M403 Homework 13

Enrique Areyan
December 5, 2012

(2.52) (i) **True**. We need to check three properties: 1) $e \in H$. This is true because H is a subgroup of K and K is a subgroup of G and hence, K inherits the identity of G and H inherits the same identity from K. 2) Since H is a subgroup, H is closed under its binary operation and 3) likewise, since H is a subgroup, H is closed under taking inverses.

(ii) **True**. Just use the same identity of the group for the subgroup and all three subgroup conditions follows trivially from the definition of group.

(iii) **False**. Since $e \notin G$, i.e., there is no identity.

(iv) **False**. Let $S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. The order of S_3 is 6, but there is no element of order 6.

(v) **True**. Since the order of S_n is $n!$, we can just apply Lagrange's Theorem.

(vi) **False**. It might be possible for the intersection to be empty.

(vii) **True**. Since the intersection of any subgroups is a subgroup. Moreover, every subgroup of a cyclic subgroup is cyclic.

(viii) **False**. Let $X = \{1\} \in \mathbb{Z}$. Then, $\langle -1 \rangle = \mathbb{Z}$

(ix) **True** $id \in F$, since the identity moves a finite number of elements (moves zero elements). If $\alpha, \beta \in F$, then $\alpha \circ \beta \in F$, since the composition will also move a finite number of elements. If $\alpha \in F$, then the inverse will move the same number of elements which means that $\alpha^{-1} \in F$.

(x) **True**. By Lagrange's theorem, a proper subgroup H of S_3 is such that $|H||S_3| = 6$. Hence, $|H| = 1, 2$ or 3. In exercise 2.70 (i) I show that every group of prime order is cyclic.

(xi) **False**. The counterexample can be found on page 148, the subgroup V of S_6 where each element has order 2 so that there is no generator and hence, V is not cyclic.

(2.53) (i) Let G be a group and H be a subgroup of G. Let $g \in G$. By definition, $gH = \{gh : h \in H\}$. In particular, since H is a subgroup, $e \in H$ and thus, $g \cdot e = g \in gH$. If we consider $a_1H, a_2H, ..., a_tH$ to be all the distinct cosets of H in G, then there exists i such that $gH = a_iH$, in particular take $g = a_i$.

(ii) Let $c \in aH \cap bH$. Then $c \in aH$ and $c \in bH$. By definition of left cosets, $c = ah_1$ for some $h_1 \in H$ and $c = bh_2$ for some $h_2 \in H$. Hence, $ah_1 = bh_2$. Operating by h_2^{-1} on both sides we get that $ah_1h_2^{-1} = b$. Let $h_3 = h_1h_2^{-1}$, then we can write $b = ah_3$ where $h_3 \in H$. Therefore, $b \in aH$. A similar arguments shows that $a \in bH$ and hence, $aH = bH$. Hence, if $i \neq j$ we must have that $a_iH \cap a_jH = \emptyset$

(2.55) Let $G = \mathbb{Z}/6 = (\{0, 1, 2, 3, 4, 5\}, +, 0)$. Let $H = \{0, 4, 2\}$ and $K = \{0, 3\}$. Both H and K are subgroups of G since, 1) $e = 0 \in H, K$. 2) for H: $4 + 4 = 8 \equiv 2 \pmod 6$ and $4 + 2 = 2 + 4 = 6 \equiv 0 \pmod 6$ (the other combinations being trivial); for K: $3 + 3 = 6 \equiv 0 \pmod 6$ (the other combinations being trivial). Finally 3) for H: the inverse of 4 is 2 and for K: the inverse of 3 is itself.

We can see that $H \cup K = \{0, 2, 3, 4\}$ is not a subgroup since the operation is not closed: take $2, 3 \in H \cup K$, the sum $2 + 3 = 5 \notin H \cup K$.

(2.57) By proposition 2.76 we know that $H \cap K$ is a subgroup of H and a subgroup of K. Therefore, by Lagrange's theorem, $|H \cap K|$ divides $|H|$ and also divides $|K|$. But $|H|$ and $|K|$ are relatively prime and so the only common divisor is one. In particular this means that $|H \cap K|$ has only one element, and since this is a group it has to contain the identity, hence $H \cap K = \{e\}$

(2.59) Let G be a group of order 4. If there exists $a \in G$ such that $\langle a \rangle = G$, then G is cyclic and we are done. Otherwise, let $a \in G$. Consider $\langle a \rangle$ as a proper subgroup of G. Since $|G| = 4$, by Lagrange's theorem it must be the case that $|\langle a \rangle|$ divides $|G|$ and hence, $|\langle a \rangle| = 2$ or $|\langle a \rangle| = 1$. If $|\langle a \rangle| = 2$ then by definition $a^2 = 1$. If $|\langle a \rangle| = 1$ then $a = 1$ which implies that $a^2 = 1$. In either case we obtain the result.
Finally, if G is cyclic then it is abelian. If the preceding result holds then by exercise 2.44 G is abelian.

(2.63) (i) By definition: $\langle (1\ 2) \rangle = \{id, (1\ 2)\}$. Let $\alpha \in S_3$ be $\alpha = (4\ 1)$. Then $(4\ 1)\langle (1\ 2) \rangle = \{(4\ 1), (2\ 4\ 1)\} \neq \langle (1\ 2) \rangle (4\ 1) = \{(4\ 1), (1\ 4\ 2)\}$

(ii) Let $f : aH \mapsto Ha^{-1}$ be defined as $f(aH) = Ha^{-1}$. If we show that this is a bijection, then we have showed that the number of left cosets and right cosets is the same.
Suppose that $g_1H = g2H$. Then, $g_1 = g_1 \cdot e \in g_1H = g_2H$, so $g_1 = g_2 \cdot h$ for some $h \in H$. Now we compute, $f(g_1H) = Hg_1^{-1} = h^{-1}g_2^{-1} = f(g_2H)$. Hence, f is injective.
Now, let Hb be a right coset. Since H is a group, b has a unique inverse b^{-1} such that $f(b^{-1}H) = H(b^{-1})^{-1} = Hb$. This means that f is surjective.
Since f is both injective and surjective, it is a bijection. In particular this means that the sets of left and right cosets have the same number of elements.

(2.64) (i) **True** by definition.

(ii) **False** since the operation of the group $\mathbb{R}^\times$ is not $+$.

(iii) **True**. The inclusion $f : \mathbb{Z} \mapsto \mathbb{R}$ is defined as $f(z) = z$. Hence, for every $z_1, z_2 \in \mathbb{Z}$, $f(z_1 + z_2) = z_1 + z_2 = f(z_1) + f(z_2)$

(iv) **True**. Just set $f(0) = (1)$. Then, $f(0 + 0) = f(0) = (1) = (1) \circ (1) = f(0) \circ f(0)$

(v) **False**. Consider $\mathbb{Z}/6$ and S_3, both of order 6 and not isomorphic (see 2.70, (ii)).

(vi) **True**. Any group of primer order is cyclic (see 2.70 (i)). Let G_1 and G_2 be two groups of prime order, then $f : G_1 \mapsto G_2$ given by $f(a^i) = b^i$ is an isomorphism.

(2.70) (i) Claim: a group G is not abelian only in case that $|G| > 4$. Proof: to be non-abelian means that there exists $x, y \in G$ such that $xy \neq yx$. Since G is a group, we know that the identity e is in G. It is obvious that the identity respects commutativity since $xe = ex = x$ and $ey = ye = y$. Hence, we need distinct x, y such that operating them in different order results in two different elements $xy \neq yx$. In sum we need at least $e, x, y, xy, yx \in G$, all distinct, in order to have a non-abelian group.

Now we need to analyze the case where G is a group such that $|G| = 5$. To do this I will show the following: Claim: a group of prime order is cyclic. Once we know that the group is cyclic we can conclude that it is abelian. Proof: Let G be a group such that $|G| = p$ where p is prime. Let $a \in G$. Consider the subgroup $\langle a \rangle$. By Lagrange's theorem, $|\langle a \rangle|$ divides $|G|$. Since $|G|$ is prime, the only divisors of $|G|$ are 1 and p. So either $|\langle a \rangle| = 1$ or $|\langle a \rangle| = p$. If $|\langle a \rangle| = 1$ then $\langle a \rangle = \{e\}$. Otherwise, $|\langle a \rangle| = p$ which implies that $\langle a \rangle = G$ so G is cyclic.

Using the above claim we can conclude that since 5 is a prime number, a group G of order 5 is cyclic. A cyclic group is abelian so G is abelian. (Note that this same argument applies to groups of order 1,2 and 3). This shows that a group of order less than 6 is abelian.

(ii) Consider the two groups: $\mathbb{Z}/6$ and S_3, both of order 6. Claim: these groups are non-isomorphic. Proof: Suppose that there exists an isomorphism $f : S_3 \mapsto \mathbb{Z}/6$. This isomorphism must preserve the identity element, i.e., $f(id) = 0$. If we take $0 = f(id) = f((1\ 2)^2) = f((1\ 2) \circ (1\ 2)) = f((1\ 2)) + f((1\ 2)) = 2f((1\ 2)) \Rightarrow 0 = 2f((1\ 2)) \Rightarrow f((1\ 2)) = 0$ OR $f((1\ 2)) = 3$. Therefore, $f((1\ 2)) = 3$ since it cannot be the identity. If we perform the same calculations but with $(1\ 3)$ we will also obtain that $f((1\ 3)) = 3$ so that f is not injective, a contradiction. Therefore, there exists no such isomorphism f.