Math 110B Final Practice

Sava Spasojevic

March 18, 2019

3) (i) Prove that a group G of order p^n for p a prime has a non-trivial center (i.e. the center $Z(G)$ of G has order > 1).

Proof. Let G be a p-group with p prime. Let G act on itself by conjugation, i.e. $\varphi : G \to S_{|G|}$ with $g \mapsto c_g$, where $c_g(k) = gkg^{-1}$. We know that $\{Orb_G(x)\}$ defines a partition of $X = G$. So

$$\sum_{\text{representatives}} |Orb_G(x)| = |G| \equiv 0 \mod p$$

But, $|Orb_G(x)||G|$ which implies that $|Orb_G(x)| \equiv 0 \mod p$ or 1. So

$$\sum |Orb_G(x)| = \sum 1 = |Z(G)| \equiv 0 \mod p$$

But, $|Z(G)| \neq 0$, which means that $|Z(G)|$ has to be divisible by p. Thus, the center is nontrivial. □

(ii) Prove that a group of order p^2 is abelian.

Proof. Let G be a group of order p^2. Then by the theorem above, $|Z(G)| = p^2$ or p. If $|Z(G)| = p^2$ then $Z(G) = G$ and we're done. If $|Z(G)| = p$, $|G/Z(G)| = p$ so it is cyclic. This means $\langle gZ(G)\rangle = G/Z(G)$, for some $g \in G$. Let $q \in G$. Then, for some $m \in \mathbb{Z}$

$$\begin{aligned} qZ(G) &= g^m Z(G) \\ qg^{-m} &= z \in Z(G) \\ q &= g^m z \end{aligned}$$

This shows that any arbitrary element in G can be written as the product of some power of g and some element in the center. So for $a, b \in G$, $z, z' \in Z(G)$, $m, n \in \mathbb{Z}$,

$$\begin{aligned} ab &= g^m z g^n z' \\ &= g^m g^n z z' \\ &= g^n g^m z z' \\ &= g^n z' g^m z \\ &= ba \end{aligned}$$

Thus, G is abelian. □

5) If $\sigma, \tau \in G$ have orders that are distinct primes p, q, and if $\sigma\tau = \tau\sigma$ then the order of $\sigma\tau$ is pq. Show that this need not be true if σ, τ do not commute

Proof. Since $\sigma\tau = \tau\sigma$ we have that $(\sigma\tau)^{pq} = \sigma^{pq}\tau^{pq} = (\sigma^p)^q(\tau^q)^p = e^q e^p = ee = e$. Let $o(\sigma\tau) = k$. We know that $k|pq$. This means $k = 1, p, q$, or pq. If $k = 1$ then $\sigma\tau = e$ which is not true since neither σ nor τ are the identity. If $k = p$ then $(\sigma\tau)^p = \sigma^p\tau^p = \tau^p = e$. This is not true since $o(\tau) = q \neq p$ and q does not divide p. Similar case when $k = p$. So $k = pq$. Consider $\sigma, \tau \in S_3$. We know that $\sigma\tau \neq \tau\sigma$ and $o(\sigma\tau) \neq o(\sigma)o(\tau)$ □

6) (i) For a prime p classify all abelian groups of order p^3.

Proof. We consider three cases.

case I: $\exists g \in G : o(g) = p^3$. Then $G \cong \mathbb{Z}_{p^3}$.

case II: $\exists g \in G : o(g) = p^2$. Consider $\langle g\rangle$. Take $h \notin \langle g\rangle$. Then we have $G/\langle g\rangle \cong \mathbb{Z}_p = \langle h\langle g\rangle\rangle$. So $G \cong \langle g\rangle \times \langle h\rangle \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p$.

case III: $\exists g \in G : o(g) = p$. Then $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. □

(ii) give an example of a nonabelian group of order p^3

D_4 is nonabelian. $|D_4| = 8 = 2^3$.

7) Given a positive integer n, and an integer k prime to the Euler function $\phi(n) = |\mathbb{Z}_n^*|$ show that every element $a \in \mathbb{Z}_n^*$ can be written as $a = b^k$ for a unique $b \in \mathbb{Z}_n^*$. Further show that $b = a^l$ for an integer l such that kl is $1 \mod \phi(n)$.

Proof. Let $a \in \mathbb{Z}_n^*$. We know that the order of a divides that order of the group, i.e. $o(a)|\phi(n)$. Suppose $o(a) = s$. Then the above statement becomes $st = \phi(n)$ for some $t \in \mathbb{Z}$ with $a^s = e$. We know that since k is prime to the Euler function $\phi(n)$, we have that $mk + \phi(n)l = 1$ for some $k, l \in \mathbb{Z}$. So,

$$a = a^1 = a^{mk+\phi(n)l} = a^{mk}a^{\phi(n)l} = a^{mk}a^{stl} = (a^m)^k(a^s)^{tl} = (a^m)^k e^{tl} = (a^m)^k$$

Take $b = a^m \in \mathbb{Z}_n^*$ since this group is closed under multiplication. This element is clearly unique. Thus, $a = b^k$.

To show the second statement, we suppose that $kl \equiv 1 \mod \phi(n)$. That is, $kl + \phi(n)m = 1$ for some $m \in \mathbb{Z}$. Suppose $o(b) = w$. Then $w|\phi(n)$, i.e. $wr = \phi(n)$ for some $r \in \mathbb{Z}$. We have,

$$b = b^1 = b^{kl+\phi(n)m} = b^{kl}b^{\phi(n)m} = b^{kl}b^{wrm} = (b^k)^l(b^w)^{rm} = a^l e^{rm} = a^l$$

Thus, $b = a^l$. □

9) Prove that if N_1, N_2 are normal subgroups of G which intersect trivially, then N_1N_2 is isomorphic to $N_1 \times N_2$.

Proof. Let $N_1, N_2 \trianglelefteq G$ with $N_1 \cap N_2 = \{e\}$. Consider the map

$$\begin{aligned} \varphi : N_1 \times N_2 &\to N_1N_2 \\ (n_1, n_2) &\mapsto n_1n_2 \end{aligned}$$

We first show it is a homomorphism. Let $n_1' \in N_1$ and $n_2 \in N_2$. Since N_1 is normal, $n_2n_1'n_2^{-1} \in N_1$.Since $n_1'^{-1} \in N_1$, $n_1'^{-1}n_2n_1'n_2^{-1} \in N_1$. Since N_2 is normal $n_1'^{-1}n_2n_1' \in N_2$. Since $n_2^{-1} \in N_2$, we have $n_1'^{-1}n_2n_1'n_2^{-1} \in N_2$. Thus, $n_1'^{-1}n_2n_1'n_2^{-1} = e$. So, for $(n_1, n_2), (n_1', n_2') \in N_1 \times N_2$, we have

$$\begin{aligned} \varphi((n_1, n_2)(n_1', n_2')) &= \varphi((n_1n_1', n_2n_2')) \\ &= n_1n_1'n_2n_2' \\ &= n_1n_1'en_2n_2' \\ &= n_1n_1'n_1'^{-1}n_2n_1'n_2^{-1}n_2n_2' \\ &= n_1n_2n_1'n_2' \\ &= \varphi((n_1, n_2))\varphi((n_1', n_2')) \end{aligned}$$

So, this map is a homomorphism. It is clearly bijective, thus it is an isomorphism. □

10) Show that if a group G acts on a set X, and if $x = gy$ for $g \in G$, $x, y \in X$, then $Stab_G(y) = gStab_G(x)g^{-1}$. Using this, show for a subgroup H of G that the kernel of the homomorphism $\pi : G \to A(G/H)$ given by $\pi(g)(xH) = gxH$ is H if and only if H is normal in G.

Proof. Let $g \in Stab_G(y)$. Then, $y = gy = x$. We have that $gxg^{-1} = gyg^{-1} = xg^{-1}$. Multiplying by g on the right gives $gx = x$, which means $g \in gStab_G(x)g^{-1}$. So $Stab_G(y) \subseteq gStab_G(x)g^{-1}$. Let $h \in gStab_G(x)g^{-1}$. We need to show $g^{-1}hg \in Stab_G(y)$. $g^{-1}hgy = g^{-1}hx = g^{-1}x = y$. □

11) Using Sylow theorems or otherwise, prove that there is no simple group of order 56.

Proof. Let G be a group such that $|G| = 56$. We need to show that $\exists N \trianglelefteq G$ such that $N \neq e, G$, i.e. there is a nontrivial normal subgroup. Note that $56 = 2^3 \cdot 7$. Let P be a Sylow 7-subgroup. The Third Sylow Theorem says the $n_7 \equiv 1 \mod 7$ and $n_7|8$. Therefore, $n_7 = 1$ or $n_7 = 8$. Suppose that $n_7 = 1$. Then P is normal and we are done.

Suppose now that $n_7 = 8$. This means there are 8 Sylow 7-subgroups. We begin by listing them $P = P_1, P_2, \ldots, P_8$. Consider the intersection of these groups $P_i \cap P_j$ $(1 \leq i \leq j \leq 8)$. Notice that $P_i \cap P_j = \{e\}$ and

$P_i \cap P_j \leq P_i$ and $P_i \cap P_j \leq P_j$ as P_i and P_j are distinct and of prime order. Consider $\bigcup_{i=1}^{8} P_i$. These are all elements of G of order dividing 7. So,

$$\left|\bigcup_{i=1}^{8} P_i\right| = 7+7+7+7+7+7+7+7-7 = 49$$
$$\left|G\Big/\bigcup_{i=1}^{8} P_i\right| = 56-49 = 7$$

There is a sylow 8-subgroup, call it Q. Notice that $Q/\{e\} \subseteq G/\bigcup_{i=1}^{8} P_i$ and $Q = (G/\bigcup_{i=1}^{8} P_i) \cup \{e\}$. This applies to any Sylow 8-subgroup and thus there is a unique Sylow 8-subgroup. Therefore G is not simple. □

12) Using groups acting on sets (for eg H acting on a set of cosets K in G), or otherwise prove that if H, K are subgroupds of a finite group G, and $HK = \{hk : h \in H, k \in K\}$, then

$$|HK| = |H||K|/|H \cap K|$$

Proof. Let H act on HK/K where $h \times h_1k \mapsto hh_1k$. We have the following

$$Orb(eK) = \{hK : h \in H\} = HK/K$$
$$Stab(eK) = \{h \in K\} = H \cap K$$

By orbit-stabilizer theorem $|HK|/|K| = |H|/|H \cap K|$. □

14) Given an n-cycle $\sigma \in S_n$, and a postive integer r, show that σ^r is conjugate to σ in S_n if and only if r is prime to n.

Proof. Let $\sigma \in S_n$ and $r \in \mathbb{Z}^+$. Suppose that $o(\sigma) = k$.

$$\begin{aligned} e = \sigma^k = g^k(\sigma^r)^k g^{-k} &\implies g^{-k}g^k = (\sigma^r)^k \\ &\implies e = (\sigma^r)^k \\ &\implies o(\sigma^r)|o(\sigma) = k \end{aligned}$$

Now, suppose that $o(\sigma^r) = j$.

$$\begin{aligned} e = (\sigma^r)^j = g^j\sigma^j g^{-j} &\implies g^{-j}g^j = \sigma^j \\ &\implies e = \sigma^j \\ &\implies o(\sigma)|o(\sigma^r) = j \end{aligned}$$

This gives the equality $o(\sigma) = o(\sigma^r)$. Recall that if G is a group and $a \in G$, $o(a^k) = \frac{o(a)}{(k,o(a))}$ □

So we have that

$$o(\sigma^r) = \frac{o(\sigma)}{(r, o(\sigma))}$$

But, $o(\sigma) = n$ since its an n-cycle, which means $(r, n) = 1$.