MATH-251: HOMEWORK 3

BLAKE FARMAN

1. *For each fixed non-zero $k \in \mathbb{Q}$, the map*

$$\varphi : \mathbb{Q} \to \mathbb{Q}$$

$$q \mapsto kq$$

is an automorphism of $\mathbb{Q}$.

Proof. Let $p, q \in \mathbb{Q}$ be distinct. Since k is fixed, by the left cancellation law $\varphi(p) = \varphi(q)$ only if $p = q$. Hence φ is injective.

To see that φ is surjective, let p be given and observe that there exists some $q \in \mathbb{Q}$ such that $\varphi(q) = p$. Since k is non-zero, take $q = \frac{p}{k}$. Then $\varphi(q) = p$. Therefore φ is a bijection.

It remains only to show that φ is a homomorphism. Let $p, q \in \mathbb{Q}$ be given. Then

$$\begin{aligned}\varphi(p+q) &= k(p+q) \\ &= kp + kq \\ &= \varphi(p) + \varphi(q).\end{aligned}$$

Therefore, φ is an automorphism of $\mathbb{Q}$. $\square$

2. *Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ do satisfy the axioms of a (left) group action.*

Proof. i) Let $g_1, g_2 \in G$ and $a \in A$ be given. Then

$$\begin{aligned}(g_1 g_2) \cdot a &= g_1 g_2 a (g_1 g_2)^{-1} \\ &= g_1 (g_2 a g_2^{-1}) g_1^{-1} \\ &= g_1 \cdot (g_2 \cdot a).\end{aligned}$$

Date: Friday, September 24, 2010.

ii) Let $a \in A$ be given. Since $A = G$, observe that $1a = a1 = a$ and $1^{-1} = 1$. So it follows that

$$\begin{aligned} 1 \cdot a &= 1a1^{-1} \\ &= 1a1 \\ &= a. \end{aligned}$$

□

3. *Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by*

$$x \mapsto gxg^{-1}.$$

For fixed $g \in G$, prove that conjugation by g is an automorphism of G. Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G, $|A| = |gAg^{-1}|$, where $gAg^{-1} = \{gag^{-1} \mid a \in A\}$.

Proof. Fix $g \in G$ and let φ be defined by

$$\varphi : G \to G$$

$$x \mapsto gxg^{-1}.$$

Let $\alpha, \beta \in G$ be distinct. Since g is fixed, by the cancellation laws $\varphi(\alpha) = \varphi(\beta)$ only if $\alpha = \beta$. Hence φ is injective.

Now let $\beta \in G$ be given. To see φ is surjective, observe that there exists some $\alpha \in G$ such that $\varphi(\alpha) = \beta$. Namely take $\alpha = g^{-1}\beta g$. Then $\varphi(\alpha) = \beta$. Therefore φ is a bijection.

It remains only to show that φ is a homomorphism. Let $\alpha, \beta \in G$ be given. Then

$$\begin{aligned} \varphi(\alpha\beta) &= g\alpha\beta g^{-1} \\ &= (g\alpha g^{-1})(g\beta g^{-1}) \\ &= \varphi(\alpha)\varphi(\beta). \end{aligned}$$

Therefore φ is an automorphism of G.

That $|A| = |gAg^{-1}|$ follows immediately from the bijective property of φ. To see x and gxg^{-1} have the same order for all x in G, let $n = |x|$ and consider $\varphi(x^n)$. From the previous homework set, $\varphi(x^n) = \varphi(x)^n$ implies $(gxg^{-1})^n = 1$ and thus

$|gxg^{-1}| \leq n$. Now suppose there exists some $k < n$ such that $(gxg^{-1})^k = 1$. Then

$$\begin{aligned} \varphi(x^k) &= (gxg^{-1})^k \\ &= 1 \\ &= \varphi(1). \end{aligned}$$

Since φ is injective, this implies $x^k = 1$. This is a contradiction. Therefore, x and gxg^{-1} have the same order. $\square$

4. *Show that the specified subset is or is not a subgroup of the given group.*

Proof. a)$H = \{a + ai \mid a \in \mathbb{R}\} \subseteq \mathbb{C}$. Let $a = \alpha + i\alpha, b = \beta + i\beta$ be given. Then $ab = (\alpha + \beta) + i(\alpha + \beta)$. Hence H is closed under addition. Furthermore, for any $a \in H$, its inverse $-a = (-\alpha) + i(-\alpha) \in H$ implies $H \leq \mathbb{C}$.

b) $H = \{\alpha + i\beta \mid \alpha^2 + \beta^2 = 1\} \subseteq \mathbb{C}$. Let $a = \alpha + i\beta, b = \gamma + i\delta$ be given. Then

$$\begin{aligned} |ab| &= (\alpha\gamma - \beta\delta)^2 + (\alpha\delta + \beta\gamma)^2 \\ &= (\alpha\gamma)^2 - 2\alpha\beta\gamma\delta + (\beta\delta)^2 + (\alpha\delta)^2 + 2\alpha\beta\gamma\delta + (\beta\gamma)^2 \\ &= \gamma^2(\alpha^2 + \beta^2) + \delta^2(\alpha^2 + \beta^2) \\ &= \gamma^2 + \delta^2 \\ &= 1. \end{aligned}$$

Hence H is closed under addition. So for any $a \in H$ consider $a^{-1} = \frac{\alpha - i\beta}{\alpha^2 + \beta^2}$. Then $a^{-1} = \bar{a} \in H$ implies H is closed under inverses. Therefore, $H \leq \mathbb{C}$.

c) $H = \{\frac{p}{q} \in \mathbb{Q} \mid (q, n) = q, \text{fixed } n \in \mathbb{Z}^+\} \subseteq \mathbb{Q}$. Let $x, y \in H$ be given. Then

$$x + y = \frac{p}{q} + \frac{r}{s} = \frac{ps + rq}{qs}.$$

If $qs \leq n$, then qs divides n. So, assume that $qs > n$. If this is the case, then it must be that there is some repeated factor of n, g $= (q, s) > 1$. Then

$$\frac{ps + rq}{qs} = \frac{gjp + gkr}{g^2jk}, \text{ for some } j, k \in \mathbb{Z}.$$

So the denominator becomes gjk, where g, j and k are all necessarily relatively prime factors of n and thus $gjk \leq n$. Therefore, H is closed under addition. Furthermore, for any $x \in H$, $x^{-1} = -x \in H$ implies that H is closed under inverses. Therefore, $H \leq \mathbb{Q}$.

d) $H = \{\frac{p}{q} \in \mathbb{Q} \mid (n,q) = 1, \text{fixed } n \in \mathbb{Z}^+\} \subseteq \mathbb{Q}$Let $x, y \in H$ be given. Then

$$x + y = \frac{p}{q} + \frac{r}{s} = \frac{ps + rq}{qs}.$$

Since $(q,n) = 1$ and $(s,n) = 1$, $(qs,n) = 1$ which implies $x + y \in H$. Hence H is closed under addition. Furthermore, for any $x \in H$, $x^{-1} = -x \in H$ implies H is closed under inverse. Therefore, $H \leq \mathbb{Q}$.

e) $H = \{a > 0 \in \mathbb{R} \mid a^2 \in \mathbb{Q}\} \subseteq \mathbb{R}$. Let $x, y \in H$ be given. Then since $\mathbb{Q}$ is closed under the commutiative multiplication operation, $(xy)^2 = x^2y^2 \in \mathbb{Q}$. Hence $xy \in H$ implies H is closed under multiplication. Furthermore, since each $x \in H$ is non-zero, it is invertible and its inverse $\frac{1}{x} \in H$. Therefore $H \leq \mathbb{R}$.

a) The set of 2-cycles in S_n for $n \geq 3$ is not closed under composition. Let $\sigma = (1 \quad 2)$ and let $\tau = (2 \quad 3)$. Then

$$\begin{aligned} \sigma\tau &= (1 \quad 2)(2 \quad 3) \\ &= (1 \quad 2 \quad 3). \end{aligned}$$

Therefore the set of 2-cycles in S_n for $n \geq 3$ is not a subgroup.

b) The set of reflections in D_{2n} for $n \geq 3$ is not closed under the group operation. Take s and sr^2 for example:

$$s(sr^2) = r^2.$$

Therefore the set of reflections in D_{2n} for $n \geq 3$ is not a subgroup.

c) $H = \{x \in G \mid |x| = n\} \cup \{1\} \subseteq G$. Let $x \in H$ be given. In order to be closed, x^2 must be an element of G. However, $(x^2)^{\frac{n}{2}} = 1$ implies that the order of x^2 is strictly less than n. Therefore H is not a subgroup of G.

d)$H = \{x \in \mathbb{Z} \mid x \equiv 1(2)\} \cup \{0\} \subseteq \mathbb{Z}$. Since the sum of any two odd integers is always even, H is not closed under addition. Therefore H is not a subgroup.

e)$H = \{x \in \mathbb{R} \mid x^2 \in \mathbb{Q}\} \subseteq \mathbb{R}^+$. Take the two elements $\sqrt(2), \sqrt(3) \in H$. The square of their sum is the irrational number

$$(\sqrt(2) + \sqrt(3))^2 = 2 + 2\sqrt(2)\sqrt(3) + 3.$$

Hence H is not a subgroup. $\square$

5. *Let A and B be groups. Prove that the following sets are subgroiups of the direct product $A \times B$:*

a)$\{(a,1) \mid a \in A\}$

b)$\{(1,b) \mid b \in B\}$

c)$\{(a,a) \mid a \in A\}$, *where here we assume $B = A$.*

Proof. Since A and B are both groups, for any two elements $(x_1, 1)$ and $(x_2, 1)$, $(1, y_1)$ and $(1, y_2)$ or (x_1, y_2) and (x_2, y_2) of the subsets, their respective products $(x_1x_2, 1), (1, y_1y_2), (x_1x_2, y_1y_2)$ are clearly an element of their respective subset. Hence the subsets are closed under addition.

Moreover, any such elements have inverses which are elements of their respective subsets, $(x, 1)^{-1} = (x^{-1}, 1)$, $(1, y)^{-1} = (1, y^{-1})$, and $(x, y)^{-1} = (x^{-1}, y^{-1})$. Therefore, all three sets are subgroups of $A \times B$. □

6 a). *Prove that if H and K are subgroups of G then so is their intersection, $H \cap K$.*

Proof. For any element $x \in H \cap K$, $x \in H$ and $x \in K$ by definition. Since H and K are both subgroups of G, $x^{-1} \in H$ and $x^{-1} \in K$ implies $H \cap K$ is closed under inverses.

Similarly, for any $x, y \in H \cap K$, $xy \in K$ and $xy \in H$ implies $H \cap K$ is closed under multiplication. Therefore $H \cap K$ is a subgroup of G. □

b). *Prove that the intersection of arbitrary non-empty subgroups of G is a subgroup.*

Proof. □

7. *Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.*

Proof. To show that $H \cup K \leq G$ implies $H \subseteq K$ or $K \subseteq H$, it suffices to show the contrapositive. So suppose it is not the case that $H \subseteq K$ or $K \subseteq H$. Then there exist elements of $H \cup K$, $x \in H$ and $y \in K$ such that $x, y \notin H \cap K$. Note then that

$$x^{-1}(xy) = y \notin H$$

implies $xy \notin H$. Furthermore,

$$(xy)y^{-1} = x \notin K$$

implies $xy \notin K$. Hence $H \cup K$ is not closed under multiplication. Therefore $H \cup K \leq G$ implies either $H \subseteq K$ or $K \subseteq H$.

Conversely, suppose without loss of generality that $H \subseteq K$. Then, by definition, for any $x, y \in H \cup K$, $x, y \in K$. Since K is a subgroup of G, $H \cup K$ is closed under multiplication and under inverses. Hence $H \cup K$ is a subgroup of G. Therefore, $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$. □