Math 1530: Homework 8

Milan Capoor

21 November 2023

6.13

Let G be a group, and let X be a set on which G acts.

(a) Suppose that $\#G = 15$ and $\#X = 7$. Prove that there is some element of X that is fixed by every element of G. (Hint. Use the Orbit-Stabilizer Counting Theorem.)

We want to show that there exists an $x \in X$ such that $gx = x$ for all $g \in G$. Equivalently, $G_x = G$ for some $X \in X$. By the Orbit-Stabilizer Counting Theorem,

$$\#X = \sum_{i=1}^{k} \#Gx_i = \sum_{i=1}^{k} \frac{\#G}{\#G_{x_i}} \implies 7 = \sum_{i=1}^{k} \#Gx_i = \sum_{i=1}^{k} \frac{15}{\#G_{x_i}}$$

Since $\#G_x$ divides $\#G$ by Lagrange's theorem, we know that $\#G_{x_i} = \{1, 3, 5, 15\}$. But since $\#G$ is finite,

$$\#Gx_i = \frac{\#G}{\#G_{x_i}}$$

so the quotient must be an integer not greater than 7. Thus, each $\#G_{x_i} = \{3, 5, 15\}$ and $\#Gx_i = \{1, 3, 5\}$

However, since $\#X = 7$, we must have that $\#Gx_i = 1$ for some i because $3 \not| 7$ and $5 \not| 7$. Thus, $\#G_{x_i} = 15$ and $G_{x_i} = G$ for some $x_i \in X$ and there is some element fixed by every element of G. $\blacksquare$

(b) What goes wrong with your proof in (a.) if $\#G = 15$ and $\#X = 6$ or $\#X = 8$?

If $\#X = 6$, then there is a possibility there is no orbit of size 1 (and thus no stabilizer of size 15) because

$$6 = 3 + 3$$

and $3 \in \{\frac{\#G}{\#G_{x_i}}\}$. Similarly, if $\#X = 8$,

$$8 = 3 + 5$$

and $5 \in \{\frac{\#G}{\#G_{x_i}}\}$. Thus, there may not be an element fixed by every element of G. $\blacksquare$

6.15abc

Let G act on itself by conjugation as described in the proof of Theorem 6.25. Let $x \in G$. The conjugacy class of x is the orbit of x for this action; i.e., it is the set $\{gxg^{-1} : g \in G\}$.

(a) Prove that G is the disjoint union of its conjugacy classes.

By Proposition 6.19(b), there is an equivalence relation on X such that the equivalence class of x is its orbit Gx. By Theorem 1.25b, X is the disjoint union of the distinct equivalence classes so

$$X = Gx_1 \cup Gx_2 \cup \cdots \cup Gx_k$$

However, here with $X = G$, Gx_i is just the conjugacy class of x_i so G is the disjoint union of its conjugacy classes. ■

(b) Prove that G is abelian if and only if each conjugacy classes of G contains a single element.

If G is abelian, then for all $x \in G$, $gxg^{-1} = xgg^{-1} = x$ for all $g \in G$. Thus, the conjugacy class of x is $\{x\}$ and all conjugacy classes have only a single element.

For the other direction, suppose each conjugacy class contains only a single element, say x', such that

$$\{x'\} = \{gxg^{-1} : g \in G\} \implies \#Gx = 1$$

By Proposition 6.19c,

$$\#Gx = \frac{\#G}{\#G_x} \implies \#G_x = \#G \implies G_x = G$$

The stabilizer of x is

$$G_x = \{gxg^{-1} = x : g \in G\} = \{gx = xg : g \in G\} = G$$

so G is abelian. ■

(c) Describe the conjugacy classes of the dihedral group D_3.

$D_3 = \{e, r_1, r_2, f_1, f_2, f_3\}$. We will consider the conjugacy classes of each element in turn using the composition formulae in Example 2.46.

(a) The conjugacy class of e is $\{e\}$ because $geg^{-1} = gg^{-1} = e$ for all $g \in G$. By part (a), we know that the conjugacy classes of D_3 are the disjoint union of the conjugacy class of e and the conjugacy classes of the other elements. Thus, the other conjugacy classes of D_3 do not contain e.

(b) r_1:

$$\begin{aligned} r_1r_1r_1^{-1} &= & & & r_1 \\ r_2r_1r_2^{-1} &= r_2^{-1} = & & & r_1 \\ f_1r_1f_1^{-1} &= f_3f_1^{-1} &= f_3f_1 &= & r_2 \\ f_2r_1f_2^{-1} &= f_1f_2^{-1} &= f_1f_2 &= & r_2 \\ f_3r_1f_3^{-1} &= f_2f_3^{-1} &= f_2f_3 &= & r_2 \end{aligned}$$

(c) r_2:

$$\begin{aligned} r_1r_2r_1^{-1} &= r_1^{-1} = & r_2 \\ r_2r_2r_2^{-1} &= r_1r_1 = & r_2 \\ f_1r_2f_1^{-1} &= f_2f_1 = & r_1 \\ f_2r_2f_2^{-1} &= f_3f_2 = & r_2 \\ f_3r_2f_3^{-1} &= f_1f_3 = & r_1 \end{aligned}$$

(d) f_1:

$$\begin{aligned} r_1f_1r_1^{-1} &= f_2r_2 = & f_3 \\ r_2f_1r_2^{-1} &= f_3r_1 = & f_2 \\ f_1f_1f_1^{-1} &= & f_1 \\ f_2f_1f_2^{-1} &= r_1f_2 = & f_3 \\ f_3f_1f_3^{-1} &= r_2f_3 = & f_2 \end{aligned}$$

(e) f_2:

$$\begin{aligned} r_1f_2r_1^{-1} &= r_1f_3 = & f_1 \\ r_2f_2r_2^{-1} &= r_2f_1 = & f_3 \\ f_1f_2f_1^{-1} &= f_1r_1 = & f_3 \\ f_2f_2f_2^{-1} &= & f_2 \\ f_3f_2f_3^{-1} &= r_2f_3 = & f_2 \end{aligned}$$

(f) f_3:

$$\begin{aligned} r_1f_3r_1^{-1} &= r_1f_1 = & f_2 \\ r_2f_3r_2^{-1} &= r_2f_2 = & f_1 \\ f_1f_3f_1^{-1} &= f_1r_2 = & f_2 \\ f_2f_3f_2^{-1} &= f_2r_1 = & f_1 \\ f_3f_3f_3^{-1} &= & f_3 \end{aligned}$$

So there are three conjugacy classes: $\boxed{\{e\}, \{r_1, r_2\}, \{f_1, f_2, f_3\}}$.

6.16b

Give two examples of non-abelian groups with 2^3 elements.[1] (Hint. There are only two such groups, up to isomorphism, and both have been used as examples in class before.)

From Example 2.23, the Quaternion Group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is a non-commutative group with 8 elements. Additionally, for $n \geq 2$, the dihedral group D_n is a non-commutative group with $2n$ elements. Thus, D_4 is a non-abelian group with 8 elements. $\blacksquare$

[1] In the book there is a proof that all groups of order p^2 for prime p are abelian. This shows the proof cannot be extended to groups of order p^3.

6.21

Let p be prime, and let G be a group of order p^n. Prove that for every $0 \leq r \leq n$, there is a subgroup H of G of order p^r. (Hint. Give a proof by induction on n. Use Theorem 6.25, which says that G has a non-trivial center $Z(G)$, and apply the induction hypothesis to G/N, where N is an appropriately chosen subgroup of $Z(G)$).

We proceed by induction on n. For $n = 0$, $G = \{e\}$ and $H = \{e\}$ is a subgroup of order p^0.

Let G be the smallest group whose order is a multiple of p (say $\#G = p^n$) for which we do not know that there is a subgroup of order p^4 for all $0 \leq r \leq n$.

By Theorem 6.25, G has a non-trivial center $Z(G)$.

Since $Z(G)$ is a subgroup of G, it has order p^r for some $0 < r \leq n$. Then by Abelian Cauchy, there is a subgroup $N \subset Z(G)$ of order p. Since $Z(G)$ is the group of elements of G that commute with every other element of G,

$$gNg^{-1} = \{ghg^{-1} : h \in N\} = \{hgg^{-1} : h \in N\} = N$$

for all $g \in G$. Thus N is normal in G. Further, by Corollary 6.26,

$$\#(G/N) = \#G/\#N = p^n/p = p^{n-1}$$

Now we consider the natural homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$. This is a p-to-1 map. If we let $H = \pi^{-1}(G/N) \subset G$ we thus get a subgroup of order p^{n-1} in G.

By the induction hypothesis, this is a group of order less than p^n so it has subgroups of order p^r for all $0 \leq r \leq n-1$. For the last equality, $G \subseteq G$ trivially so for all $0 \leq r \leq n$, there is a subgroup H of G of order p^r. $\blacksquare$

6.23

In Example 6.36 the book shows that there are exactly two groups of order 10. Do a similar calculation to find all groups of order 15.

If $\#G = 15$, Sylow 1 gives us that there are 3-Sylow and 5-Sylow subgroups of G.

Sylow 3 tells us that the number of distinct p-Sylow subgroups (n) of G is congruent to 1 mod p and divides k.

We will start with the 3-Sylow subgroups. Then $15 = 3^1 \cdot 5$ so $n \mid 5$ and $n \equiv 1 \bmod 3$. Thus, $n = 1$. So there is only one 3-Sylow subgroup of G. We will call it H_3.

Similarly, for the 5-Sylow Subgroups $15 = 5^1 \cdot 3 \implies (n \mid 3) \wedge (n \equiv 1 \bmod 5)$. Thus, $n = 1$. So there is only one 5-Sylow subgroup of G. Call it H_5.

By Proposition 2.51, all groups of prime order are cyclic. Thus, the 3-Sylow subgroup is cyclic and the 5-Sylow subgroup is cyclic. Further, by Remark 6.33, $H_3 \cap H_5 = \{e\}$ so

$$H_3 = \{e, a, a^2\}, \qquad H_5 = \{e, b, b^2, b^3, b^4\}$$

When do a and b commute?

$$aba^{-1} \in aH_5a^{-1} = H_5 \implies aba^{-1} = b^j \quad 0 \leq j \leq 4$$

by normality of H_5. What is the value of j?

As in Example 6.36,

$$b = a^{-1}b^j a = (a^{-1}ba)^j = (a^{-1}(a^{-1}b^j a)a)^j = a^{-2}b^{j^2}a^2 = a^{-2}(a^{-1}b^j a)^{j^2}a^2 = a^{-3}b^{j^3}a^3 = b^{j^3}$$

So $b^{j^3-1} = e$ and

$$j^3 \equiv 1 \bmod 5 \implies j = 1$$

This tells us that $aba^{-1} = b \implies ab = ba$ so G is abelian. Does ab have order 15?

$$e = (ab)^k = a^k b^k \implies a^k = b^{-k} \in H_3 \cap H_5 \implies a^k = b^k = e \implies 3 \mid k \text{ and } 5 \mid k \implies 15 \mid k$$

So G is a cyclic group of order 15 and all groups of order 15 are isomorphic to $\mathcal{C}_{15}$.

■

6.25

Let G be a finite group of order $\#G = pq$, where p and q are primes satisfying $p > q$. Assume further that $p \not\equiv 1(\mod q)$

(a) Prove that G is an abelian group. (Hint. Example 6.37 provides a starting point for the proof.)

Let n_p be the number of p-Sylow subgroups and n_q the number of q-Sylow subgroups.

By Sylow 3, $n_q \equiv 1 \mod q$ and $n_q \mid p$. Since p is prime, $n_q \in \{1, p\}$ but $p \not\equiv 1 \mod q$ so $n_q = 1$. Thus, there is only one q-Sylow subgroup of G and it is normal. Further, since $p > q$, q is the largest power of itself which divides $\#G$ so the order of the q-Sylow subgroup is q.

Now look at the p-subgroups. Let H be one of them. By Example 6.37, H is normal. Let H' be another p-Sylow subgroup. Then by Sylow 2,

$$H = aH'a^{-1} \quad a \in G$$

but since H is normal,

$$H = aHa^{-1}$$

so

$$aHa^{-1} = aH'a^{-1} \implies H = H'$$

so there is only one p-Sylow subgroup.

Call the p-Sylow subgroup A and the q-Sylow subgroup B. Then consider the set of products $AB = \{ab : a \in A, b \in B\}$. Since p and q are distinct, $A \cap B = \{e\}$. By Lemma 6.39,

$$\#(AB) = \frac{\#A \cdot \#B}{\#(A \cap B)} = \frac{p \cdot q}{1} = pq = \#G \implies G = AB$$

and further, we have a well-defined bijection $\frac{A \times B}{A \cap B} \to AB$.

Thus,

$$G = \{a^i b^j : 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$$

To show that two elements of G commute, then, it is sufficient to show that elements of A and B commute. Consider the product $hgh^{-1}g^{-1}$ with $h \in A$ and $g \in B$.

Since B is normal, $hgh^{-1} \in A$ so $(hgh^{-1})g^{-1} \in A$. But since A is also normal, $gh^{-1}g^{-1} \in A \implies h(gh^{-1}g^{-1}) \in A$. Thus, $hgh^{-1}g^{-1} \in A \cap B$. But $A \cap B = \{e\}$ so $hgh^{-1}g^{-1} = e \implies hg = gh$. Thus, G is abelian. $\blacksquare$

(b) Prove that G is a cyclic group.

Let $A = \langle a \rangle$ be the p-Sylow subgroup and $B = \langle b \rangle$ be the q-Sylow subgroup as above. By Example 6.36, to show that G is cyclic, we just need to show that it is abelian and that ab has order pq.

We have already shown that G is abelian so all the remains is to show that ab has order pq:

$$\begin{aligned} e = (ab)^k &= a^k b^k \\ &\implies a^k = b^{-k} \in A \cap B = \{e\} \\ &\implies a^k = b^k = e \\ &\implies p \mid k \text{ and } q \mid k \\ &\implies pq \mid k \end{aligned}$$

Thus the smallest number for which $(ab)^k = e$ is pq so the order of ab is pq and G is cyclic. $\blacksquare$

6.28

Let G be a group of order $\#G = 75$.

(a) Prove that G has a subgroup H with all three of the following properties:

- H has order $\#H = 25$.

  $25 = 5^2$ and $5 \mid 75$ but $5^3 \not| 75$ so by Sylow 1, G has at least one 5-Sylow subgroup H of order 25. $\blacksquare$

- H is a normal subgroup of G.

  By Sylow 3, the number of distinct 5-Sylow subgroups of G is congruent to 1 mod 5 and divides 3. The divisors of 3 are $\{1, 3\}$. Of these, only $1 \equiv 1 \bmod 5$ so H is the only 5-Sylow subgroup of G.

  Let S be the set of Sylow p-subgroups. By Sylow 2, G acts on S by conjugation: $g \cdot H = gHg^{-1}$. In class we showed that

  $$\frac{\#G}{\#S_H} = \#S$$

  Since H is the only 5-Sylow subgroup of G, $\#S = 1$. Thus,

  $$S_H = \{a \in G \mid aHa^{-1} = H\} = G$$

  so H is normal. $\blacksquare$

- H is abelian.

  H is a group with $25 = 5^2$ elements so by Corollary 6.26, H is abelian. $\blacksquare$

(b) Suppose that the subgroup H in (a.) is cyclic of order 25. Prove that G is abelian.

We know from above that H is a unique 5-Sylow subgroup of G.

Now consider the 3-Sylow subgroups:

$$n \mid 25, \quad n \equiv 1 \bmod 3 \implies n = 1$$

so there is a unique 3-Sylow subgroup of order 3 in G.

Let K be the 3-Sylow subgroup. Then $H \cap K = \{e\}$ and by Lemma 6.39,

$$\#(HK) = \frac{\#H \cdot \#K}{\#(H \cap K)} = \#H \cdot \#K = 25 \cdot 3 = 75$$

Though HK is not generally a subgroup of G, it is a subset since H and K are cyclic subgroups of G so all their elements are elements of G and thus by closure, the set of products is in G. This further tells us that since $HK \subseteq G$ and $\#HK = \#G$ (and G is finite), $HK = G$, i.e.,

$$G = \{h^i k^j : h^i \in H, k^j \in K\}$$

To show that G is abelian, it is sufficient to show that H and K commute. Consider the product $hkh^{-1}k^{-1}$ with $h \in H$ and $k \in K$.

Since both H and K are normal,

$$\underbrace{(hkh^{-1})}_{\in K} k^{-1} = h \underbrace{(kh^{-1}k^{-1})}_{\in H} \implies hkh^{-1}k^{-1} \in H \cap K = \{e\}$$

so

$$hkh^{-1}k^{-1} = e \implies hk = kh$$

so G is abelian. ∎