Abstract Algebra

: Lecture 10

Leo

2024.10.24

Today we talk about group actions.

all invertible mats.

Example 1. *Recall: Let $G = \mathrm{GL}(V)$, this is a linear group. And we have a set V, also a vector space.*

1. *Each $g \in G$ is a bijection from V to V;* ✓.
2. *$\forall v \in V$ and $1 \in G$ we have $v^1 = v$;* ✓.
3. *$\forall v \in V$ and $g, h \in G$ we have $v^{gh} = (v^g)^h$.*

We called G acts on V.

$k^n \xrightarrow{A} k^n \xrightarrow{B} k^l$.

$x \longmapsto BAx = x^{AB} = (x^A)^B$.

Definition 2. *Let G be a group and Ω be a set. We say that G acts on Ω if*

(1). each element of G is a bijection from Ω to Ω;

(2). $\forall \omega \in \Omega$, $\omega^1 = \omega$;

(3). $\forall \omega \in \Omega$ and $g, h \in G$ we have $\omega^{gh} = (\omega^g)^h$.

We denote this action by $\boxed{G \curvearrowright \Omega}$.

G is a group composed of bij. from Ω to Ω.

$\boxed{\text{i.e. } (hg)w = h(gw).}$

Example 3. *$Sym(\Omega)$ and $Alt(\Omega)$ acts on Ω naturally.* ✓.

$Sym(\Omega) \curvearrowright \Omega$, $Alt(\Omega) \curvearrowright \Omega$.

Example 4. *Let G be a group, for each element $g \in G$, we define action $g : x \mapsto xg$ forall $x \in G$. We denote this map by $\hat{g}$, called right multiplication. This is a group action. We denote the group of this action by $\hat{G}$.*

$\hat{G} = \{\hat{g} \mid \hat{g} : x \mapsto xg \text{ for all } x \in G, \text{ where } g \in G\}$.

$\rightarrow x^g = g^{-1}xg$.

Example 5. *Let G be a group, for each element $g \in G$, we define action $g : x \mapsto g^{-1}xg$ forall $x \in G$. We denote this map by $\tilde{g}$, called conjugation. This is a group action. We denote the group of this action by $\tilde{G}$.*

$\tilde{G} = \{\tilde{g} \mid \tilde{g} : x \mapsto g^{-1}xg \text{ for all } x \in G, \text{ where } g \in G\}$.

Example 6. *Let G be a group, for each element $g \in G$, we define action $g : x \mapsto g^{-1}x$ forall $x \in G$. We denote this map by $\breve{g}$, called left multiplication. This is a group action. We denote the group of this action by $\breve{G}$.*

$\check{G} = \{\check{g} \mid \check{g} : x \mapsto g^{-1}x \text{ for all } x \in G, \text{ where } g \in G\}$.

Exercise 7. *If we ~~right~~ write group action in another way, i.e. $(gh)\omega = g(h\omega)$, check example 4,5,6.*

Proposition 8. *1.* $\hat{g}, \breve{g}, \tilde{g} \in \mathrm{Sym}(G)$.

2. $\hat{G}, \breve{G}, \tilde{G} \leqslant \mathrm{Sym}(G)$.

$(\hat{g}\hat{h})w = w(h \cdot g) = (w \cdot h) \cdot g = \hat{g}(\hat{h}w)$.

$(\tilde{g}\tilde{h})w = g^{-1}h^{-1}whg = g^{-1}(\tilde{h}w)g = \tilde{g}(\tilde{h}w)$.

$(\check{g}\check{h})w = g^{-1}h^{-1}w = g^{-1}(h^{-1}w) = \check{g}(\check{h}w)$.

$xg = g_1^{-1}xg_1$ for some g_1.

$\hat{G}\cap\check{G} = \{\bar{g} \mid \bar{g}: x\mapsto xg,\ xg = g_1^{-1}x$ for some $g_1^{-1}\}$.

$x=1 \Rightarrow g = g_1^{-1}g_1 = 1$

$x^{\bar{g}\bar{g}_1} = (xg)^{\bar{g}_1} = (g_1^{-1}x)^{\bar{g}_1} = g_1^{-1}xg_1 \in \tilde{G}. \Rightarrow g_1^{-1}xg_1 = x \Rightarrow g_1x = xg_1$

$\Rightarrow \bar{g} = \bar{1}$.

for all $x\in G$. $g_1\in Z(G)$. $g_1^{-1}\in Z(G) \Rightarrow \hat{G}\cap\check{G} = Z(\check{G}) = Z(\hat{G})$,

3. $\forall g,h\in G$, $\hat{g}\check{h} = \check{h}\hat{g}$.
4. $\forall g\in G$, $\hat{g}\check{g} = \tilde{g}$;
5. $\hat{G}\cap\check{G} = Z(\hat{G}) = Z(\check{G})$, $\hat{G}\cap\tilde{G} = \check{G}\cap\tilde{G} = \{1\}$;
6. $\langle\hat{G},\check{G}\rangle = \hat{G}\check{G} = \hat{G}\circ\check{G} = \hat{G}:\check{G} = \check{G}:\hat{G}$;

$Z(\hat{G}) = \{\bar{g} \mid \bar{g}: x\mapsto xg = gx\}. = Z(\check{G})$

$C\in(G\times H)$, $C\cong A\leq Z(G)\times\{0\}\cong Z(G)$.

Definition 9. *For two groups G and H, assume there exist $C\lesssim Z(G)$ and $C\lesssim Z(H)$. s.t. $C\neq\{1\}$. Let $Z_1\leqslant Z(G)$ and $Z_2\leqslant Z(H)$. s.t. $Z_1\simeq Z_2\simeq C$. Let ϕ be an isomorphism from Z_1 to Z_2. Let $X = (G\times H)/\langle(x,x^{\phi})|x\in Z_1\rangle\simeq(G\times H)/C$. This group X is called a central product of G and H, denoted by $G\circ H$.*

Definition 10. *Let $H,K<G$ s.t. $H\lhd G$ and $H\cap K=\{1\}$. Then $\langle H,K\rangle = HK = H\rtimes K = H:K$ called a semi-direct product of H and K.*

G acts on Ω also can be said as an action of G on Ω or group action of G on Ω.

Orb(w).

Definition 11. *Let G act on Ω. Then G partitions Ω into orbits, where an orbit is $\Delta=\omega^G=\{\omega^g|g\in G\}$, where $\omega\in\Omega$. So $\Omega=\bigsqcup_{\omega\in\Omega}\omega^G$.*

$w_1\sim w_2 \Leftrightarrow \exists g\in G$ s.t. $g(w_1)=w_2$. ($w_1^g = w_2$).

equil. rel.

Example 12. *$\tilde{G}$ acts on G naturally, i.e. $x^g = g^{-1}xg$. $G = x_0^G\sqcup x_1^G\sqcup\cdots\sqcup x_t^G$, where $x_0=e$, $x_i^G=\{g^{-1}x_ig|g\in G\}$ called a conjugacy class of x_i, denoted by $C(x_i)$. $C(x_i)=\{g^{-1}x_ig|g\in G\}$ is a orbit of the action of $\tilde{G}$ on G.* ✓.

Stab(w).

Definition 13. *For G acting on Ω, $G_\omega=\{g\in G|\omega^g=\omega\}$ called the stabilizer of ω in G. It's easy to check that G_ω is a subgroup of G.* ✓.

$|Orb(w)| = |G : Stab(w)| \Leftrightarrow |G| = |Orb(w)|\,|Stab(w)|$.

Theorem 14. *(Orbit-Stabilizer Theorem) For G acting on Ω, For $\omega\in\Omega$, $|G|=|\omega^G|\cdot|G_\omega|$.*

Orb(w) =

证明. Let $\Delta=\omega^G=\{\delta_1,\delta_2,\ldots,\delta_m\}$ write $\delta=\delta_1$. Let g_i s.t. $\delta^{g_i}=\delta_i$ for $1\leqslant i\leqslant m$. ✓.

Claim: For any element $x\in G$, $\delta^x=\delta_i\Leftrightarrow x\in G_\delta g_i$. Which is due to $\delta^x=\delta_i=\delta^{g_i}\Leftrightarrow\delta^{xg_i^{-1}}=\delta\Leftrightarrow xg_i^{-1}\in G_\delta\Leftrightarrow x\in G_\delta g_i$.

$\delta^x = \delta_i = \delta^{g_i} \Rightarrow \delta^{xg_i^{-1}} = \delta$ $xg_i^{-1}\in Stab(\delta)$ $x\in g_iStab(\delta)$

Recall $G=G_\delta\sqcup G_\delta g_2\sqcup\cdots\sqcup G_\delta g_m$, we have $|G|=|G_\delta|+|G_\delta g_2|+\cdots+|G_\delta g_m|$, i.e. $|G|=|\Delta||G_\delta|$. □

$= m\,|G_\delta| = |\Delta|\,|G_\delta|$. ✓.

类方程.

Oberserve: consider conjugate action of G on itself, $|x^G|=1$ iff $x\in Z(G)$. So by Orbit-Stabilizer Theorem, $|G|=|Z(G)|+|C(g_1)|+\cdots+|C(g_r)|$ and $|g_i^G|\mid|G|$ due to $|G|=|C(g_i)|\cdot|C_G(g_i)|$. ✓.

$x\in Z(G)\Leftrightarrow gx=xg.\ \forall g$
$\Leftrightarrow x=g^{-1}xg.\ \forall g$
$\Leftrightarrow C_x=\{x\}$
$\Leftrightarrow |C_x|=1$.

Theorem 15. *(Sylow's 1st Theorem) Let G be a finite group, $|G|=p^em$ s.t. p is a prime and $(p,m)=1$, a subgroup H of G s.t. $|H|=p^e$ exists. And H is called a Sylow p-subgroup of G, denoted by $H\in Syl_p(G)$.*

Recall: If G is abelian, then let $H=\{g\in G||g|\mid p^e\}$. Then H is a subgroup of G and $|H|=p^e$. In other words H is a Sylow p-subgroup of G.

(+1 at a time).

① induction on $|G|$. $|G| = p^nm$.

证明. Write $|G|=|Z(G)|+|C(g_1)|+\cdots+|C(g_r)|$. If $p||Z(G)|$ then $Z(G)$ has a Sylow p-subgroup N and $N\lhd G$. Then $\bar{G}=G/N$ has order $|\bar{G}|<|G|$. If $|N|=p^e$ then N is a Sylow p-subgroup of G. If $|N|<p^e$ then $|\bar{G}|<p^em$. By induction, $\bar{G}$ has a Sylow p-subgroup $\bar{N}$, the preimage of $\bar{N}$ is a Sylow p-subgroup of G.

Orb(g_i), but is also a conjugacy class.

Stab(g_i). otherwise $p \nmid |G|$.

Now suppose $p \nmid |Z(G)|$. Then $p \nmid |C(g_i)|$ for some i. By Orbit-Stabilizer Theorem, $|G| = |C(g_i)| \cdot |C_G(g_i)|$. Then $p^e \mid |C_G(g_i)|$ and by induction $C_G(g_i)$ has a Sylow p-subgroup N, which is also a Sylow p-subgroup of G. $\square$

Theorem 16. *(Cauthy) If $p \mid |G|$ then G has a subgroup of order p.*

Lemma 17. *If G is a p-group i.e. $|G| = p^n$ then G has a non-trivial center.* (不由 Sylow's law 导出)

9. This exercise outlines a proof of Cauchy's Theorem due to James McKay (*Another proof of Cauchy's group theorem*, Amer. Math. Monthly, 66(1959), p. 119). Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:

ordered. $x_i \cdots x_p x_1 \cdots x_{i-1}$

$$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}.$$

$x_{i-1} x_i$ $(x_i \cdots x_p)^{-1} = x_1 \cdots x_{i-1}$

(a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p.

Define the relation $\sim$ on $\mathcal{S}$ by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

(b) Show that a cyclic permutation of an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.

(c) Prove that $\sim$ is an equivalence relation on $\mathcal{S}$.

(d) Prove that an equivalence class contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

(e) Prove that every equivalence class has order 1 or p (this uses the fact that p is a *prime*). Deduce that $|G|^{p-1} = k + pd$, where k is the number of classes of size 1 and d is the number of classes of size p.

(f) Since $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element x in G with $x^p = 1$, i.e., G contains an element of order p. [Show $p \mid k$ and so $k > 1$.] Otherwise, $p \mid$ LHS, RHS $\equiv 0 \pmod p$