Imperial College London
Department of Mathematics

Solutions to Question Sheet 6 - Probl. Class week 9

MATH40003 Linear Algebra and Groups — Term 2, 2022/23

Problem sheet released on Monday of week 8. All questions can be attempted before the problem class on Monday of week 9. Solutions will be released after the problem class.

Question 1 Suppose $(G,\cdot)$ is a group and H is a subgroup of G. Prove that each of the following is an equivalence relation on G (where g,h are elements of G):

(i) $g \sim_1 h$ if and only if there is $k \in G$ with $h = kgk^{-1}$;

(ii) $g \sim_2 h$ if and only if $h^{-1}g \in H$.

In the case where $(G,.)$ is the group $(\mathbb{R}^2,+)$ and H is the subgroup $\{(x,x) \in \mathbb{R}^2 : x \in \mathbb{R}\}$, describe geometrically the $\sim_2$-equivalence classes. What are the $\sim_1$-equivalence classes?

Solution: (i) Clearly $g \sim_1 g$ (take $k = e$). If $g \sim_1 h$ take k with $kgk^{-1} = h$. Then $g = k^{-1}hk = k^{-1}h(k^{-1})^{-1}$. So $h \sim_1 g$. Finally if $g \sim_1 h$ and $h \sim_1 f$ take $k, j \in G$ with $h = kgk^{-1}$ and $f = jhj^{-1}$. So $f = jkgk^{-1}j^{-1} = (jk)g(jk)^{-1}$, so $g \sim_1 f$, as required.

(ii) $g \sim_2 g$ as $g^{-1}g = e \in H$. If $g \sim_2 h$ then $h^{-1}g \in H$, so $g^{-1}h = (h^{-1}g)^{-1} \in H$, whence $h \sim_2 g$. If $g \sim_2 h$ and $h \sim_2 f$ then $g^{-1}h, h^{-1}f \in H$. So taking the product, $g^{-1}f \in H$ and $g \sim_2 f$. (Note that each of the three things to be verified corresponds to one of the conditions in the test for a subgroup.)

In the example the equivalence class C containing a point $(a,b) \in \mathbb{R}^2$ has the property that $(c,d) \in C$ iff there is $(x,x) \in H$ with $(c,d) = (a,b) + (x,x)$. So we might write $C = (a,b) + H$. In other words, C is the line through (a,b) which is parallel to the line H.

This group is abelian (and written additively), so $g \sim_1 h$ iff there is k with $h = k + g - k = g$. So the $\sim_1$-classes are just sets of size 1 (i.e. $\sim_1$ is the equality relation!).

Question 2 Suppose $(G,\cdot)$ is a group and H,K are subgroups of G.

(i) Show that $H \cap K$ is a subgroup of G.

(ii) Show that if $H \cup K$ is a subgroup of G then either $H \subseteq K$ or $K \subseteq H$.

Solution: (i) Use the test from the notes. As $e \in H \cap K$ we have $H \cap K \neq \emptyset$. If $g,h \in H \cap K$ then $g,h \in H$, so $gh \in H$ as H is a subgroup. Similarly $gh \in K$, so $gh \in H \cap K$. Also $g^{-1} \in H$ as H is a subgroup and $g \in H$; similarly $g^{-1} \in K$. So $g^{-1} \in H \cap K$.

(ii) If not, there exist $h \in H \setminus K$ and $k \in K \setminus H$. We have $hk \in H \cup K$, so $hk \in H$ or $hk \in K$. In the first case we have $hk = h'$ for some $h' \in H$. Rearranging, we obtain $k = h'h^{-1}$. As $h, h' \in H$ and H is a subgroup, this means $k \in H$ contradicting how it was chosen. But also the case $hk \in K$ leads to a similar contradiction. Thus no such choice of h,k is possible: we have either $H \subseteq K$ or $K \subseteq H$.

Question 3 Which of the following groups are cyclic?

(a) S_2.

(b) $\mathrm{GL}(2,\mathbb{R})$.

(c) $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a,b \in \{1,-1\} \right\}$ under matrix multiplication.

(d) $(\mathbb{Q},+)$.

Solution:

(a) Yes. It is $\langle g \rangle$, where $g = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

(b) No. $\mathrm{GL}(2,\mathbb{R})$ is not abelian, so it cannot be cyclic.

(c) No. Every element has order 1 or 2, so they all generate proper cyclic subgroups.

(d) No. Suppose $\frac{p}{q}$ is a generator, in lowest terms. All of the powers of this generator have the form $\frac{np}{q}$ for $n \in \mathbb{Z}$. But such an element has denominator at most q, and this is a contradiction (since $\mathbb{Q}$ has elements with denominators greater than q).

Question 4 Let G and H be finite groups. Let $G \times H$ be the set $\{(g,h) \mid g \in G, h \in H\}$ with the binary operation $(g_1,h_1) * (g_2,h_2) = (g_1g_2, h_1h_2)$.

(a) Show that $(G \times H, *)$ is a group.

(b) Show that if $g \in G$ and $h \in H$ have orders a,b respectively, then the order of (g,h) in $G \times H$ is the lowest common multiple of a and b.

(c) Show that if G and H are both cyclic, and $\gcd(|G|,|H|) = 1$, then $G \times H$ is cyclic. Is the converse true?

Solution:

(a) Easy; just check the group axioms. The identity is (e_G, e_H).

(b) We have $(g,h)^t = (g^t, h^t)$. Now

$$\begin{aligned}(g^t,h^t) = (e_G,e_H) &\iff a \text{ divides } t \text{ and } b \text{ divides } t \\ &\iff \mathrm{lcm}(a,b) \text{ divides } t.\end{aligned}$$

So $\mathrm{ord}(g,h)$ is $\mathrm{lcm}(a,b)$.

(c) Let $|G| = m$ and $|H| = n$. Since $G \times H$ has order mn, it is cyclic if and only if there exists an element (g,h) with order mn. Let $g \in G$ have order m and $h \in H$ have order n. By (b), (g,h) has order mn, so $G \times H$ is cyclic. The converse is also true. That is, if $G \times H$ is cyclic then G and H are cyclic and have coprime order. Assume $G \times H$ is cyclic and let (g,h) be a generator of $G \times H$. Then, since $G \times H$ has order mn, $o(g,h) = mn$. Let $a = o(g)$ and $b = o(h)$. We show that $a = m$, $b = n$ and $gcd(a,b) = 1$. By Theorem 2.2 (consequence of Lagrange), $a \mid m = |G|$ and $b \mid n = |H|$, in particular $a \leq m$ and $b \leq n$. Moreover, by (b), $mn = o(g,h) = lcm(a,b)$. This implies that $a = m$ and $b = n$ (if $a < n$ or $b < n$, then $lcm(a,b) \leq ab < mn$). Now we see that $lcm(a,b) = ab$ and therefore a and b are coprime.

Let $(g,h) \in G \times H$ have order mn and suppose g has order a and h has order b. Then a divides m and b divides m and $lcm(a,b)$ is equal to mn (by (b)). It follows that $a = m$ and $b = n$ and m,n are coprime.

Question 5 Find an example of each of the following:

(a) an element of order 3 in the group $\mathrm{GL}(2, \mathbb{C})$.

(b) an element of order 3 in the group $\mathrm{GL}(2, \mathbb{R})$.

(c) an element of infinite order in the group $\mathrm{GL}(2, \mathbb{R})$.

(d) an element of order 12 in the group S_7.

Solution:

(a) E.g. $\begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$, where $\omega = \mathrm{e}^{2\pi \mathrm{i}/3}$, or as in (b).

(b) E.g. $\begin{pmatrix} \cos 2\pi/3 & \sin 2\pi/3 \\ -\sin 2\pi/3 & \cos 2\pi/3 \end{pmatrix}$.

(c) E.g. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(d) E.g. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 7 & 5 \end{pmatrix}$, or $(1234)(567)$ in cycle notation.

Question 6 Prove that if $\{x_1, \ldots, x_n\}$ is any finite subset of $(\mathbb{Q}, +)$, then the subgroup $\langle x_1, \ldots, x_n \rangle$ is cyclic.

Solution: Let $d_1, \ldots, d_n$ be the denominators when $x_1, \ldots, x_n$ are expressed in lowest terms. Then each of $x_1, \ldots, x_n$ is in the cyclic subgroup generated by $1/\ell$, where ℓ is $\mathrm{lcm}(d_1, \ldots, d_n)$. So $\langle x_1, \ldots, x_n \rangle$ is a subgroup of the cyclic group $\langle 1/\ell \rangle$ and is therefore cyclic (theorem in notes).