Notes on Homework 6

Math 307 Abstract Algebra Homework 6

Your name

Five points for each question.

1. (a) Let $H = \langle (1,2,3) \rangle \in A_4$. Write down all the left cosets of H in A_4, and the right cosets of H in S_4.

   (b) Let $H = \{e^{it} : t \in [0, 2\pi)\} \leq \mathbb{C}^*$. Describe geometrically the left cosets of H.

2. Suppose K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

3. Let G be a group with $|G| = pq$, where p, q are primes. Prove that every proper subgroup of G is cyclic. Give an example to show that such a group G may not be cyclic.

4. Let G be a group of order p^2 for a prime p. Show that G is cyclic or $g^p = e$ for all $g \in G$.

5. Show that a group of order 55 cannot have exactly 20 elements of order 11? Give a reason for your answer.

   [Hint: If G is cyclic, then number of elements of order 11 equal???

   If G is not cyclic, then $a \in G$ has order 1, 5, or 11. So, ...]

6. Let G be a group, and $H \leq K \leq G$. Suppose $a_1K, \ldots, a_rK$ are distinct cosets of K in G, and $b_1H, \ldots, b_sH$ are distinct cosets of H in K. Prove that a_ib_jH with $1 \leq i \leq r, 1 \leq j \leq s$ are all the distinct cosets of H in G. Deduce that

   $$|G : H| = |G : K|\,|K : H|.$$

   Recall that $H \leq G$ is a normal subgroup if $aH = Ha$ for all $a \in G$.

7. (a) Prove that if $H \leq G$ and $|G : H| = 2$, then H is normal.

   (b) Deduce that if $H \leq S_n$ contains a an odd permutation, then H has a normal subgroup.

8. Let $H \leq G$.

   (a) Prove that the map $f : aH \to Ha$ defined by $f(ah) = ha$ is a bijection.

   (b) Prove that H is normal if and only if $aHa^{-1} \subseteq H$ for all $a \in G$.

9. (Extra credits) Prove that A_5 has no subgroup of order 30.

   [Hint: Prove by contradiction. Assume $H \leq A_5$ has 30 elements. Then $A_n - H$ is a left coset as well as a right coset of H in A_n. Argue that H has an element $\sigma_1 = (i_1, i_2)(j_1, j_2)$, and then show that $\sigma_2 = (i_1, j_2), (i_2, j_1), \sigma_3 = (i_1, j_1)(i_2, j_2) \in H$. Then argue that $\{\varepsilon, \sigma_1, \sigma_2, \sigma_3\}$ is a 4-element subgroup of H, ...]

Some basic results

Theorem 8.1 Let $g = (g_1, \ldots, g_k) \in G_1 \oplus \cdots \oplus G_k$. If $|g_1|, \ldots, |g_k|$ are finite, then $|g| = \text{lcm}(|g_1|, \ldots, |g_k|)$; if one of the $|g_i|$ is infinite, then $|g|$ is infinite.

$n_1 \quad n_k$

Proof: Suppose $m = \text{lcm}(n_1, \cdots, n_k)$, $n_j = |g_j|$ $j = 1, \cdots, k$.

Then

$$(g_1, \cdots, g_k)^m = (g_1^m, g_2^m, \cdots g_k^m) = (e_1, \cdots, e_k)$$

$\because \; n_j \mid m \quad \forall j = 1, \cdots, k$.

Assume $(g_1, \cdots, g_k)^l = (e_1, \cdots, e_k)$.

$\therefore \; g_j^l = e_j \quad \forall j = 1, \cdots, k$

$\therefore \; |g_j| \mid l$. $\therefore$ l is a common multiple of $n_1, \cdots, n_k$.

So $l \geq m$.

Hence m is the smallest positive integer such that $(g_1, \cdots, g_k)^m = (e_1, \cdots, e_k)$.

i.e., $|(g_1, \cdots, g_k)| = m$.

Theorem 8.2 Let $G_1, \ldots, G_k$ be finite cyclic groups. Then $G_1 \oplus \cdots \oplus G_k$ is cyclic if and only if $\gcd(|G_i|, |G_j|) = 1$ for all $1 \leq i, j \leq k$, equivalently, $\text{lcm}(|G_1|, \ldots, |G_k|) = \prod_{j=1}^{k} |G_j|$.

In particular, $\mathbf{Z}_{n_1 \cdots n_k} = \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_k}$ if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Remark If $k > 1$ and one of the cyclic group G_i is infinite, then $G_1 \oplus \cdots \oplus G_k$ is not cyclic.

$\mathbb{Z}_6$ one of g_i has infinite order, then $(g_1, \cdots, g_k)^n = (g_1^n, \cdots, g_i^n, \cdots g_k^n) \neq (e_1, \cdots, e_k)$ $\because g_i^n \neq e_i$.

$\therefore |(g_1, \cdots, g_k)|$ is infinite.

Example: $\mathbb{Z}_6 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{121}$

$= \{(a, b, c) : a \in \mathbb{Z}_6, b \in \mathbb{Z}_5, c \in \mathbb{Z}_{121} = \mathbb{Z}_{11^2}\}$

$|(a, b, c)| = \text{lcm}(|a|, |b|, |c|)$

$|(3, 2, 1)| = \text{lcm}(2, 5, 121) = 1210$

Max $|(1, 1, 1)| = \text{lcm}(6, 5, 121) = 6 \cdot 5 \cdot 121 = 3630$

$\mathbb{Z}_6 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{121} = \langle (1, 1, 1) \rangle$

Example: $\mathbb{Z}_6 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{121}$ has $6 \times 10 \times 121$ elements

$|(1, 1, 1)| = \text{lcm}(6, 10, 121) = 2^1 \cdot 3 \cdot 5 \cdot 11^2 < 3630$

$2 \cdot 3 \quad 2 \cdot 5 \quad 11^2$

$6 \times 10 \times 121$

$m \mid 3630$ ✓ $\quad 4 \mid m$ is impossible

More results

Notation Let k be a factor of n; set $U_k(n) = \{x \in U(n) : x = pk + 1, p \in \mathbf{N}\}$.

Example Let $U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$. Then
$U_4(20) = \{1, 9, 13, 17\} \cong U(5) = \{1, 2, 3, 4\}$,
$U_5(20) = \{1, 11\} \cong U(4) = \{1, 3\}$, and
$U(20) \cong U(4) \oplus U(5) \cong U_5(20) \oplus U_4(20)$.

$= \{\bar{k} \in \mathbb{Z}_{20} : \gcd(k, 20) = 1\}$ under multiplication (modulo 20)

$\mathbb{Z}_{20} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_5$.

$\phi([9]_{20}) = ([9]_4, [9]_5) = ([3]_4, [4]_5)$

$\phi: U(20) \to U(4) \oplus U(5)$

$\phi([x]_{20}) = ([x]_4 \oplus [x]_5)$.

$\phi([1]) = ([1], [1])$

$\phi([21]) = ([21]_4, [21]_5) = ([1]_4, [1]_5)$

Theorem 8.3 If $\gcd(s, t) = 1$, then $U(st) \cong U(s) \oplus U(t)$, $U_t(st) \cong U(s)$ and $U_s(st) \cong U(t)$.

Proof. Define $\phi : U(st) \to U(s) \oplus U(t)$ $\phi(x) = (x_1, x_2) \in U(s) \oplus U(t)$ such that $x_1 = x \pmod{s}$ and $x_2 = x \pmod{t}$. We will show that it is a group isomorphism.

Well defined: If $\gcd(x, st) = 1$, then $\gcd(x_1, s) = 1$ and $\gcd(x_2, t) = 1$. So, $(x_1, x_2) \in U(s) \oplus U(t)$. ✓

One-one: If $\phi(x) = (x_1, x_2) = \phi(y)$, then $x = sp_1 + x_1 = sp_2 + x_2$ and $y = tq_1 + x_1 = sq_2 + x_2$ for some $p_1, p_2, q_1, q_2 \in \mathbf{Z}$, So, $x - y = s(p_1 - p_2) = t(q_1 - q_2)$ is divisible by s and t. Thus, $x - y = 0 \in \mathbf{Z}(st)$.

Onto: Because $\gcd(s, t) = 1$, there exist $u_1, u_2 \in \mathbf{Z}$ be such that $u_1 = sp_1 + 1 = tp_2$, i.e., $1 = tp_2 - sp_1$, and $u_2 = sq_1 = tq_2 + 1$, i.e., $1 = sq_1 - tq_2$. Regard $u_1, u_2 \in U(st)$. Then for any $(x_1, x_2) \in \mathbf{Z}_1 \oplus \mathbf{Z}_2$, $\phi(u_1x_1 + u_2x_2) = (x_1, x_2)$.

Operation preserving: Suppose $x, y \in U(st)$. Then $\phi(xy) = ([xy]_s, [xy]_t) = ([x]_s[y]_s, [x]_t[y]_t) = \phi(x)\phi(y)$.

Combining the above, we see that ϕ is an isomorphism.
The proof of $U(s) \cong U_t(st)$ is left as an homework. □

Remark For any $m = p_1^{r_1} \cdots p_k^{r_k}$, where $p_1, \ldots, p_k$ are distinct primes and $r_1, \ldots, r_k \in \mathbf{N}$, we have

$$U(m) \cong U(p_1^{r_1}) \oplus \cdots \oplus U(p_k^{r_k}).$$

For any prime p we have

(1) $U(2) = \{1\}, U(4) = \mathbf{Z}_2$, $U(2^n) \cong \mathbf{Z}_2 \oplus \mathbf{Z}_{2^{n-2}}$ for $n \geq 3$;
(2) $U(p^n) \cong \mathbf{Z}_{p^n - p^{n-1}}$ if $p > 2$.

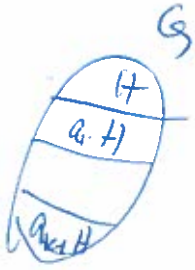
$U(3^n) \cong \mathbb{Z}_{3^n - 3^{n-1}}$.

Examples

$U(105) \sim U(3 \cdot 5 \cdot 7) \sim U(3) \oplus U(5) \oplus U(7) \sim \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_6$.

$U(720) \sim U(16 \cdot 9 \cdot 5) \sim U(19) \oplus U(9) \oplus U(5) \sim \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_4$.

$U(2018) \cong \mathbb{Z}_m$ for some m.
$\cong U(p_1^{r_1}) \cdots U(p_k^{r_k})$
$\cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$.



Chapter 9 Normal subgroups and Factor Groups

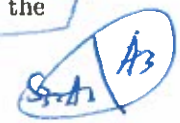
Definition A subgroup H of a group is normal if $aH = Ha$ for all $a \in G$. We write $H \triangleleft G$.

Theorem 9.1 A subgroup H is normal if and only if H is normal, i.e., $gHg^{-1} \leq H$ for all $g \in G$.

Proof. Done in homework.

Theorem 9.2 Let $H \leq G$. Then $G/H = \{aH : a \in G\}$ is a group (known as the factor group) under the operation $(aH)(bH) = (ab)H$ if and only if $H \triangleleft G$.

Proof. Key step: The operation is well-defined if and only if H is normal.



Example: $G = S_3$ $\quad H_1 = A_3 = \langle (1,2,3) \rangle = \{\varepsilon, (1,2,3), (1,3,2)\}$

is normal because

$\sigma H_1 = H_1 \sigma = H_1$ if $\sigma \in A_3$

$gHg^{-1} = \{ghg^{-1} : h \in H\}$

$\leq H$

$\sigma H_1 = H_1 \sigma = S_3 - A_3$ if $\sigma \in S_3 - A_3$

$*$	A_n	$S_n - A_n$
A_n	A_n	$S_n - A_n$
$S_n - A_n$	$S_n - A_n$	A_n

Remark Example $G = S_3$

$H_2 = \langle (1,2) \rangle$

$= \{\varepsilon, (1,2)\}$ is not normal!

For $\sigma = (1,3)$

$\sigma H_2 \neq H_2 \sigma$

Example 2

$T = \{e^{it} : t \in [0, 2\pi)\}$

$\leq \mathbb{C}^*$ is normal

All cosets are:

$rT : r > 0$.

$(rT) * (sT)$

$= (rs)T$

i.e. $1T = T$ satisfies

$1 \cdot T) * (sT) = sT$