Course Notes

Introduction to Abstract Algebra

Alex Rutar

BSM Fall 2018

Contents

Chapter 1

Introduction

1.1 Principles

In general, algebraic structures require three properties:

- A set
- Operations on the set
- Properties of these operations

We develop theories and want to look at examples to demonstrate these properties. This course will focus on propeties of rings and groups.

1.1.1 Rings

A ring consists of a set along with two binary operations which satisfy $(R, +, \cdot)$. Then for all $a, b, c \in R$,

1. $(a + b) + c = a + (b + c)$
2. $a + b = b + a$
3. $\exists 0 \in R$ so that $a + 0 = a$
4. $\forall a \in R$, there exists $b \in R$ so that $a + b = 0$
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
6. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$

There are some common examples:

1. Rings of numbers
   (a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
   (b) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$
   (c) $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\}$
2. Rings of polynomials

$$\mathbb{Z}[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 | \forall a_i \in \mathbb{Z}\}$$

   $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}[x, y]$ etc.

3. Rings of functions, such that $C[a,b]$

4. Rings of matrices $M_n(\mathbb{Z})$: all $n \times n$ square matrices with integer entries (more generally matrices with any entries in a ring).

5. Given any set X, consider $\mathcal{P}(X)$ and define the symmetric difference

$$A \oplus B = (A \cup B) \setminus (A \cap B)$$

Then $(\mathcal{P}(X), \oplus, \cap$ is a ring. Interestingly, $A = -A$ in this ring.

A ring with identity means we have some $1 \neq 0$ so that $a \cdot 1 = 1 \cdot a = a$. A division ring is a ring with identity such that all nonzero elements have a multiplicative inverse. A field is a commutative division ring $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[\sqrt{2}]$.

1.1.2 Groups

Def'n. 1.1.1 *A group is a set G together with an operation $*$ which satisfies*

1. $(a * b) * c = a * (b * c)$
2. $\exists e \in G : a * e = a = e * a$
3. $\forall a \in G \exists b \in G : a * b = e = b * a$

Here are some common examples of groups

1. Additive groups:
   (a) If $(R, +, \cdot)$ is a ring, then $(R, +)$ is a (commutative) group.
   (b) If V is a vector space, then $(V, +)$ is a group

2. Multiplicative groups:
   (a) R is a ring with identity, and write

$$R^\times = \{a \in R \mid \exists b \text{ s.t. } a \cdot b = 1 = b \cdot a\}$$

   in other words the elements having a multiplicative inverse. These are called the **units** of the ring, and $R^\times$ is called the **unit group** or the **multiplicative group** of R.
   (b) $\mathbb{Z}^\times = \{1, -1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ (similarly for $\mathbb{R}, \mathbb{C}$).
   (c) $M_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$.
   (d) $M_n(\mathbb{Z})^\times = \mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) | \det A = \pm 1\}$.

3. Matrix groups: matrices under addition and multiplication

4. Composition of permutations. Let T be any set, and $A : T \to T$ be bijective. Let S_T be the collection of all permutations on T. Then $(S_T, \circ)$ (composition action) forms a group.

   We write $S_n = S_{\{1,2,\dots,n\}}$, the group of permutations on n elements. We can notate the elements of S_n by writing

   $$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

   Clearly $|S_n| = n!$.