The tenth problem set (Review style)

Thursday, December 11, 2014
1:15 PM

1. Let G be a finite cyclic group. Suppose $|G|=n$ and d is a positive divisor of n. Prove that

   (a) $\exists\, g\in G,\ o(g)=d$.

   (b) $\exists\, N \trianglelefteq G,\ |G/N|=d$.

2. Give a group G and its subgroup H s.t. $H \ntrianglelefteq G$.

3. For $g\in G$, let $\rho_g : G \to G$, $\rho_g(x)=gxg^{-1}$.

   Prove that ρ_g is an isomorphism.

4. Let $\phi: G\to H$ be an isomorphism. Prove that

   (a) $\phi^{-1}: H\to G$ is an isomorphism.

   (b) $o(g) = o(\phi(g))$.

5. Prove that $\mathbb{Z}_{mn}^{\times} \simeq \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$ if $\gcd(m,n)=1$.

   Use this to show $\mathbb{Z}_{35}^{\times}$ is NOT cyclic.

   (Remark. One can show $\mathbb{Z}_{p^n}^{\times}$ is cyclic if p is an odd prime. For small numbers you can check this by finding the orders of elements.)

6. Suppose that G is a finite group and $|G| = p^2$ where p is prime. Prove that either $G \simeq \mathbb{Z}_{p^2}$ or $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

(Hint. (1) $Z(G) \neq \{e\}$.

(2) $|G/Z(G)| \mid p^2 \Rightarrow$ it is either $1, p, p^2$.

By (1) it cannot be p^2. Since $G/Z(G)$ cannot be cyclic, $|G/Z(G)| \neq p$. And so G is abelian.

(3) Suppose G is NOT cyclic. Conclude that

$e \neq g \in G \Rightarrow o(g) = p$.

(4) Suppose $e \neq a, b \in G$ and $b \notin \langle a \rangle$.

Show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

(5) Consider $\mathbb{Z} \times \mathbb{Z} \to G$,

$(i, j) \mapsto a^i b^j$,

and use the first isomorphism theorem.)

7. Suppose H, K are normal subgroups of G, and

$H \cap K = \{e\}$.

(a) Prove that $\forall h \in H, k \in K, hk = kh$.

(b) Prove that $H \times K \simeq HK$.

(Hint. (a) Show that $hkh^{-1}k^{-1} \in H \cap K$.

(b) Consider $(h,k) \longmapsto hk$.)

8. Let G be a cyclic group of order n. Prove that

$$f: G \to G, \quad f(g) = g^k \quad \text{is a group isomorphism}$$

if and only if $\gcd(k,n) = 1$.

(Hint. ($\Longrightarrow$) Suppose $G = \langle g_0 \rangle$. Since f is onto,

conclude $G = \langle g_0^k \rangle$. Consider $o(g_0^k)$.

($\Longleftarrow$) (1) f is a group homomorphism.

(2) $\operatorname{Im} f = \langle f(g_0) \rangle$.

(3) Consider $o(g_0^k)$.)

9. For a group G, let $\operatorname{Aut}(G) := \{\phi : G \to G \mid \phi \text{ is an isomorphism}\}$

Show that $(\operatorname{Aut}(G), \circ)$ is a group.

10. Let G be a cyclic group of size n. Prove that

$$\operatorname{Aut}(G) \simeq \mathbb{Z}_n^{\times}.$$

(Hint. Suppose $G = \langle a \rangle$. Let $\phi \in \operatorname{Aut}(G)$. Then

$\phi(g_0)=g_0^k$ for some $k \Rightarrow \phi(g_0^{2^i})=\phi(g_0)^{2^i}=g_0^{2^i k}$

$\Rightarrow \forall g\in G,\ \phi(g)=g^k$. Use problem 8.

Notice. $(f_{k_1}\circ f_{k_2})(g)=f_{k_1}(g^{k_2})=(g^{k_2})^{k_1}=g^{k_1k_2}$

$\Rightarrow f_{k_1}\circ f_{k_2}=f_{k_1k_2}$.)

11. Show that $\mathrm{Aut}(\mathbb{Z})\simeq \mathbb{Z}_2$.

12. Suppose G is a finite group. Then

$$|Cl(g)|=[G:C_G(g)],$$

where $Cl(g):=\{aga^{-1}\mid a\in G\}$ and

$$C_G(g)=\{a\in G\mid ag=ga\}.$$

(Recall. $G\curvearrowright G$ by conjugation. And

$$|O(x)|=[G:G_x].)$$

13. Find $|C_{S_5}((1,2)(3,4))|$.

(Hint. First find $|Cl((1,2)(3,4))|$. Then use problem 12.)

14. Find the sizes of conjugacy classes of D_n.

How many conjugacy classes are there?

(Hint. Suppose $\underline{a}$ is the reflection about x-axis and $\underline{b}$ is the $\frac{2\pi}{n}$-rotation about the origin.

$\Rightarrow G = \langle b \rangle \cup a\langle b \rangle$, and $b^i a = a b^{-i}$.

- $b^j b^i b^{-j} = b^i$; $(ab^j) b^i (ab^j)^{-1} = a b^i a$
$$= b^{-i}.$$

$\Rightarrow Cl(b^i) = \{b^i, b^{-i}\}$.

- $b^j (ab^i) b^{-j} = a b^{i-2j}$

$$(ab^j)(ab^i)(ab^j)^{-1} = a(b^j a) b^i b^{-j} a$$
$$= b^{i-2j} a$$
$$= a b^{2j-i}.$$

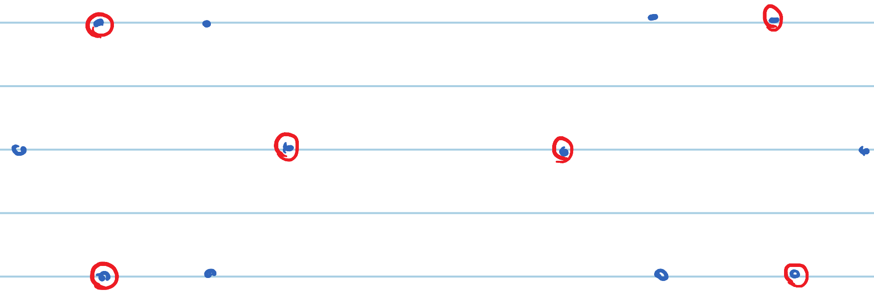
$\Rightarrow Cl(ab^i) = \{ a b^{i-2j}, a b^{2j-i} \mid 0 \le j \le n-1 \}$

Your answer depends on whether n is odd or even.

15. Prove that, for any positive integers k and n, there is a subgroup H of D_{kn} which is isomorphic to D_n.

(Hint. Consider regular n-gons whose vertices are among the vertices of a regular kn-gon.

For instance



- How many such regular n-gons do we have?
- Notice that D_{kn} sends one such n-gon to another such n-gon.
- Consider the stabilizer of one such n-gon., and compute its size.)

16. Let H and K be two normal subgroups of G. Suppose $H \cap K = \{e\}$. Prove that G is isomorphic to a subgroup of $G/H \times G/K$.

(Hint. Consider $g \mapsto (gH, gK)$.)

17. Suppose G is a finite group, and $|G| = p^m q^n$,

where p and q are two distinct primes.

Suppose $\exists\, P \trianglelefteq G$, $Q \trianglelefteq G$, $|P| = p^m$ and $|Q| = q^n$.

Prove $pq \mid |Z(G)|$.

(Hint. (1) Show $P \cap Q = \{e\}$.

(2) Use problem 7 and conclude

$Z(G) \simeq Z(P) \times Z(Q)$.)

18. Show that $S_4 \not\simeq D_{12}$.

(Hint. $\nexists\, \sigma \in S_4$, $o(\sigma) = 12$.)

19. Show that $G := \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} \,\middle|\, x = [\pm 1]_n, y \in \mathbb{Z}_n \right\}$ is

a subgroup of $GL_2(\mathbb{Z}_n) = \{A \in M_2(\mathbb{Z}_n) \mid \det(A) \in \mathbb{Z}_n^\times\}$

(You do not need to show $GL_2(\mathbb{Z}_n)$ is a group.)

Prove that $G \simeq D_n$.

(Hint. $D_n = \langle b \rangle \cup a\langle b \rangle$ as above.

$$a^i b^j \longmapsto \begin{bmatrix} [(-1)^i] & [j]_n \\ 0 & 1 \end{bmatrix}.)$$

20. Suppose $H \le S_n$ and $|H|$ is odd. Then $H \subseteq A_n$.

(Hint. $\mathrm{sgn}: S_n \to \{\pm 1\}$.

$$\left.\begin{array}{ll} \forall\, h \in H, & o(\mathrm{sgn}(h)) \mid o(h) \\ & o(\mathrm{sgn}(h)) \mid |\{\pm 1\}| = 2 \\ & o(h) \mid |H| \\ & 2 \nmid |H| \end{array}\right\} \Rightarrow o(\mathrm{sgn}(h)) = 1 \Rightarrow \mathrm{sgn}(h) = 1 \Rightarrow h \in A_n.)$$

21. Suppose p and q are two primes.

ⓐ Prove that any group of order p is cyclic.

ⓑ Suppose G is a finite group and $|G| = pq$.

Prove that either G is abelian or $Z(G) = \{e\}$.

(Hint. ⓐ $e \ne a \in P \Rightarrow 1 \ne o(a) \mid |P| = p \Rightarrow o(a) = p$

$$\left.\begin{array}{l} \Rightarrow |\langle a \rangle| = o(a) = p \\ \langle a \rangle \subseteq P \end{array}\right\} \Rightarrow P = \langle a \rangle.$$

ⓑ $|Z(G)| \mid |G| = pq \Rightarrow |Z(G)| \in \{1, p, q, pq\}$.

If G is NOT abelian and $Z(G) \ne \{e\}$, then

$|Z(G)| = p$ or $q \Rightarrow |G/Z(G)| = q$ or p

$\Rightarrow G/Z(G)$ is cyclic which is a contradiction.)

22. $Z(S_n) = \{(1)\}$ if $n \geq 3$.

(Hint. $\sigma \in Z(S_n) \Rightarrow \forall i \neq j$, $\sigma (i, j) \sigma^{-1} = (i, j)$

$= (\sigma(i), \sigma(j))$

$\Rightarrow \forall i \neq j$, $\sigma(i) \in \{i, j\}$.

$\Rightarrow \sigma(i) \in \bigcap_{i \neq j} \{i, j\} \underset{n \geq 3}{=} \{i\}$.)