Selected Solutions to Homework 2, Math 4107

Ernie Croot

February 6, 2008

Page 35.

11. I know several ways to prove this. Here is one way:

Partition G into a union of disjoint sets of the type $\{a, a^{-1}\}$. In the case $a = e$, the identity element, we will have that $a^{-1} = e$; and so, the set $\{a, a^{-1}\}$ will consist only of $\{e\}$ in that case. In general, such a set will contain only one element if $a = a^{-1}$; that is, $a^2 = e$. Now, if $\{e\}$ is the only set where $\{a, a^{-1}\}$ contains only one element, then we would have that

$$|G| \ = \ |\{e\}| + |\{a_1, a_1^{-1}\}| + \cdots + |\{a_k, a_k^{-1}\}| \ = \ 1 + 2k,$$

which would contradict the fact that $|G|$ is even. So, there must be at least one other set besides $\{e\}$ having only one element; and therefore, there is an element $a \neq e$ satisfying $a^2 = e$.

Page 47.

6.

a. We have that $G = \{e, a, a^2, ..., a^9\}$, and $H = \{e, a^2, a^4, a^6, a^8\}$. The cosets of H are H and aH; and note,

$$H \cup aH \ = \ \{e, a^2, a^4, a^6, a^8\} \cup \{a, a^3, a^5, a^7, a^9\} \ = \ G.$$

b. If $H = \{e, a^5\}$, then the cosets of H are H, aH, a^2H, a^3H and a^4H.

c. (Recall Herstein's funny notation $A(S)$ for the symmetric group on the set S.) Here, H is the set of all permutations that fix the element x_1. There are two such permutations:

$$\sigma_1 \ = \ e \ = \ \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \text{ and } \sigma_2 \ = \ \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}.$$

Since $A(S)$ has $6 = 3!$ elements, we must have that there are three cosets of H. These cosets are

$$H,\ \alpha H,\ \text{and}\ \beta H,$$

where

$$\alpha \ = \ \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix},$$

and where

$$\beta \ = \ \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}.$$

15. To prove that $Z < G$, first suppose $a \in Z$. Then, $a^{-1} \in Z$, because if $ag = ga$, for all $g \in G$, multiplying by a^{-1} on the right and left, we get $ga^{-1} = a^{-1}g$ for all $g \in G$. Also, if $a, b \in Z$, then $abg = agb = gab$ for all $g \in G$, meaning that $ab \in Z$. Thus, $Z < G$.

The center of G is a normalizer for some subgroup $H < G$ if and only if G is abelian. First, if G abelian, then $Z = G = C(\{e\})$. Now suppose that $Z = C(H)$, for some $H < G$. Then, since $H < C(H)$, we would have $H < Z$. But this would give us that $H \triangleleft G$, since $a^{-1}Ha = H$ (because H being in the center of the group, commutes with everything). But $H \triangleleft G$ implies $C(H) = G$. So, $Z = C(H)$ implies $Z = G$, and therefore G is abelian.

19. I am not sure why this is a starred problem, as it is easier than problem 15, which was not starred: If H has finite index in G, then there is a finite number of left cosets $a_1H, ..., a_kH$ and a finite number of right cosets $Hb_1, ..., Hb_k$ of H. So, each conjugate

$$a^{-1}Ha \ = \ (a_iH)a \ = \ a_i(Ha) \ = \ a_i(Hb_j) \ = \ a_iHb_j$$

for some $i, j \leq k$. So, the conjugates of H lie in the finite set of subsets of G of the form

$$\{a_iHb_j \ : \ i, j = 1, ..., k\};$$

and therefore, there can be at most k^2 conjugates of H.

38. Let (a) be the largest cycle in G, and suppose that it has order n. We will show that $G = (a)$: First, note that every $x \in (a)$ satisfies $x^n = e$. So, by the hypothesis of the problem, all the elements of G such that $x^n = e$ belong to (a).

Now suppose that $(a) \neq G$. Then, there exists some $b \in G$ such that $b \notin (a)$; and therefore, $b^n \neq e$. We will presently show that there exist integers m, m' such that the element $y = a^m b^{m'}$ has order equal to $\text{lcm}(\text{order}(a), \text{order}(b)) > \text{order}(a)$. Thus, (a) was not the largest cycle in G, as (y) is even larger. This gives a contradiction, and we conclude that $G = (a)$.

To see how to pick m, m' for our element y, we begin with the following basic fact:

Claim. If the order of a is n, and the order of b is n', and if $\gcd(n, n') = 1$, then the order of ab is nn'.

Proof of the Claim. Let t be the order of ab. Since $(ab)^t = e$ we conclude $a^t = b^{-t}$. Thus, a^t belongs to the cycle (a) and to the cycle (b). Now suppose that $c \in (a) \cap (b)$. Then, $c^n = e$ and $c^{n'} = e$; so, upon writing the $\gcd(n, n') = 1$ as a linear combination, we see that $e = c^{\gcd(n,n')} = c$. So, $(a) \cap (b) = \{e\}$, and we conclude that $a^t = e$. Thus, $n|t$. A similar calculation shows that $n'|t$, and then since $(n, n') = 1$ we conclude $nn'|t$. To show $t = nn'$ one just observes that $(ab)^{nn'} = a^{nn'} b^{nn'} = e$.

It is a fairly simple exercise to now show that there exist integers m, m' such that $\text{order}(a)/m$ and $\text{order}(b)/m'$ are coprime, and

$$\text{lcm}(\text{order}(a), \text{order}(b)) \;=\; \text{lcm}\left(\frac{\text{order}(a)}{m},\; \frac{\text{order}(b)}{m'}\right).$$

If so, then $\text{order}(a^m)$ is coprime to $\text{order}(b^{m'})$, and we may apply the above claim to finish the proof of the theorem.

Page 53.

1. If $aHbH = cH$ for all $a, b \in G$, then consider what happens when $b = a^{-1}$. We have that $aHa^{-1}H = cH$ for some c. In fact, $c = e$ since $aHa^{-1}H$ contains e, and the only left-coset cH of H containing e is the trivial coset H iteself. Thus, $aHa^{-1}H = H$. This obviously means that $a^{-1}Ha = H$, and therefore $H \triangleleft G$.

12. In the finite version of this problem, we have that since $M \cap N = \{e\}$, from the fact that $|MN| = |M||N|/|M \cap N| = |M||N|$, we deduce that all the products mn, $m \in M$ and $n \in N$, must be distinct.

Now, since $N \triangleleft G$, we deduce that $mN = Nm$, and therefore $mn = n'm$, for some $n' \in N$. We will show that $n' = n$. To do this, we also use the normality of M, which tells us that $n'M = Mn'$, and therefore $n'm = m'n'$, for some $m' \in M$. So, we have $mn = n'm = m'n'$, and then using the fact that every element of MN has a unique representation as mn, $m \in M$ and $n \in N$, we conclude that $m' = m$ and $n' = n$. Therefore, $mn = n'm = nm$, and we are done.

Page 65.

8.

a. Since G has $2n$ elements, and since N has n elements, since we know all index-2 subgroups of a group are normal, to show $N \triangleleft G$ it suffices to show $N < G$: We will prove N is a subgroup using the 1-step subgroup test, which amounts to checking that if $a, b \in N$, then $ab^{-1} \in N$. In our case if $a, b \in N$, then $a = y^i$ and $b = y^j$ for some $0 \leq i, j \leq n-1$. So, $b^{-1} = y^{n-j}$. Therefore, $ab^{-1} = y^{i+n-j} = y^m$, where $0 \leq m \leq n-1$ and $m \equiv i + n - j \equiv i - j \pmod{n}$. Thus, $ab^{-1} \in N$, and we are done.

b. Since $N \triangleleft G$ we may form the quotient group G/N, which has $|G|/|N| = 2$ elements. Since there is only one isomorphism class of groups of order 2, namely the cyclic group $\{1, -1\}$ (under multiplication) or $\mathbb{Z}_2$ (under addition), we conlude that $G/N \cong \{1, -1\}$ (multiplication).