$
$$\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$$

for all elements $r, r' \in R$.

Definition 2.2.2: *A nonzero element $a \in R$ is a **zero divisor** if $ab = 0$ or $ba = 0$ for some $b \neq 0$.*

Definition 2.2.3: *An element $a \in R$ is a **unit** if there exists $c \in R$ with $ac = ca = 1$ (in a ring where the multiplicative identity exists).*

Example 3: Consider the following groups:

- $\mathbb{Z}$ has no zero divisors and units $\{\pm 1\}$.
- $\mathbb{Z}/n\mathbb{Z}$ has units $\{\bar{m} : (m, n) = 1\}$ and the zero divisors are non-zero non-units.

Observe that an element $a \in R$ cannot be both a unit and a zero divisor. If a is a unit and $ab = 0$, then we can show that $b = 0$. Indeed, let $c \in R$ with $ca = 1$. Then $b = (ca)b = c(ab) = 0$ as desired. Hence a is not also a zero divisor.

2.3 Other structures

Definition 2.3.1: *A commutative ring with identity $1 \neq 0$ and no zero divisors is called an **integral domain**.*

Definition 2.3.2: *A **field** is a commutative ring with identity $1 \neq 0$ such that every nonzero element is a unit.*

Examples of fields include $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.