# Course Notes

## Introduction to Abstract Algebra

*Alex Rutar*

BSM Fall 2018

# Contents

**1 Fundamentals of Groups** **3**
1.1 Principles . . . 3
1.1.1 Rings . . . 3
1.1.2 Groups . . . 4
1.1.3 The group $\mathbb{Z}_m$ . . . 5
1.2 Basics of Groups . . . 5
1.2.1 Functions between Groups . . . 5
1.3 Examples of Finite Groups . . . 6
1.3.1 Group Definitions . . . 6
1.3.2 Cyclic Groups . . . 6
1.3.3 Permutation Groups . . . 7
1.3.4 Dihedral Groups . . . 8
1.4 Subgroups . . . 8

# Chapter 1

# Fundamentals of Groups

## 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 $S_n = S_{\{1,2,\ldots,n\}}$, 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 $|S_n| = n!$.

### 1.1.3 The group $\mathbb{Z}_m$

**Def'n. 1.1.2** *Let $\sim$ be an equivalence relation. We then define the **quotient group** $G/\sim$ given by the equivalence classes of elements in $G$.*

To construct $\mathbb{Z}_m$, we define $\mathbb{Z}_m = \mathbb{Z}/\sim$ where $a \sim b$ if $a \cong b \pmod{m}$. Since we have a division algorithm in $\mathbb{Z}$, for any $d \in \mathbb{Z}$, we can write $d = tm + r$ with $0 \leq r \leq m-1$. Thus $\overline{d} = \overline{r}$, so we can represent $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. As a result we usually do not bother writing $\bar{\cdot}$.

**Prop. 1.1.3** *We have $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$.*

Proof Obvious. □

**Thm. 1.1.4** $\mathbb{Z}_m^\times = \{\overline{a} \mid \gcd(a, m) = 1\}$.

Proof Assume $\overline{a} \in \mathbb{Z}_m^\times$ so there exists $\overline{x}$ with $\overline{x} \cdot \overline{a} = 1$. Then $\overline{xa} = \overline{1}$ so $xa \cong 1 \pmod{m}$ so $m | xa - 1$. Let $d = \gcd(a, m)$ so $d|a$ and $d|m$. Thus $d|xa - 1$ and $d|xa$ so $d|1$ and $\gcd(a, m) = 1$.

Conversely, suppose $\gcd(a, m) = 1$. Then by Bézout's Lemma, get $x, y$ so that $xa + ym = 1$, so $xa \cong 1 \pmod{1}$ and $\overline{xa} = \overline{1}$ and $\overline{xa} = \overline{1}$ and we have our multiplicative inverse. □

We thus have $|\mathbb{Z}_m^\times| = \phi(m)$.

## 1.2 Basics of Groups

### 1.2.1 Functions between Groups

**Def'n. 1.2.1** *Let $(G, \blacklozenge)$, $(H, \star)$ be groups. A mapping $f : G \to H$ is called an **homomorphism** if*

$$f(u \blacklozenge v) = f(u) \star f(v)$$

*If $f$ is also a a bijection, then we call $f$ an **isomorphism**.*

**Prop. 1.2.2** *$G$ and $H$ are isomorphic if and only if their Cayley Tables are the same up to permutation of elements.*

Proof Obvious. □

# 1.3 Examples of Finite Groups

## 1.3.1 Group Definitions

**Def'n. 1.3.1** *We say that $(G,*)$ with $*: G\times G\to G$ is a **group** if for all $a,b,c\in G$*

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

We have our first basic proposition:

**Prop. 1.3.2** *The identity and inverses are unique.*

Proof If $e,f$ are both identities, then $e = e*f = f$. If $u,v$ are both inverses of $x$, then $u*(x*v) = u*e = u$ and $(u*x)*v = e*v = v$ so $u = v$. □

**Def'n. 1.3.3** *If $ab = ba$ for all $a,b\in G$ then we say that $G$ is **commutative**.*

**Def'n. 1.3.4** *Let $G$ be a group with $G = \{g_1, g_2, \dots, g_n\}$. Then the **Cayley Table** for $G$ is the matrix $M\in M_n(G)$ where $M_{ij} = g_ig_j$.*

**Prop. 1.3.5** *In each column or row, each element occurs exactly once. Furthermore, if $M_{ij} = e$, then $M_{ji} = e$.*

Proof This follows directly by left or right cancellation, and by commutativity of the elements with their inverse. □

## 1.3.2 Cyclic Groups

**Def'n. 1.3.6** *The **order of an element** $g\in G$ is $o(g) := \left|\{g^d | d\in\mathbb{Z}\}\right|$. The **order of a group** $G$ is $|G|$.*

We certainly have $o(g)\le |G|$ for any $g\in G$. Equality holds when $o(g) = \infty$ and $G$ is countable, or $G = \{g^d : d\in\mathbb{Z}\}$.

**Def'n. 1.3.7** *A collection $H = \{g_1, g_2, \dots, g_k\}$ **generates** $G$ if we can write any $g\in G$ as a product of elements in $H$.*

**Def'n. 1.3.8** *We say that $G$ is **cyclic** if $G = \{g^d : d\in\mathbb{Z}\}$ for some $g\in G$. Equivalently, it is generated by a set of cardinality one.*

**Ex. 1.3.9** Note that $\mathbb{Z}_{13}^\times$ is cyclic with generator 2.

**Lemma 1.3.10** *If $o(g)$ is finite and $d\in\mathbb{Z}$, then*

$$o(g^d) = \frac{o(g)}{\gcd(o(g),d)}$$

Proof Let $o(g) = K$ and $t = \gcd(K,d)$ and write $K = tK_1$ and $d = td_1$ with $K_1, d_1$ coprime. Thus $o(g^d)$ is the smallest positive integer $l$ with $(g^d)^l = 1$. But then $(g^d)^l = 1 \Leftrightarrow g^{dl} = 1 \Leftrightarrow o(g)|dl$ and $k|dl$, that is $tK_1|td_1l$ and $k_1|d_1l$. Thus $K_1|l$ so the smallest positive intger $l$ is $K_1$ and $o(g^d) = K_1 = \frac{o(g)}{\gcd(o(g),d)}$ as desired. □

### 1.3.3 Permutation Groups

Recall that $S_n$ is the symmetric group of degree $n$, consisting of all permutations of $[n]$. Thus $|S_n| = n!$. Instead of using the matrix form, we can write the permutation group using the cycle form.

**Ex. 1.3.11** Write

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 3 & 1 & 2 & 9 & 8 & 5 & 6 \end{pmatrix} = (14)(2785)(3)(69)$$

We can also write $(14)(2785)(69)$, in other words excluding elements which map to themselves.

In general, a cycle $(a_1 a_2 \dots a_k)$ indicates that $a_1 f = a_2$, $a_2 f = a_3, \dots, a_k f = a_1$. In $S_n$, each permutation can be expressed in a cycle form (using disjoint cycles). The cycle form is unique up to ordering within the cycles, and ordering among the cycles.

**Ex. 1.3.12** In $S_5$, the possible cycle structures are

$$I, (ab), (abc), (abcd), (abcde), (ab)(cd), (ab)(cde)$$

We then have

$$\begin{aligned} o(I) &= 1 \\ o((ab)) &= 2 \\ o((abc)) &= 3 \\ o((abcd)) &= 4 \\ o((abcde)) &= 5 \\ o((ab)(cd)) &= 2 \\ o((ab)(cde)) &= 6 \end{aligned}$$

For $f = (abc)$, $f^2 = (abc)(abc) = (acb)$, $f^3 = (abc)(acb) = abc$. For $f = (abcd)$, $f^2 = (ac)(bd)$, $f^3 = (abdc)(ac)(bd)(adcb)$, and $f^4 = (abcd)(adcb) = (abcd)$.

If $f = (a_1 a_2 \dots a_k)$, $o(f) = k$.

**Prop. 1.3.13** *Suppose $f = \gamma_1 \gamma_2 \dots \gamma_i$ for disjoint cycles. Then $o(f) = lcm(o(\gamma_1), o(\gamma_2), \dots, o(\gamma_i))$.*

Proof Note that the $\gamma_i$ commute, so that

$$\begin{aligned} f^d = I &\Leftrightarrow (\gamma_1 \gamma_2 \dots \gamma_i)^d = I \\ &\Leftrightarrow \gamma_1^d \gamma_2^d \dots \gamma_i^d = I \\ &\Leftrightarrow \gamma_i^d = I \quad \forall i \end{aligned}$$

The last line holds since the $\gamma_i^d$ operates on disjoint sets. Thus we have our formula, as desired. □

### 1.3.4 Dihedral Groups

Fix a regular polygon with $n$ vertices. Let $D_n$ be the collection of rigid motions with map the regular $n-$polygon to itself. Since $r^n = 1$ and $s^2 = 1$, we have

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

Thus $|D_n| = 2n$. We can compute the oprations on $D_n$:

$$\begin{aligned} r^a \cdot r^b &= r^{a+b} \\ sr^a \cdot r^b &= sr^{a+b} \\ r^a \cdot sr^b &= sr^{b-a} \\ sr^a \cdot sr^b &= r^{b-a} \end{aligned}$$

Thus $o(sr^a) = 2$ and $o(r^a)$ is given by the usual formula.

## 1.4 Subgroups

**Def'n. 1.4.1** *A subset $H$ of a group $G$ is called a **subgroup** if $H$ is also a group with the same operation. We write $H \leq G$.*

For example, $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.