Abstract Algebra Notes

Contents

1. Groups

1.1. Group Basics

Definition (group): A *group* is a set G with an operation $\times : G \times G \to G$ which satisfies the following properties:

a) There exists an element $e \in G$ such that $a \times e = e \times a = a$ for all $a \in G$ (if the operation is represented multiplicatively, then often we write it as 1_G, or just 1).
b) For every $a \in G$, there exists $a^{-1} \in G$ such that $a \times a^{-1} = a^{-1} \times a = e$.
c) The operation is associative, i.e. for every $a, b, c \in G$, we have $a \times (b \times c) = (a \times b) \times c$.

From here on out, the operation $\times$ will take a number of forms, such as $+$ or $\cdot$, or it won't make an appearance at all and implicit multiplication (such as ab) will represent the operation.

Example *(standard examples/nonexamples)*:
- Consider $(\mathbb{Z}, +)$. The identity is 0, and the inverse of n is $-n$.
- Consider $(\mathbb{Z}^\times, \cdot)$, where $\mathbb{Z}^\times = \mathbb{Z}\backslash\{0\}$. The identity is 1, but not every element has an inverse. For example, $2 \cdot n \neq 1$ for any integer n.
- Consider $(\mathbb{C}^\times, \cdot)$. The identity is 1, and the inverse of z is z^{-1}.
- Consider $(\mathrm{SL}_n(\mathbb{C}), \times)$, where $\mathrm{SL}_n(\mathbb{C})$ is the set of $n \times n$ matrices with elements in $\mathbb{C}$ that have determinant 1. The identity is I_n, and since every element has nonzero determinant, an inverse exists and is given by the inverse matrix.
- Consider $\{1, 2, \ldots, n\}$ and the set of functions T on it that are bijective. Then S_n denotes the group of all of these functions, and is called the *symmetric group*. The identity permuation is just $f(x) = x$, and the inverse of an element is given by the inverse function.
- The integers mod n form a group under addition, and is what's known as *cyclic*, since a single element (say 1) generates the entire group by repeatedely applying the operation to the element. A group with size n where a single element generates it is often called a *cyclic group*, and is denoted C_n.
- The group G with one element 1 is called the *trivial group*.

Definition (abelian): Suppose $(G, \cdot)$ is a group. If for every $a, b \in G$ we have $ab = ba$, then the group is called *abelian*.

Taking $\mathrm{SO}(n)$ as an example, we see that not every group is abelian.

Proposition (identity and inverse are unique): Let $(G, \cdot)$ be a group. Then the identity is unique. Furthermore, every element has a unique inverse.

Proof: Suppose e_1, e_2 are identities. Then $e_2 = e_1 e_2 = e_1$. Now suppose x, y are inverse of a. Then $x = xe = x(ay) = (xa)y = ey = y$. ∎

Definition (left/right inverse): Suppose $(G, \cdot)$ is a group. An element a has a *left inverse* if there exists $\ell \in G$ such that $\ell a = e$. An element a has a *right inverse* if there exists $r \in G$ such that $ar = e$.

Proposition (left and right inverse imply invertible): Suppose $(G, \cdot)$ is a group, and $a \in G$ has left inverse ℓ and right inverse r. Then $\ell = r$ and a is invertible with inverse ℓ.

Proof: We have

$$\ell = \ell(ar) = (\ell a)r = r.$$

Then we have

$$\ell a = e = ar = a\ell.$$

■

Proposition (cancellation law): Suppose $(G, \cdot)$ is a group. If $a, b, c \in G$ such that $ab = ac$ or $ba = ca$.

Proof: Multiply the first equation by a^{-1} on the left, and second equation by a^{-1} on the right.■

Definition (subgroup): Suppose $(G, \star)$ is a group. Then a subset H of G is a *subgroup of* G, denote $H \leq G$, if when inheriting the operation $\star$, H is a group. If $H \neq G$, then H is a *proper subgroup of* G, denoted $H < G$.

Example *(subgroup generated by element)*: Let x be an element of a group G. Then the subset

$$\langle x \rangle = \{..., x^{-2}, x^{-1}, 1, x^1, x^2, ...\}$$

is a subgroup of G.

Proposition: If $H \leq G$, then H has the same identity as G, and the inverse of an element in H is the same as the elements' inverse in G.

Proof: Let 1_G denote the identity in G, and let 1_H denote the identity in H. Since $H \subseteq G$, we have $h1_G = 1_G h = h$ for all $h \in H$. Thus 1_G is an identity of H. Since the identity of a group is unique, this implies $1_G = 1_H$.

Now suppose $h \in H$ has inverse $h_H^{-1} \in H$ and inverse $h_G^{-1} \in G$. Since $h, h_H^{-1} \in G$, this implies that h_H^{-1} is an inverse of h in G. Since inverses are unique, this implies $h_G^{-1} = h_H^{-1}$. ■

Definition (order of group and element): The *order* of a group G is the number of elements in it. The *order* of an element $x \in G$ is the smallest $n \in \mathbb{N}$ such that $x^n = 1$, and is denoted ord x. If no such n exists, then the order is ∞.

Proposition: Suppose G is a group. If $g^n = 1$, then ord g divides n.

Proof: Suppose otherwise. Thus $n = a \cdot \text{ord } g + b$, where $b < \text{ord } g$ and $a, b \in \mathbb{Z}_{\geq 0}$. Then we have

$$g^n = g^{a \cdot \text{ ord g}} g^b = g^b.$$

Since ord g is the minimal number such that $g^k = 1$, $g^b \neq 1$, so we have a contradiction. ■

Proposition: Suppose G is a finite group. Then ord g is finite for all $g \in G$.

Proof: If not, then the sequence $g, g^2, g^3, \ldots$ would contain pairwise distinct elements, and thus G would not be finite, contradiction. ■

1.2. Isomoprhisms and Homomorphisms

Definition (isomorphism): Let $(G, \times)$ and $(H, \star)$ be groups. A bijection $\varphi : G \to H$ is called an *isomorphism* if

$$\varphi(g_1 \times g_2) = \varphi(g_1) \star \varphi(g_2)$$

for all $g_1, g_2 \in G$. If there exists an isomorphism between G and H, then we say they are *isomorphic*, and denote it $G \cong H$.

Example *(isomorphisms)*:
- The identity map from G to itself is trivially an isomorphism.
- Define the map $\varphi : \mathbb{Z}\backslash 2\mathbb{Z} \to S_2$ by $\varphi(\{1, 2\}) = 0$ and $\varphi(\{2, 1\}) = 1$. Then it's easy to check that φ is an isomorphism, so $\mathbb{Z}\backslash 2\mathbb{Z} \cong S_2$.

Definition (automorphism): If $\varphi : G \to G$ is an isomorphism, then φ is an *automorphism*.

1.3. Classifying Groups of Order n

This section will be dedicated to classifying all groups of a certain order (up to isomorphism), for reasonable n.

1.3.1. Order 1

Let $G = \{e\}$. Any operation $\times : G \times G \to G$ will just be $e \times e = e$, so only one group exists.

1.3.2. Order 2

Since 2 is prime, the only group is C_2.

1.3.3. Order 3

Since 3 is prime, the only group is C_3.

1.3.4. Order 4

2. Rings

3. Fields