Math 516 **Fall 2006** **Radford**

Written Homework # 3 Solution

11/22/06

You may use results form the book in Chapters 1–4 of the text, from notes found on our course web page, and results of the previous homework.

---

1. (**20 points total**) Let G be a group and $H, K \leq G$.

(a) (**7**) Suppose that $HK \leq G$ and let $f : H{\times}K \longrightarrow HK$ be defined by $f((h,k)) = hk$ for all $(h,k) \in H{\times}K$. Show that f is a homomorphism if and only if $hk = kh$ for all $h \in H$ and $k \in K$.

Solution: Let $h \in H$ and $k \in K$. First observe that

$$(h,e)(e,k) = (he,ek) = (h,k) = (eh,ke) = (e,k)(h,e);$$

in particular (h,e) and (e,k) commute.

Suppose that f is a homomorphism. The last two equations give

$$hk = f((h,k)) = f((e,k)(h,e)) = f((e,k))f((h,e)) = ekhe = kh.$$

Therefore $hk = kh$ for all $h \in H$ and $k \in K$.

Conversely, suppose that $hk = kh$ for all $h \in H$ and $k \in K$. Then for $(h,k), (h',k') \in H{\cap}K$ we have

$$\begin{aligned} f((h,k)(h',k')) &= f((hh',kk')) \\ &= (hh')(kk') \\ &= h(h'k)k' \\ &= h(kh')k' \\ &= (hk)(h'k') \\ &= f((h,k))f((h',k')). \end{aligned}$$

Therefore f is a homomorphism.

Suppose in addition that $H, K \trianglelefteq G$.

(b) (**6**) Show that $HK \trianglelefteq G$.

Solution: First of all the calculation

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$$

shows that $HK \leq G$. Note that we only use $H \leq G$ and $K \trianglelefteq G$ for this calculation. To show that $HK \trianglelefteq G$ we let $g \in G$ and note that

$$g(HK) = (gH)K = (Hg)K = H(gK) = H(Kg) = (HK)g.$$

(c) (**7**) Suppose that $H \cap K = (e)$. Show that $hk = kh$ for all $h \in H$ and $k \in K$ and that the homomorphism of part (b) is an isomorphism. [Hint: For $h \in H$ and $k \in K$ consider $hkh^{-1}k^{-1}$.]

Solution: Let $h \in H$ and $k \in K$. Then $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$; thus $hkh^{-1}k^{-1} \in K, H$ from which $hkh^{-1}k^{-1} \in H \cap K = (e)$ follows. Multiplying both sides of $hkh^{-1}k^{-1} = e$ on the right by k and then multiplying both sides of the resulting equation on the right by h yields $hk = kh$.

To show that f is an isomorphism we need only show that f is injective in light of part (a). Suppose $(h, k), (h', k') \in H \cap K$ and $f((h, k)) = f((h', k'))$. Then $hk = h'k'$ from which $kk'^{-1} = h^{-1}h'$ follows. Thus $kk'^{-1} \in K \cap H = (e)$ which means $kk'^{-1} = e = h^{-1}h'$. Therefore $k = k'$ and $h = h'$. We have shown $(h, k) = (h', k')$; thus f is injective.

2. (**20 points total**) Use the theory of finite cyclic groups and induction on $|G|$ to prove Cauchy's Theorem for abelian groups:

Theorem 1 *Let G be a finite abelian group and suppose that p is a prime integer which divides $|G|$. Then G as an element of order p.*

[Hint: Let $a \in G$ and set $H = <a>$. Then $|G/H||H| = |G|$.]

Solution: Our proof uses two facts about finite cyclic groups. If G is cyclic and p divides $|G|$ then G has an element of order p since G has exactly one (cyclic) subgroup for every divisor of $|G|$. If $G = <a>$ has order m and $a^n = e$ then $m|n$.

We proceed by induction on $|G|$. The case $|G| = 1$ is vacuous since p does not divide $|G|$ in this case. Suppose $m \geq 1$ and that the theorem holds for all abelian groups of order less than or equal to m. Let G be an abelian group such that $|G| \leq m + 1$ and suppose that p divides $|G|$. Then $|G| > 1$ so we may chose an $a \in G$ with $a \neq e$. If p divides $|<a>|$ then $<a>$, hence G, has an element of order p.

Suppose p does not divide $|<a>|$. Since G is abelian $H = <a> \trianglelefteq G$. Since $|G| = |G/H||H|$ and $|H| > 1$ it follows that p divides $|G/H|$ and $|G/H| < |G|$. Since G/H is abelian, by our induction hypothesis there is an element $bH \in G/H$ or order p. Let $n = |<b>|$. Then $(bH)^n = b^n H = eH = H$ from which we deduce $p|n$. Thus $<b>$ has an element of order p.

We have shown the conclusion of the theorem holds when $|G| \leq m + 1$. Thus the theorem follows by induction.

3. (**20 points total**) Let G be a finite group. For every positive divisor d of $|G|$ let n_d denote the number of cyclic subgroup of G of order d. Show that

$$|G| = \sum_{d|\,|G|} \varphi(d) n_d,$$

where φ is the Euler phi-function. [Hint: Consider the equivalence relation on G defined by $a \sim b$ if and only if $<a> = <b>$.]

Solution: Since "$=$" is an equivalence relation "$\sim$" is also. Let $\mathcal{C}$ be the set of cyclic subgroups of G. Then the set of equivalence classes $\mathcal{E}$ of $\sim$ is in bijective correspondence with $\mathcal{C}$ via

$$[x] \mapsto <x>$$

for all $x \in G$. (Indeed, if $f : G \longrightarrow \mathcal{C}$ is the surjective function given by $f(x) = <x>$ then $[x] = f^{-1}(<x>)$.) Let $E = [x]$ and $C = <x>$. Since E consists of the generators of C it follows that $|E| = \varphi(|C|)$. By Lagrange's Theorem $|C|$ divides $|G|$. Thus

$$\begin{aligned} |G| &= \sum_{E \in \mathcal{E}} |E| \\ &= \sum_{C \in \mathcal{C}} \varphi(|C|) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{d||G|} \left(\sum_{C\in\mathcal{C}, d=|C|} \varphi(|C|) \right) \\
&= \sum_{d||G|} \left(\sum_{C\in\mathcal{C}, d=|C|} \varphi(d) \right) \\
&= \sum_{d||G|} n_d \varphi(d).
\end{aligned}
$$

Comment: When G is cyclic of order n observe that the formula is

$$n = \sum_{d|n} \varphi(d)$$

since G has exactly one subgroup (which is cyclic) of order d for all divisors of n.

4. (**20 points total**) Let G be a finite group of order pqr, where p, q, r are primes and $p < q < r$.

(a) (**10**) Show that G is not simple.

(b) (**10**) Show that G has a subgroup of prime index.

[Hint: See the text's discussion of groups of order $30 = 2{\cdot}3{\cdot}5$. If needed, you may use the formula of Exercise 3.]

Solution: Let n_s be the number of Sylow-s subgroups of G, where $s = p, q, r$. For each s, by the Sylow Theorems $n_s|$ divides $|G|$ and $n_s = 1 + ks$ for some integer k. In particular s does not divide n_s.

Suppose that no Sylow-s subgroup is normal. Then $n_s \geq 1 + s$ for $s = p, q, r$. Since n_p is among q, r, qr and $q < r$ we conclude $n_p \geq q$. Since n_q is among p, r, pr and $p < q$, $r \leq qr$ we conclude $n_q \geq r$. Since n_r is among p, q, pq and $p, q < r$ we have $n_r = pq$. Since each Sylow-s subgroup of G is cyclic of prime order, each of these subgroups has $s - 1$ elements of order s. Counting the elements of order p, q, and r respectively gives the estimate

$$q(p-1) + r(q-1) + pq(r-1) \leq pqr$$

or

$$-q - r + qr \leq 0$$

which means

$$qr \leq q + r \leq 2r.$$

From the last inequality we have $qr \leq 2r$ or $q \leq 2$, a contradiction. Therefore some Sylow s-subgroup of G is normal. We have shown G is not simple and part (a) is established.

As for part (b), by part (a) there exists $N \trianglelefteq G$ or prime order. Let $H \leq G$ be a Sylow-s subgroup, where $s \neq |N|$. Then $|H| = s$ and $HN \leq G$ since $H \leq G = \mathrm{N}_G(N)$. Now $H \cap N \leq H, K$; thus $|H \cap N|$ divides $|H|, |N|$ by Lagrange's Theorem. Thus since $|H|$ and $|N|$ are relatively prime $|H \cap N| = 1$. Therefore $|H||N| = |HN||H \cap N| = |HN|$. Now $|G|$ is the product of three primes, two of which are $|H|$ and $|N|$. Thus

$$|G : HN| = \frac{|G|}{|HN|} = \frac{|G|}{|H||N|}$$

is the third prime.

5. (**20 points total**) Let G be a finite group of order pqr, where p, q, r are primes, $p < q < r$, and $r \not\equiv 1 \pmod{q}$. Show that G has a subgroup of index p.

Solution: The solution to Problem 4 suffices when H and N are Sylow-q and Sylow-r subgroups, or vice versa. Thus we need only show that G has a normal Sylow-q subgroup or a normal Sylow-r subgroup.

Suppose that G has neither a normal Sylow-q subgroup nor a normal Sylow-r subgroup. Then $n_r = pq$ and n_q is among p, r, pr. Since $p < q$ and $r \not\equiv 1 \pmod{q}$ necessarily $n_q = pr$. Estimating the number of elements of order q or r we derive

$$pr(q-1) + pq(r-1) \leq pqr$$

or

$$-pr - pq + pqr \leq 0$$

Therefore

$$qr \leq r + q < 2r$$

from which $q < 2$ follows. This contradiction shows that one of the Sylow-q subgroups of G or one of the Sylow-r subgroups of G is normal.

Comment: The counting arguments for Problems 4 and 5 involved a few types of elements. By taking into account more, a common solution can be given for both. Several of you did this. In particular the special condition in Problem 5 does not have to be used and thus it is not necessary. Here is a sketch.

Suppose that no Sylow q-subgroup of G an no Sylow r-subgroup of G is normal. Then $n_q, n_r > 1$ which means $n_q \geq r$ and $n_r = pq$. Since $n_p \geq 1$ in any case, the number of element of G of orders p, q, or r account for *at least* $1(p-1) + r(q-1) + pq(r-1)$ elements of the prq elements of G. But

$$\begin{aligned} 1(p-1) + r(q-1) + pq(r-1) &= p - r + qr - pq - 1 + pqr \\ &= (p-r)(1-q) - 1 + pqr \\ &= (r-p)(q-1) - 1 + pqr \\ &> prq \end{aligned}$$

since $(r-p)(q-1) \geq 2$. This contradiction shows that G has a normal Sylow q-subgroup of a normal Sylow q-subgroup.