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

Written Homework # 2 Solution

10/09/06

Let G be a non-empty set with binary operation. For non-empty subsets $S, T \subseteq G$ we define the product of the sets S and T by

$$ST = \{st \,|\, s \in S, t \in T\}.$$

If $S = \{s\}$ is a singleton then we set

$$sT = \{s\}T = \{st \,|\, t \in T\}$$

and if $T = \{t\}$ is a singleton we set

$$St = S\{t\} = \{st \,|\, s \in S\}.$$

We denote the set of inverses of elements of S by S^{-1}.

You may assume multiplication of sets is associative and $(ST)^{-1} = T^{-1}S^{-1}$. *From this point on G is a group*, not necessarily finite.

---

1. (**20 total**) Suppose that $H \leq G$.

(a) (**5**) Suppose that G is abelian. Show that $H \trianglelefteq G$.

Solution: Let $g \in G$ and $h \in H$. Since G is abelian $ghg^{-1} = hgg^{-1} = he = h \in H$. Therefore $H \trianglelefteq G$.

(b) (**5**) Suppose that $a^2 = e$ for all $a \in G$. Show that G is abelian.

Solution: Let $a, b \in G$. Then $e = (ab)^2 = (ab)(ab)$ shows that $e = abab$. Multiplying both sides of this equation on the left by a and on the right by b gives $ab = aeb = a(abab)b = a^2bab^2 = ebae = ba$. Therefore $ab = ba$ which shows that G is abelian.

(c) (**10**) Suppose that G is *finite* and $a^2 = e$ for all $a \in G$. Show, by induction, that $|G| = 2^n$ for some $n \geq 0$. [Hint: Suppose $e \neq a \in G$ and consider the quotient G/H, where $H = <a>$.]

Solution: We give a very formal, and detailed, proof by induction. For $m \geq 1$ let P_m be the statement:

"If G is a group which satisfies $a^2 = e$ for all $a \in G$ and $|G| \leq m$ then $|G|$ is a power of 2."

We will show that P_1 is true and for $m \geq 1$ if P_m is true then P_{m+1} is true (that is P_m implies P_{m+1}).

P_1 is true; for in this case $|G| = 1 = 2^0$.

Suppose $m \geq 1$ and P_m is true (our induction hypothesis). We need to show that P_{m+1} is true.

Let G be a group which satisfies $a^2 = e$ for all $a \in G$ and $|G| \leq m+1$. We must show that $|G|$ is a power of 2.

Now G is a abelian by part (b). Since P_1 is true we may assume $|G| > 1$. In this case there exists $x \in H$, $x \neq e$. Choose such an element a and set $H = <a>$. Then $H \trianglelefteq G$ by part (a). Since $a^2 = e \neq a$ it follows that $|H| = 2$.

Consider the quotient G/H. Note $|G/H| = |G|/|H| = |G|/2$. Now $|G/H| \leq m$; otherwise $(m+1)/2 \geq |G|/2 > m$ which implies $m+1 > 2m$, or $1 > m$, a contradiction. Since $(aH)^2 = a^2H = eH = H$ for all $a \in G$, by the induction hypothesis $|G/H|$ is a power of 2. Therefore $|G| = 2 \cdot |G/H|$ is a power of 2. We have shown that P_m implies P_{m+1}.

We have shown that P_1 is true and that P_m implies P_{m+1} for all $m \geq 1$. Therefore P_m is true for all $m \geq 1$ by the Principle of Mathematical Induction.

Remark: Part (a) is rather trivial but is included for part (c).

2. (**20 total**) Suppose that $H, K \leq G$ and let $f : H \times K \longrightarrow HK$ be the set map defined by $f((h,k)) = hk$ for all $(h,k) \in H \times K$.

(a) (**10**) For fixed $h \in H$ and $k \in K$ show that

$$f^{-1}(hk) = \{(hx, x^{-1}k) \,|\, x \in H \cap K\}.$$

Solution: Let $x \in H \cap K$. Then $(hx, x^{-1}k) \in H \times K$ since $H, K \leq G$. Since $f((hx, x^{-1}k)) = hxx^{-1}k = hek = hk$ we have shown that

$$\{(hx, x^{-1}k) \,|\, x \in H \cap K\} \subseteq f^{-1}(hk).$$

To complete part (a) we need only establish the other inclusion.

Suppose that $(h', k') \in f^{-1}(hk)$. Then $h'k' = f((h', k')) = hk$. From the equation $hk = h'k'$ we derive $h(kk'^{-1}) = h'$, thus $kk'^{-1} = h^{-1}h'$, and $k' = (h'^{-1}h)k$. Let $x = kk'^{-1}$. Then $h' = hx$ and $x \in K \cap H$ follow from the second and third equations. From the fourth and third we deduce $k' = (h^{-1}h')^{-1}k = (kk'^{-1})^{-1}k = x^{-1}k$. Therefore $(h', k') = (hx, x^{-1}k)$. We have shown

$$f^{-1}(hk) \subseteq \{(hx, x^{-1}k) \,|\, x \in H \cap K\}.$$

(b) (**5**) For fixed $h \in h$ and $k \in K$ show that the function

$$b : H \cap K \longrightarrow f^{-1}(hk)$$

defined by $b(x) = (hx, x^{-1}k)$ for all $x \in H \cap K$ is a bijection.

Solution: By part (a) the problem is to show that

$$b : H \cap K \longrightarrow \{(hx, x^{-1}k) \,|\, x \in H \cap K\}$$

defined by $b(x) = (hx, x^{-1}k)$ for all $x \in H \cap K$ is injective. Suppose that $x, x' \in H \cap K$ and $b(x) = b(x')$. Then $(hx, x^{-1}k) = (hx', x'^{-1}k)$ which implies $hx = hx'$. By left cancellation $x = x'$. Thus b is injective.

(c) (**5**) Now suppose that H, K are *finite*. Use parts (a)–(b) to show that

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

Solution: (**5**) Suppose that X is a finite set and $f : X \longrightarrow Y$ is surjective. Then

$$|X| = \sum_{y \in Y} |f^{-1}(y)|$$

since the fibers of f partition X. Thus by parts (a) and (b)

$$|H||K| = |H \times K| = \sum_{x \in HK} |f^{-1}(x)| = \sum_{x \in HK} |H \cap K| = |HK||H \cap K|.$$

Remark: The conclusion of part (c) is an important counting principle stated in the text and proved there somewhat differently. Here we base a proof on fibers which is an idea emphasized in the text discussion of cosets and quotient groups.

3. (**20 total**) Suppose that H is a non-empty subset of G.

(a) (**6**) Show that $H \leq G$ if and only if $HH = H$ and $H^{-1} = H$.

Solution: Suppose $H \leq G$. Then $HH = \{hh' \mid h, h' \in H\} \subseteq H$ since H is closed under products. Thus $HH \subseteq H$. Since $h = he \in HH$ for all $h \in H$ it follows that $H \subseteq HH$. Therefore $HH = H$.

Now $h^{-1} \in H$ for all $h \in H$. Therefore $H^{-1} \subseteq H$. As $(a^{-1})^{-1} = a$ for all $a \in G$, the inclusion $H^{-1} \subseteq H$ implies $H = (H^{-1})^{-1} \subseteq H^{-1}$. Therefore $H^{-1} = H$.

Conversely, suppose that $HH = H$ and $H^{-1} = H$. Let $a, b \in H$. Then $ab^{-1} \in HH^{-1} = HH = H$. By assumption $H \neq \emptyset$. Therefore $H \leq G$.

(b) (**6**) Suppose that $H, K \leq G$. Using part (a), show that $HK \leq G$ if and only if $HK = KH$.

Solution: Suppose that $HK \leq G$. Then, using part (a), $KH = K^{-1}H^{-1} = (HK)^{-1} = HK$. Therefore $KH = HK$.

Conversely, suppose that $HK = KH$. Then, using part (a) again,

$$(HK)(HK) = H(KH)K = H(HK)K = HHKK = HK$$

and

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK.$$

Thus $HK \leq G$ by part (a).

(c) (**7**) Suppose that H is *finite*. Show that $H \leq G$ if and only if $HH \subseteq H$. [Hint: Suppose that $HH \subseteq H$ and $a \in H$. Show that the list $a, a^2, a^3, \ldots$ must have a repetition.]

Solution: If $H \leq G$ then $HH = H$ by part (a); hence $HH \subseteq H$. Conversely, suppose that $H \subseteq G$ and $HH \subseteq H$. Let $a \in H$. Then

$$a, a^2, a^3, \ldots$$

is a sequence of elements which lie in H since H is closed under the group operation. Since H is finite there must be a repetition in this sequence. Thus $a^\ell e = a^\ell = a^m$ for some $1 \leq \ell < m$. By left cancellation $e = a^{m-\ell}$. Since $m - \ell > 0$ it follows that $a^0 = e \in H$ and, as $m - \ell - 1 \geq 0$, $a^{-1} = a^{m-\ell-1} \in H$.

Remark Part (a) gives a very important way of saying what it means to be a subgroup in terms of *sets* instead of elements. Part (c) shows that "finite" can be a rather powerful assumption.

4. (**20 total**) Suppose that $|G| = 6$.

(a) (**4**) Use Exercise 1 to show that $a^2 \neq e$ for some $a \in G$.

Solution: Suppose that $a^2 = e$ for all $a \in G$. Then $|G|$ is a power of 2 by Exercise 1, a contradiction. Therefore $a^2 \neq e$ for some $a \in G$.

(b) (**4**) Use Exercise 2 to show that G has *at most* one subgroup of order 3. (Thus if G has a subgroup N of order 3 then $N \trianglelefteq G$.)

Solution: Suppose that $H, K \leq G$ are subgroups of order 3. Since $H \cap K \leq H$, it follows by Lagrange's Theorem that $|H \cap K| = 1, 3$. By the formula of Exercise 2

$$9 = |H||K| = |HK||H \cap K|.$$

Since $|HK| \leq 6$ necessarily $|H \cap K| \neq 1$; thus $|H \cap K| = 3$. Since $H \cap K \subseteq H, K$, and $|H|$, $|H \cap K|$, $|K|$ are all equal, we deduce $H = H \cap K = K$.

(c) (**4**) Use Lagrange's Theorem and parts (a) and (b) to show that G has an element a of order 2 and an element b of order 3.

Solution: By Lagrange's Theorem an element of G has order $1, 2, 3$ or 6 as these are the divisors of $|G| = 6$.

Suppose that $x \in G$ has order 6. Then $a = x^3$ has order 2 and $b = x^2$ has order 3. Thus we may assume that G has no elements of order 6.

Since $|G|$ is not a power of 2, by part (a) there is some element of G whose order is not 1 or 2. Let b be such an element. Then b must have order 3. Let $a \notin H = <b>$. Since a does not have order 3 by part (b), and a does not have order 1 since $a \neq e$, necessarily a has order 2.

(d) (**4**) Let $N = <b>$. Show that $|G : N| = 2$. (Thus $N \trianglelefteq G$.) Show that $ab = ba$ or $ab = b^2a = b^{-1}a$.

Solution: $N = <b>$ has order 3 since b does. Since $|G| = |G : N||N||$ we have $6 = |G : N|3$ so $|G : N| = 2$. (Thus $N \trianglelefteq G$.) Now $\{ae, ab, ab^2\} = aN = Na = \{ea, ba, b^2a\}$ since $N \trianglelefteq G$. If $ab \neq ba, b^2a$ then $ab = ea = ae$ which means $b = e$ by left cancellation, contradiction. Thus $ab = ba$ or $ab = b^2a$.

(e) (**4**) Suppose that $ab = ba$. Use Lagrange's Theorem to show that G is cyclic. [Hint: Consider $<ab>$.]

Solution: Since $ab = ba$ it follows that $(ab)^m = a^m b^m$ for all $m \geq 0$. The calculations

$$(ab)^0 = e, (ab)^1 = ab, (ab)^2 = a^2b^2 = eb^2 = b^2,$$

$$(ab)^3 = a^3b^3 = a^2ae = eae = a, (ab)^6 = a^6b^6 = ee = e,$$

and

$$(ab)^6 = a^6b^6 = ee = e$$

show that $b^2 = b^{-1}, a \in <ab>$ and $|<ab>| \leq 6$. By Lagrange's Theorem $2 = |a|, 3 = |b^{-1}|$ divide $|<ab>| = |ab| \leq 6$. Therefore 6 divides $|ab|$ which means $|ab| = 6$; thus $G = <ab>$.

Remark: A more efficient way to do this exercise would be to use Cauchy's theorem. As it turns out we can use more elementary arguments since 6 is such a small size for group.

5. (**20 total**) We continue Exercise 4.

   (a) (**10**) Show that $G = \{e, b, b^2, a, ab, ab^2\}$.

   Solution: $N = \{e, b, b^2\}$ has 3 elements; thus $aN = \{ae, ab, ab^2\}$ does also since the left cosets of a subgroup of a finite group have the same number of elements. Since a does not have order 1 or 3 it follows $a \notin H$. As $|G : H| = 2$ it follows that H and aH are the left cosets of G. Since the left cosets partition G, $G = H \cup aH$ is a disjoint union.

   (b) (**10**) Suppose that $ab = b^2 a$. Complete the multiplication table

	e	b	b^2	a	ab	ab^2
e						
b						
b^2						
a						
ab						
ab^2						

   for G.

[Hint: Let $N = <b> = \{e, b, b^2\}$. Then $N \trianglelefteq G$ and $|G/N| = 2$. Note that $G/N = \{N, aN\}$ by part (a). Since aN has order 2 the multiplication table for G/N is given by

	N	aN
N	N	aN
aN	aN	N

.]

You can ignore this hint and simply use the relations

$$a^2 = e, \qquad b^3 = e, \qquad ab = b^2 a$$

to compute *all* of the products. However, it would be very illuminating to use the hint and see how many calculations you then need to make using the relations.

Comment: The relations $a^2 = e = b^3$ and $ab = b^2a$ completely determine the group table in Exercise 5. In light of Exercise 4 there is *at most one* non-abelian group G (up to isomorphism) of order 6. Since S_3 has order 6 and is non-abelian, $G \simeq S_3$.

Solution: $b^2a = ab$ and $(ab)^2 = abab = b^2aab = b^2eb = b^3 = e$. Coset multiplication is multiplication of sets. Using the relations $a^2 = e$, $b^3 = e$, the results of the two preceding calculations, the multiplication table for G/N, and the fact that each element of G must appear once in each row and column of the multiplication table for G, we must have:

	e	b	b^2	a	ab	ab^2
e	e	b	b^2	a	ab	ab^2
b	b	b^2	e	ab^2	a	ab
b^2	b^2	e	b	$\mathbf{ab}$	ab^2	a
a	a	ab	ab^2	e	b	b^2
ab	ab	ab^2	a	b^2	$\mathbf{e}$	b
ab^2	ab^2	a	ab	b	b^2	e

The single lines are not part of the table; they indicate the role the table for G/N plays in the construction of the table for G.

One further comment. From our solution of part (c) of Exercise 4 we know that any element not in N must have order 2. Thus the calculation which shows $(ab)^2 = e$ was not necessary. It was, of course, a good exercise in the use of the relation $ab = b^2a$.