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

Written Homework # 1 Solution

10/11/06

Remark: Most of the proofs on this problem set are just a few steps from definitions and were intended to be a good warm up for the course. Sometimes the significance of a problem is far more interesting than its solution.

1. (**20 total**) Let G be a group.

a) Suppose that H, K are subgroups of G. Show that $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Solution: *If*. Suppose $H \subseteq K$ or $K \subseteq H$. Then $H \cup K = K$ or $H \cup K = H$. In either case $H \cup K \leq G$ as $H, K \leq G$.

Only if. Suppose that $H \cup K \leq G$. To show that $H \subseteq K$ or $K \subseteq H$ we need only show $H \not\subseteq K$ implies $K \subseteq H$.

Suppose $H \not\subseteq K$. Then there is an $h \in H$ such that $h \notin K$. Let $k \in K$. Then $h, k \in H \cup K$ which means $hk \in H \cup K$ since $H \cup K \leq G$. If $hk \in K$ then $h = he = h(kk^{-1}) = (hk)k^{-1} \in K$, a contradiction. Therefore $hk \in H$ which means $k = ek = (h^{-1}h)k = h^{-1}(hk) \in H$. We have shown $K \subseteq H$.

Remark: Most proved the interesting implication of part a) by contradiction. The argument starts this way. Suppose that $H \not\subseteq K$ and $K \not\subseteq H$. Then there is an $h \in H$ with $h \notin K$ and a $k \in K$ with $k \notin H$. Since $h, k \in H \cup K \leq G$ the product $hk \in H \cup K$. ..... (contradiction in short order).

Here are some elementary comments on the structure of compound statements which apply to this problem in particular. "P if and only if

Q" is a combination of two statements, "P if Q" and "P only if Q", and is thus logically equivalent to "(P if Q) and (P only if Q)". "P if Q" is logically equivalent to "Q implies P", and "P only if Q" is logically equivalent to "P implies Q". To establish "P implies Q" is a matter of showing that if P is true then Q is true.

"P or Q" is logically equivalent to "(not P) implies Q". This equivalence was used in the argument for the "only if" part in part a). The statement "not (P or Q)" is logically equivalent to "(not P) and (not Q)".

b) Let I be a non-empty set and suppose that $\{H_i\}_{i \in I}$ is an indexed family of subgroups of G which satisfies the following condition: For all $i, j \in I$ there is an $\ell \in I$ such that $H_i, H_j \subseteq H_\ell$. Show that the union $H = \cup_{i \in I} H_i$ is a subgroup of G.

Solution: $H \neq \emptyset$ since $I \neq \emptyset$ and at least one of the H_i's is not empty (in fact none of the H_i's are empty). Let $a, b \in H$. Then $a \in H_i$ and $b \in H_j$ for some $i, j \in I$. By assumption there is an $\ell \in I$ such that $H_i, H_j \subseteq H_\ell$. Therefore $a, b \in H_\ell$. Since $H_\ell \leq G$ it follows that $ab^{-1} \in H_\ell$. Since $H_\ell \subseteq H$ we have $ab^{-1} \in H$. Therefore $H \leq G$.

Remark: The intersection of a non-empty family of subgroups is always a subgroup; this is not true of unions in general by part a). Part b) gives an important condition under which the union is a subgroup.

2. (**20 total**) Suppose that G and G' are groups.

a) Show that the Cartesian product of sets $G \times G'$ is a group where

$$(g, g')(h, h') = (gh, g'h')$$

for all $(g, g'), (h, h') \in G \times G'$.

Solution: $G \times G'$ is not empty since G and G' are not empty. Let $(g, g'), (h, h'), (\ell, \ell') \in G \times G'$. The calculations

$$[(g, g')(h, h')](\ell, \ell') = (gh, g'h')(\ell, \ell') = ((gh)\ell, (g'h')\ell') = (g(h\ell), g'(h'\ell'))$$

and

$$(g,g')[(h,h')(\ell,\ell')] = (g,g')(h\ell,h'\ell') = (g(h\ell),g'(h'\ell'))$$

show that the operation in $G{\times}G'$ is associative.

The calculations

$$(g,g')(e,e') = (ge,g'e') = (g,g') \text{ and } (e,e')(g,g') = (eg,e'g') = (g,g')$$

establish that (e,e') is an identity element for $G{\times}G'$. For $(g,g') \in G{\times}G'$ the computations

$$(g,g')(g^{-1},g'^{-1}) = (gg^{-1},g'g'^{-1}) = (e,e')$$

and

$$(g^{-1},g'^{-1})(g,g') = (g^{-1}g,g'^{-1}g') = (e,e')$$

show that (g,g') has an inverse.

Remark: The proof of part a) needs to be done to be certain of the details of the direct product construction. It is straightforward and not terribly interesting.

b) Suppose that $f : G \longrightarrow G'$ is a group isomorphism. Show that $|g| = |f(g)|$ for all $g \in G$.

Solution: Let $n \in \mathbf{Z}$. Since f is an *injective* homomorphism, $g^n = e$ if and only if $f(g^n) = f(e)$ if and only if $f(g)^n = e'$. This is enough. (Note that bijective is not used, just injective.)

Now let $G = \mathbf{Z}_2 = \{0,1\}$ and $V = G{\times}G$.

c) Set $e = (0,0)$, $a = (1,0)$, $b = (0,1)$, and $c = (1,1)$. Write down the table for the group structure of V.

Solution:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

d) Show that there is *no* isomorphism $f : V \longrightarrow \mathbf{Z}_4$.

Solution: Suppose there is such an isomorphism f. Then $f(x) = 1$ for some $x \in V$. Now 1 has order 4. Thus x has order 4 by part b). But examination of the group table of part b) shows that all elements of V have order 1 or 2. This contradiction shows that there can be no such isomorphism.

Remark: I can not find a reference for this: A statement P about an abstract group is a property of groups if whenever P is true for a group G it is also true for any group isomorphic to G. Thus "G has element of order 4" is a property of groups. Whether or not a property is true for a particular group is a different matter. Note that "G has 3 elements of order 2" is also a property of groups. The statement "The integer 1 belongs to G" is not.

3. (**20 total**) Let G be a group.

a) Suppose that X is a non-empty set and $G{\times}X \longrightarrow X$ is a left action of G on X. Show that $x \sim y$ if and only if $y = g{\cdot}x$ for some $g \in G$ defines an equivalence relation on X and for $x \in X$ the equivalence class

$$[x] = G{\cdot}x,$$

the G-orbit of x.

Solution: Let $x \in X$. Then $x = e{\cdot}x$; so $x \sim x$. Suppose that $x \sim y$. Then $y = g{\cdot}x$ for some $g \in G$. Thus

$$g^{-1}{\cdot}y = g^{-1}{\cdot}(g{\cdot}x) = (g^{-1}g){\cdot}x = e{\cdot}x = x$$

means that $y \sim x$. Suppose that $x \sim y$ and $y \sim z$. Then $y = g{\cdot}x$ and $z = h{\cdot}y$ for some $g, h \in G$. Therefore

$$(hg){\cdot}x = h{\cdot}(g{\cdot}x) = h{\cdot}y = z$$

which implies that $x \sim z$. Now

$$[x] = \{y \in X \,|\, y \sim x\} = \{g{\cdot}x \,|\, g \in G\} = G{\cdot}x$$

for all $x \in X$.

Now suppose that H is a subgroup of G.

b) Show that $h{\cdot}g = hg$, the product of h and g in G, for all $h \in H$ and $g \in G$ defines a left action of the group H on the set G.

 Solution: $e{\cdot}a = ea = a$ for all $a \in G$. For $g, h, a \in G$ associativity gives $(gh){\cdot}a = (gh)a = g(ha) = g{\cdot}(h{\cdot}a)$.

c) Show that $[x] = Hx$ for all $x \in G$, where $Hx = \{hx \,|\, h \in H\}$.

 Solution: $[x] = H{\cdot}x = Hx$ for all $x \in G$ by part a).

d) For $x, y \in G$ show that $f : [x] \longrightarrow [y]$ given by $f(hx) = hy$ for all $h \in H$ is a *well-defined* function which is a set bijection. [Note: $hy \in [y]$ for all $h \in H$. Well-defined means that if $h, h' \in H$ then $hx = h'x$ implies $hy = h'y$.]

 Solution: *Well-defined*. Suppose $h, h' \in G$ and $hx = h'x$. Then by right cancellation $h = h'$. Therefore $hy = h'y$. We have shown that $f : [x] \longrightarrow [y]$ given by $f(hx) = hy$ for $h \in H$ is a well-defined function.

 Interchanging the roles of x and y we conclude that $g : [y] \longrightarrow [x]$ given by $g(hy) = hx$ is a well defined function. Since $g(f(hx)) = g(hy) = hx$ and $f(g(hy)) = f(hx) = hy$ for all $h \in H$ it follows that f and g are inverse functions. Therefore f (and hence g) are bijective.

 Remark: Well-defined is an issue when for a given input a choice needs to be made to determine the output. In this case we let $z \in [x]$. Then $z = wx$ for some $w \in H$. *Choose such a* w, call it h, and write $z = hx$.

e) Now suppose that G is *finite*. Show that $|H|$ divides $|G|$.

 Solution: The equivalence classes of any equivalence relation on G partition G. Consider the left action of part b) by H on G and the resulting equivalence relation of part a). By part d) all classes have the same number of elements. Therefore $|[x]|$ divides G for all $x \in G$. Since $[e] = H$ by part c) it follows that $|H|$ divides G.

4. (**20 total**) Let G, G', and G'' be groups.

a) Show that the identity map $1_G : G \longrightarrow G$ is an isomorphism.

Solution: $1_G(ab) = ab = 1_G(a)1_G(b)$ for all $a, b \in G$. Therefore the bijection 1_G is a homomorphism of G.

b) Suppose that $f : G \longrightarrow G'$ and $f' : G' \longrightarrow G''$ are homomorphisms (respectively isomorphisms). Show that the composite $f' \circ f : G \longrightarrow G''$ is a homomorphism (respectively an isomorphism). [You may assume that the composition of bijective functions is bijective.]

Solution: We need only show that $f' \circ f$ is a homomorphism. This follows by

$$(f' \circ f)(ab) = f'(f(ab)) = f'(f(a)f(b)) = f'(f(a))f'(f(b)) = (f' \circ f)(a)(f' \circ f)(b)$$

for all $a, b \in G$.

c) Suppose that $f : G \longrightarrow G'$ is an isomorphism. Show that its composition inverse $f^{-1} : G' \longrightarrow G$ is an isomorphism.

Solution: Since f and f^{-1} are inverse functions $f^{-1}(f(a)) = a$ for all $a \in G$ and $f(f^{-1}(x)) = x$ for all $x \in G'$. Therefore

$$\begin{aligned} f^{-1}(xy) &= f^{-1}(f(f^{-1}(x))f(f^{-1}(y))) \\ &= f^{-1}(f(f^{-1}(x)f^{-1}(y))) \\ &= f^{-1}(x)f^{-1}(y) \end{aligned}$$

for all $x, y, \in G'$.

Remark: You might think of parts a)–c) as describing an "algebra of isomorphisms". Reminiscent of the group axioms?

d) Show that the set $\mathrm{Aut}(G)$ of all isomorphisms from G to itself (that is the set of all automorphisms of G) is a subgroup of $S_G = \mathrm{Sym}(G)$.

Solution: By part a) $1_G \in \mathrm{Aut}(G)$. By part b) the set $\mathrm{Aut}(G)$ is closed under composition. By part c) every element of $\mathrm{Aut}(G)$ has an inverse in $\mathrm{Aut}(G)$. Therefore $\mathrm{Aut}(G) \leq \mathrm{Sym}(G) = S_G$.

e) The symbolism $G \sim G'$ means there exists an isomorphism $f : G \longrightarrow G'$. Show that "$\sim$" satisfies the axioms of an equivalence relation;

(a) $G \sim G$,

(b) $G \sim G'$ implies $G' \sim G$,

(c) $G \sim G'$ and $G' \sim G''$ implies $G \sim G''$.

Solution: (a) Let G be a group and take $f = 1_G$ which is an isomorphism by part a). (b) Suppose $G \sim G'$ and let $f : G \longrightarrow G'$ be an isomorphism. Then $f^{-1} : G' \longrightarrow G$ is an isomorphism by part b). Therefore $G' \sim G$. (c) Suppose that $G \sim G'$ and $G' \sim G''$. Let $f : G \longrightarrow G'$ and $f' : G' \longrightarrow G''$ be isomorphisms. Then $f' \circ f : G \longrightarrow G''$ is an isomorphism by c). Therefore $G \sim G''$.

Remark: Any set of groups can be partitioned by isomorphism classes.

5. (**20 total**) Let G be a group and $\mathrm{Aut}\,(G)$ be the group of all automorphisms of G under function composition; see Exercise 4.d).

a) For $g \in G$ let $\sigma_g : G \longrightarrow G$ be the function defined by $\sigma_g(x) = gxg^{-1}$ for all $x \in G$. Show that $\sigma_g \in \mathrm{Aut}\,(G)$.

Solution: Let $g, h \in G$. Then

$$\begin{aligned}(\sigma_g \circ \sigma_h)(x) &= \sigma_g(\sigma_h(x)) \\ &= g(hxh^{-1})g^{-1} \\ &= ghxh^{-1}g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= \sigma_{gh}(x)\end{aligned}$$

for all $x \in G$ means that

$$\sigma_g \circ \sigma_h = \sigma_{gh} \tag{1}$$

for all $g, h \in G$. Since $\sigma_e(x) = exe^{-1} = exe = x$ for all $x \in G$ we have

$$\sigma_e = 1_G. \tag{2}$$

Let $g \in G$. By (1) and (2) we compute $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{gg^{-1}} = \sigma_e = 1_G$; thus $\sigma_g \circ \sigma_{g^{-1}} = 1_G$ for all $g \in G$. Since $(g^{-1})^{-1} = g$, replacing g by g^{-1} in the lasrt equation gives $\sigma_{g^{-1}} \circ \sigma_g = 1_G$. Therefore σ_g has a function inverse which is $\sigma_{g^{-1}}$. We have shown that σ_g is an automorphism of G.

b) Let $\pi : G \longrightarrow \mathrm{Aut}\,(G)$ be the function defined by $\pi(g) = \sigma_g$ for all $g \in G$. Show that π is a group homomorphism. [Thus $g{\cdot}x = \pi(g)(x)$ defines a left action of G on itself.]

Solution: Using (1) we calculate

$$\pi(gh) = \sigma_{gh} = \sigma_g \circ \sigma_h = \pi(g) \circ \pi(h)$$

for all $g, h \in G$. Therefore π is a homomorphism.