Selected Solutions to Math 4107, Set 4

November 9, 2005

Page 90.

1. There are 3 different classes: $\{e\}, \{(1\,2),\ (1\,3), (2\,3)\}, \{(1\,2\,3),\ (1\,3\,2)\}$. We have that $c_e = 1$, $c_{(1\ 2)} = 3$, and $c_{(1\ 2\ 3)} = 2$. And, note that

$$|S_3| \ = \ 6 \ = \ 1 + 3 + 2.$$

4. One way that we can define the Dihedral group is through the symbols R, which means rotate clockwise by $2\pi/n$, and F, which means flip about a specific vertex. We have that $R^n = F^2 = e$, and $FR = R^{-1}F$. This uniquely determines the properties of D_n, and we have that it contains the $2n$ distinct elements $e, R, R^2, ..., R^{n-1}, F, FR, FR^2, ..., FR^{n-1}$.

Now, if r is one of the pure rotations $e, ..., R^{n-1}$, and α is also a pure rotation, then $\alpha^{-1}r\alpha = r$. On the other hand, if $\alpha = FR^j$, then

$$\alpha^{-1}r\alpha \ = \ (R^{-j}F)r(FR^j) \ = \ FR^jrR^{-j}F \ = \ FrF \ = \ r^{-1}.$$

So, the set of conjugates of r are $\{r, r^{-1}\}$.

Now we consider the conjugates of FR^j. If R^i is any pure rotation, then $R^{-i}FR^jR^i = FR^{2i+j}$. Thus, the conjugates of FR^j can be described as $\{FR^k : k \equiv j \pmod 2\}$.

In the case where n is even we have that the conjugates of elements of the form FR^j break down into two classes, those of the form $\{FR^k \ : \ k \text{ even}\}$, and those of the form $\{FR^k \ : \ k \text{ odd}\}$. Also, the conjuages of a pure rotation r take the form $\{r, r^{-1}\}$. There is only one case where this set contains only one element, and that is when r is a rotation by 180 degrees. So, in the case

n even we will have that the class sizes $c_a = 1$ only if a is the identity or rotation by 180 degrees; $c_a = 2$ if a is any other pure rotation; and, there are two classes where $c_a = n/2$. In total we will have that

$$\sum c_a \;=\; 1 + 1 + \frac{n-2}{2} \times |c_R| + |c_{FR}| + |c_{FR^2}| \;=\; n + n/2 + n/2 \;=\; 2n.$$

In the case n odd all the sets $\{r, r^{-1}\}$ have two elements, and there is only one equivalence class for FR. So, in this case we have $c_{R^j} = 2$, $c_{FR} = n$. So,

$$\sum c_a \;=\; 1 + \frac{n-1}{2}|c_R| + |c_{FR}| \;=\; 1 + (n-1) + n \;=\; 2n.$$

5.

a. For every r cycle in S_n, there are r different ways that it can be written in the form $(x_1 \; x_2 \; \cdots \; x_r)$; for example, the 3-cycle $(1\ 2\ 3)$ could also be written as (2 3 1) or (3 1 2). Now, the number of ways of writing the cycle is the number of sequences of r numbers chosen from among $1, ..., n$, and there are $n(n-1)\cdots(n-r+1) = n!/(n-r)!$ such sequences. In total, then, there are $n!/(r(n-r)!)$ r-cycles in S_n.

b. The set of conjugates of an element $\alpha \in S_n$ is the set of all elements having the same cycle structure as α. So, the conjuages of a cycle $(x_1 \; \cdots \; x_r)$ is the set of all r-cycles. So, there are $n!/(r(n-r)!)$ conjugates of $(1 \; \cdots \; r)$.

c. σ commutes with the cycle $c = (1\ 2 \; \cdots \; r)$ if and only if

$$\sigma c \sigma^{-1} \;=\; (\sigma(1)\ \sigma(2) \; \cdots \; \sigma(r)) \;=\; (1\ 2 \; \cdots \; r).$$

Now, these last two cycles are equal if and only if for some $j = 0, ..., r-1$ we have

$$\sigma(i) \;\equiv\; i + j \pmod{r}, \quad \text{for } i = 1, ..., r.$$

Thus, σ fixes $r+1, ..., n$, and acts as $(1 \; \cdots \; r)^j$ on $\{1, ..., r\}$. It follows that

$$\sigma \;=\; (1\ 2 \; \cdots \; r)^j \tau,$$

where τ fixes $r+1, ..., n$.

Page 101.

7.

a. The number of 3-Sylow subgroups divides 30 and is congruent to $1 \pmod 3$. So, this number is 1 or 10. Similarly, the number of 5-Sylow subgroups divides 30 and is $1 \pmod 5$, giving us 1 or 6 of them. We cannot have that there are both 10 Sylow-3 subgroups, and 6 Sylow-5 subgroups, because from the Sylow-3 subgroups we would get 20 elements of order 3, and from the Sylow-5 subgroups we would get 24 elements of order 5. In total, we would have $20 + 24 = 44$ elements, which exceeds 30.

We conclude that either there is only one Sylow-3, or there is only one Sylow-5. Since all Sylow-3's are conjugate to each other, and since all Sylow-5's are conjugate to each other, we will have that either the Sylow-3 is normal or the Sylow-5 is normal.

b. Say that the 3-Sylow in part a is normal, and write it as P. Consider then the map $\varphi : G \to G/P$. We have that $|G/P| = 10$, and it is easy to see that there can be only one Sylow-5 in that group, for the number of sylow-5's must be $1 \pmod 5$ and divide 10. Now, each sylow-5 back in G must map to a Sylow-5 in G/P, because if $a \in G$ has order 5, then $\varphi(a)$ has order 5 in G/P (since, $\varphi(a)^5 = \varphi(a^5) = \varphi(1) = 1$, we either have a is in the kernel, or else a has order 5. If a is in the kernel, it must have belonged to P, but we know that P intersects the Sylow-5's only at the identity.) So, if there were six Sylow-5's in G, then they must all map down to a single Sylow-5 in G/P. This cannot happen, though, because it would mean that φ is at best a six-to-1 map, but it is a 3-to-1 map. So, the Sylow-5 must be normal.

Similarly, if the Sylow-5 was the one that was normal in part a, then we can't have that there are 10 Sylow-3's: If Q is that Sylow-5, then $\psi : G \to G/Q$ is 5-to-1, and yet since $|G/Q| = 6$ has at most one Sylow-3, if there were 10 Sylow-3's in G, then ψ would have to be 10 to 1.

c. From part b, if P is our Sylow-3 and Q is our Sylow-5, both of which are normal, then G contains PQ, which has order 15. Since PQ has index $|G|/15 = 2$, it must be normal. (Because G has only two left-cosets of PQ, namely PQ, aPQ, and only two right cosets PQ, PQa. Both aPQ and PQa are the elements of G not contained in PQ, and so $aPQ = PQa$, and left cosets equal right cosets, which gives us that PQ is normal.)

d. As we know, all groups of order 15 are ableian and cyclic. So, half of G is this large cyclic group of order 15. Now, suppose that $x \in G$ has order 2. Such x exist, since G must have a 2-Sylow subgroup. Let $C = PQ$. Then, $G = C \cup (xC)$ (Note that xC is disjoint from C, because xC contains

x, which has order 2, while every element of C has order dividing 15).

How can we multiply elements in G? To answer that question, we begin by observing that since C is normal, $xCx = x^{-1}Cx = C$. So, conjugation by x is an automorphism of C. All automorphisms of a cyclic group take the form $\theta(c) = c^j$, where j is coprime to the order of G. Therefore, we must have that there exists j such that $xc = c^j x$ for all $c \in C$; moreover, j can only be one of $1, 2, 4, 7, 8, 11, 13, 14$. We can further reduce the list of possible j by observing that $xcx = c^j$ implies $c = xc^jx = (xcx)^j = c^{j^2}$ So, $c^{j^2-1} = e$, which imlies $j^2 - 1 \equiv 0 \pmod{15}$. This means that j can only be $1, 4, 11, 14$. Once we have settled on a value for j we have completely pinned down how we multiply in our group: An arbitrary $g \in G$ has the form xc or c, where $c \in C$. And, if $g_1 = xc_1$ and $g_2 = xc_2$, for example, then $g_1g_2 = xc_1xc_2 = x^2c_1^jc_2 = c_1^jc_2$.

If $j = 1$, then we are saying that x commutes with C, and we would have that G is an abelian group of order 30, which must be cyclic.

If $j = 14 \equiv -1 \pmod{15}$, then we have that G satisfies the relations of a dihedral group D_{15}, which we know has order 30 and is non-abelain.

The other two values $j = 4$ and 11 also turn out to give us two more non-abelian groups. In total, then there are 3 non-abelian groups of order 30, and 1 abelian group of order 30.

15.

a. What $(ab)^p = a^pb^p$ is really saying is that taking pth powers is a homomorphism from G to G (though not necessarily an automorphism, because it may fail to be injective). We must also have then that $(ab)^{p^2} = ((ab)^p)^p = (a^pb^p)^p = a^{p^2}b^{p^2}$; and, in fact, $(ab)^{p^j} = a^{p^j}b^{p^j}$.

Suppose now that P is any p-Sylow subgroup of G having size $|P| = p^J$. Then, as we know, $\varphi : G \to G$ given by $\varphi(a) = a^{p^J}$ is a homomorphism. The kernel consists of all elements of order dividing p^J, which must include any and all Sylow-p subgroups. But, in fact, this kernel is itself a p-group, because if $q||\ker(\varphi)|$, $q \neq p$, q prime, then the by Sylow's theorem this kernel (being a subgroup) would have to contain an element of order q. Call this element a. Then we have $a^q = e$ and $a^{p^J} = e$, which is impossible unless $a = e$. So, since the kernel is a p-group, its order is at most of size $|P|$; but, since it also contains P, its order is at least $|P|$, meaning that the kernel has size $|P|$ and is a Sylow-p itself.

Because the kernel is normal Sylow-p, and because all the other (potential) Sylow-p's are conjugate to it, we must have that there is only one

Sylow-p, namely P.

b. We know that $(ab)^{p^j} = a^{p^j} b^{p^j}$, for all j. Now, write $|G| = p^J m$, where p does not divide m. Then, it is not difficult to show that there exits an integer k such that $p^k \equiv 1 \pmod{m}$; and so, $p^k \equiv 1 \pmod{d}$, for any divisor d of m.

Let N be the set of all elements of G such that $x^m = 1$. We claim that N is a subgroup of G, and is in fact the subgroup we are looking for (but that takes some work to prove). Since G is finite, to show $N < G$ we just need to check that if $a, b \in N$, then $ba \in N$. To this end, we start with

$$(ab)^{p^k} \;=\; a^{p^k} b^{p^k}.$$

Now, if you write out the left-hand-side, you get

$$abababab \cdots ab \;=\; aaaaaaa \cdots abbbbbb \cdots b.$$

If we cancel off an a on the left and a b on the right of both sides, we get

$$(ba)^{p^k - 1} \;=\; a^{p^k - 1} b^{p^k - 1}.$$

Now, since $p^k \equiv 1 \pmod{m}$ we have $m | p^k - 1$; and so, the right-hand-side here is just the identity. That is to say,

$$(ba)^{p^k - 1} \;=\; e.$$

Thus, the order of ba must divide $p^k - 1$, and it must divide $|G| = p^J m$. It follows that the order of ba divides m, and therefore

$$(ba)^m \;=\; e,$$

which means $ba \in N$. Thus, N is a subgroup.

Next, we show that $|N| = m$. To do that, we observe that if $q^j || m$, where q is prime, then G contains a Sylow-q subgroup of order q^j. This subgroup lies in N, since $a^m = e$ for every a in this Sylow-q. Since N contains these Sylow-q's, for all primes $q \neq p$, we must have that product of the orders of these subgroups divides $|N|$. But, the product of these orders equals m, and so $m||N|$. It is easy to see that $|N|$ also divides m, giving us $|N| = m$ (for if not, then $|N|$ is divisible by a power of p, meaning that it contains an element b of order p, which will fail to satisfy $b^m = e$).

Finally, we wish to show that N is normal in G; if so, then $G = NP$, and we are done. First, we observe that the cosets Nq, where q runs through the elements of P are all disjoint and their union is G (because, if Nq and Nq' have an element in common, then $q(q')^{-1} \in N$, which means it is the identity or has order dividing $|N|$; the latter is impossible, since the order of $q(q')^{-1}$ is a power of p, and p does not divide m.). We likewise can decompose G into left cosets of N as qN, where q runs through the elements of P. Now, if $p^k \equiv 1 \pmod{m}$ and if $k > J$ (so that $p^k > |P|$), then for every element nq of the coset Nq we have

$$(nq)^{p^k-1} \;=\; q^{p^k-1}n^{p^k-1} \;=\; q^{-1}.$$

So, Nq is the set of those elements sent to q^{-1} upon taking (p^k-1)th powers. A similar computation shows qN is also those elements sent ot q^{-1}. Thus,

$$qN \;=\; Nq,$$

and we deduce that N is normal.

c. P by itself has a non-trivial center, being a p-group. Now suppose $q \in P$ lies in the center of P. If we always have q lies in the center of G, then the center of G is non-trivial.

We wish to show that q commutes with every element of G. To that end, let nr be an arbitrary element of $NP = G$, with $n \in N$ and $r \in P$. Then, since $nr \in nP = Pn$, we have $nr = r'n$, for some $r' \in P$; also, $nr \in Nr = rN$, implies $nr = rn'$. So, $r'n = rn'$ implies $r^{-1}r' = n'n^{-1}$. Since N and P are disjoint, the only way this could hold is if $r^{-1}r' = e = n'n^{-1}$. Thus, $r = r'$, and it follows that $nr = rn$. So,

$$q(nr) \;=\; qrn \;=\; rqn \;=\; rnq \;=\; (nr)q.$$

Here we have used the fact that q commutes with all of P, as well as the fact that $nr = rn$. We conclude that q lies in the center of G, and we are done.