Algebra I

Hui Sun

October 8, 2024

Contents

Chapter 1

Groups

We will talk about some facts about groups.

Proposition 1.1. Here are some basic properties of groups.

1. If G is a group, and $e' \in G$ is an identity element, then $e' = e$.
2. Moreover, if $g \in G$ has inverses h_1, h_2, then h_1, h_2.
3. Let $g \in G$, and $gh = gf$, then $h = f$.

Definition 1.1 (abelian). A group G is commutative or abelian if for all $a, b \in G$, we have $ab = ba$.

Here are some examples:

1. Cyclic groups are commutative. A cyclic group $G = \langle g : g^n = e \rangle$, i.e., it is the group generated subject to this condition and generated by one element. Equivalently, for every $h \in G$, there exists m such that $h = g^m$.
2. $M_n(\mathbb{Z})$ under addition is commutative, under multiplication is not commutative.
3. $GL_n(\mathbb{Z})$ is a group under multiplication since it's determinant is a unit.

$$\begin{tikzcd} Gl_n(\mathbb{Z}) \arrow[r] & M_n(\mathbb{Z}) \arrow[d, "\det"] \\ \mathbb{Z}^* \arrow[u] & \mathbb{Z} \arrow[l] \end{tikzcd}$$

4. $GL_1(\mathbb{Z}) = Z^*$ is abelian.
5. $GL_2(\mathbb{Z})$ is not abelian, and so is not higher n
6. The dihedral group $D_n = \langle r, s : r^n = e, s^2 = e, rs = sr^{-1} \rangle$. Since $r^{-1} \neq r$ for $n > 2$, we have $rs \neq sr$. Hence D_n is not abelian for $n > 2$.
7. Alternatively, we can describe D_n explicity, i.e., by $rs = sr^{-1}$, then we can always write s in front of an r.
$$D_n = \{e, r, \ldots, r^{-1}, s, sr, \ldots, sr^{n-1}\}$$
8. S_n is also not abelian for $n > 2$. For example, $(123)(12), (23)(123)$. However, disjoint cycles commute.

Remark: orders of elements in groups.

1. $c_n = \langle f; f^n = e \rangle = \{e, f, f^2, \ldots, f^{n-1}\} \cong \{0, 1, \ldots, n-1\}$ under addition modulo n. Now given $m \in \{0, 1, \ldots, n-1\}$, what is $|m|$?

Definition 1.2 (order). The order of m, is the least positive integer l, denoted $|m|$ such that $lm = 0$. Moreover, if there exists integer k such that $lm = kn$, then l is the least positive integer suc that $\frac{lm}{n} \in \mathbb{Z}$.

Proposition 1.2. Elements m with $\gcd(m, n) = 1$ has order n. Moreover,

$$|m| = \frac{n}{\gcd(m, n)}$$

Proposition 1.3. If $\gcd(m, n) = 1$, then $m \in (\mathbb{Z}/n\mathbb{Z})^*$.

Proof. $m \in (\mathbb{Z}/n\mathbb{Z})^*$ if there exists l such that $lm = 1 \mod n$, which implies that $lm = 1 + kn$, i.e. $lm - kn = 1$, this implies that m, n are relatively prime. Moreover, this is if and only if $|m| = n$ in the additive group. □

Example 1.1. $\mathbb{Z}/12\mathbb{Z} : \{0, 1, 2, \ldots, 11\}$, and $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$, for the multiplicative group, $|5| = 2, |7| = 2, |11| = 2$. This implies

$$(\mathbb{Z}/12\mathbb{Z})^* \cong C_2 \times C_2$$

where $C_2 \times C_2 = \{(a, b) : a, b \in \pm 1\}$.

Definition 1.3 (group homomorphism). A group homomorphism $\varphi : G \to H$ is a function φ such that

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2), \varphi(e_G) = e_H, \varphi(g^{-1}) = \varphi(g)^{-1}$$

Definition 1.4 (isomorphism). An isomorphism φ is a bijective isomorphism. In other words, in there exists $\psi : H \to G$ such that

$$\varphi \circ \psi = id_H, \psi \circ \varphi = id_G$$

In fact,requiring φ as a bijection we can show ψ is indeed a homomorphism.

1.1 Lecture 10/08

Coproducts in Mod_R is direct sum.

We state the snake lemma here.

Proposition 1.4. Let

$$\begin{tikzcd} & A \arrow[r, "i"] \arrow[d, "\alpha"] & B \arrow[r, "p"] \arrow[d, "\beta"] & C \arrow[r] & 0 \\ 0 \arrow[r] & D \arrow[r, "j"] & E \arrow[r, "q"] & F & \end{tikzcd}$$

be a commutative diagram such that the rows are exact. Then

$$\begin{tikzcd} \ker\alpha \arrow[r] & \ker\beta \arrow[r] & \ker\gamma \arrow[dll] \\ \text{coker}\alpha = D/\alpha(A) \arrow[r] & \text{coker}\beta = E/\beta(B) \arrow[r] & \text{coker}\gamma = F/\gamma(C) \end{tikzcd}$$

is also exact.

We first talk about group actions. Let S be a sinite set with an action of a finite group G.

Theorem 1.1. Then

$$S \cong \bigsqcup_{s \in S/\sim} Orb(s) = \bigsqcup_{[s] \in S/\sim} G/stab(s)$$

where the $s \sim t$ if $t = g \cdot s$.

Definition 1.5. An element $s \in S$ is a fixeed point if $Stab(s) = G$, i.e. for all $g \in G$, we have

$$g \cdot s = \{s\}$$

Equivalently, $Orb(s) = \{s\}$.

Example 1.2. Conjugation action of G on itself

$$G = \bigcup_{[g] \in G/\sim} G/Stab(g)$$

where $Stab(g) = \{h \in G; hgh^{-1} = g\}$, This is called the centralizer of g, denoted by $Z(g)$.

For the fixed points g under conjugation, then for all $h \in G$, we have $gh = hg$, i.e., g is in the center of G. In other words,

$$g \in Z(G) = \bigcap_{g \in G} Z(g)$$

Corollary 1.1 (Class formula). We have

$$|G| = |Z(G)| + \sum_{g \in G/\sim, g \notin Z(G)} |G/Z(G)|$$

Definition 1.6. A finite group is a p group if $|G| = p^r$.

We see that if G is a nontrivial p-group, then

$$|G| = |Z(G)| + \sum |G/Z(g)|$$

so mod p, we have $|Z(G)| \equiv 0$. Hence if $e \in Z(G)$, then $Z(G)$ is trivial.

Definition 1.7 (normalizer). Let $N_G(S) = Stab(S)\{g \in G : gSg^{-1} = S\}$, and

$$Z_G(S) = \bigcap_{s \in S} N_G(\{s\}) = \{g \in G : gsg^{-1} = s, \forall s \in S\}$$

Remark: if $H \subset G$, we have $N_G(H) = \{g \in G : aHg^{-1} = H\}$. We observe that H is normal in $N_G(H)$, i.e., the largest subgroup of G in which H is normal. And $N_G(H)/H$ is called the weyl group.

Lemma 1.1. Let H be a subgroup of G, then

$$|G/N_G(H)| = \{A\}$$

where A is the set of subgroups that are conjugate to H.

Corollary 1.2. If H has finite index in G, then the number of subgroups of G conjugate to H is finite and divides $|G/H|$.