THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 3 Solutions
8th February 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

Compulsory Part

1. (a) Yes. Let $ia, ib \in i\mathbb{R}$ where $a, b \in \mathbb{R}$, then $ia + (ib)^{-1} = ia + (-ib) = i(a-b) \in i\mathbb{R}$.

   (b) Yes, let z_1, z_2 be m-th roots of unity, then $z_1^m = z_2^m = 1$. Consider $(z_1 z_2^{-1})^m = z_1^m / z_2^m = 1$, so $z_1 z_2^{-1}$ is again an m-th root of unity.

   (c) No. Let $A, B \in GL(n, \mathbb{R})$ be matrices with determinant -1, then $\det(AB) = \det(A)\det(B) = (-1)^2 = 1$. So the set of matrices with determinant 1 is not closed under multiplication, therefore would not form a subgroup.

   (d) Yes, let $A, B \in \{M \in GL(n, \mathbb{R}) : M^T M = I\}$, then for the matrix AB^{-1}, consider $(AB^{-1})^T(AB^{-1}) = (B^{-1})^T A^T A B^{-1} = (B^{-1})^T B^{-1} = (B^T)^{-1} B^{-1} = (BB^T)^{-1} = I$. Here, we have used the facts that the inverse of tranpose is equal to the transpose of inverse, and that left inverse is equal to right inverse. The above calculation shows that $M = AB^{-1}$ satisfies $M^T M = I$, so it is closed under matrix multiplication.

2. (a) The generators of $\mathbb{Z}_{20}$ consists of those numbers that are coprime to 20, so they are $1, 3, 7, 9, 11, 13, 17$ and 19.

   (b) Recall that any subgroups of a cyclic group is cyclic, so it is of the form $\langle k \rangle$. By proposition 3.2.6, the subgroup $\langle k \rangle$ only depends on $\gcd(k, 20)$. The possible gcds are $1, 2, 4, 5, 10, 20$.

   For $\gcd(k, 20) = 1$, we get the subgroup $\mathbb{Z}_{20}$, this is described in part (a).

   For $\gcd(k, 20) = 2$, we get $\langle 2 \rangle \cong \mathbb{Z}_{10} \leq Z_{20}$. The generators are $2, 6, 10, 14, 18$.

   For $\gcd(k, 20) = 4$, we get $\langle 4 \rangle \cong \mathbb{Z}_5 \leq \mathbb{Z}_{20}$. The generators are $4, 8, 12, 16$.

   For $\gcd(k, 20) = 5$, we get $\langle 5 \rangle \cong \mathbb{Z}_4 \leq \mathbb{Z}_{20}$. The generators are $5, 15$.

   For $\gcd(k, 20) = 10$, we get $\langle 10 \rangle \cong \mathbb{Z}_2 \leq \mathbb{Z}_{20}$. The generator is 10.

   For $\gcd(k, 20) = 20$, we get $\langle 0 \rangle = \{e\} \leq \mathbb{Z}_{20}$. The generator is 0.

3. Since H is a subgroup of G if and only if it is closed under multiplication and closed under taking inverse. It suffices to prove that when H is finite, closedness under multiplication implies closedness under taking inverse. Let $a \in H$ be an element, then since H is closed under multiplication, the subset $\{a^n : n \in \mathbb{Z}_{>0}\} \subset H$ and is finite. Therefore by pigeonhole principle, there are $i > j$ such that $a^j = a^i$, thus $a^{i-j} = e$, i.e. a has finite order, say $|a| = m$. Then $a^{m-1} = a^m a^{-1} = a^{-1}$, thus $a^{-1} \in \{a^n : n \in \mathbb{Z}_{>0}\} \subset H$. We have shown that H is closed under taking inverse, so it is a subgroup.

4. Denote $HK := \{hk : h \in H, k \in K\}$. It suffices to prove that for any $h_1k_1, h_2k_2 \in HK$, we have $(h_1k_1)(h_2k_2)^{-1} \in HK$. This is clear because G is abelian, we have $(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_2^{-1}k_1k_2^{-1}$, since H, K are subgroups, $h_1h_2^{-1} \in H$ and $k_1k_2^{-1} \in K$. So that $(h_1k_1)(h_2k_2)^{-1} = h_1h_2^{-1}k_1k_2^{-1} \in HK$ as desired.

   For a counter-example of the statement in the case when G is non-abelian, consider $G = D_3 = \{e, r, r^2, s, sr, sr^2\}$ and take $H = \{e, s\}$, $K = \{e, rs\}$. Then $HK = \{e, s, rs, srs\}$, here $srs = r^{-1}ss = r^{-1} = r^2$. Note that $(rs)s = r \notin HK$, so it is not a subgroup.

5. See solution to Tutorial 4 Q1.

6. Let $a, b \in H$, then a, b have finite orders, say $|a| = m$ and $|b| = n$. We have $(ab^{-1})^{mn} = a^{mn}(b^{mn})^{-1} = e$, where in the first equality we have used the fact that G is abelian. So ab^{-1} has order at most mn, which is finite, i.e. $ab^{-1} \in H$. This subgroup H is called the torsion subgroup of G.

Optional Part

1. (a) Yes. Let $r, s \in \mathbb{Q}$, and consider $er, es \in e\mathbb{Q}$. Then $(er) + (es)^{-1} = er - es = e(r - s) \in e\mathbb{Q}$. So $e\mathbb{Q}$ is a subgroup.

   (b) No. $\pi + \pi^2$ is not equal to π^k for any $k \in \mathbb{Z}$, therefore the subset $\{\pi^n : n \in \mathbb{Z}\}$ is not closed under group operation, so it is not a subgroup.

   (c) Yes. Write the set as

   $$H = \left\{ \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix} \in GL(n, \mathbb{R}) : \lambda_1, ..., \lambda_n \neq 0 \right\}.$$

   Denote the diagonal matrix as $\mathrm{diag}(\lambda_1, ..., \lambda_n)$. Then for $A, B \in H$, write $A = \mathrm{diag}(\lambda_1, ..., \lambda_n)$ and $B = \mathrm{diag}(\eta_1, ..., \eta_n)$, we have $AB^{-1} = \mathrm{diag}(\lambda_1\eta_1^{-1}, ..., \lambda_n\eta_n^{-1})$. Therefore $AB^{-1} \in H$, since each of $\lambda_1\eta_1^{-1}, ..., \lambda_n\eta_n^{-1}$ are non-zero.

   (d) Yes. Let H be the set of matrices with determinant ± 1. Let $A, B \in H$, then $\det(AB^{-1}) = \det(A)\det(B)^{-1}$ is either 1 or -1, so $AB^{-1} \in H$ again.

2. We may write $S_3 = \{e, (12), (13), (23), (123), (132)\}$. The identity e is conventionally defined as the empty product. First note that $(132) = (123)^2$. We have $(123)(12) = (13)$. Therefore we also have $(23) = (12)(13)(12) = (12)(123)$.

   Try to interpret the above in terms of $D_3 = \langle r, s \rangle$. There is an isomorphism $D_3 \cong S_3$, where $r \leftrightarrow (123)$ and $s \leftrightarrow (12)$.

3. A subgroup of order 5 and 3 are in particular groups of prime orders. So they must be cyclic. Thus we can start by considering elements of order 5 and 3 respectively.

   By tutorial 2 Q3, elements of order 5 in S_6 are precisely the 5-cycles, by tutorial 2 Q1c, there are $6!/5 = 144$ many 5-cycles. Each 5-cycle generates a subgroup of order 5 in S_6 but they need not be distinct. As each subgroup has exactly 4 generators (there are 4

numbers in $\{0,1,2,3,4\}$ that are coprime to 5.) There are $144/4 = 36$ distinct subgroups of order 5.

Similarly, the elements of order 3 in S_6 are either 3-cycles or $(3,3)-cycles$ (i.e. cycles of the form $(abc)(def)$.) There are $6!/(3!\cdot 3) = 40$ many 3-cycles and $6!/(3^2\cdot 2!) = 40$ many $(3,3)$-cycles in S_6. Each element generates a subgroup of order 3, but similar to above, they are double-counted, because the group $\mathbb{Z}_3$ has exactly 2 generators. So in total there are $(40+40)/2 = 40$ many subgroups of order 3.

4. Consider $H = \langle (12),(34)\rangle = \{e,(12),(34),(12)(34)\} \leq S_4$. It has order 4 and is not cyclic since $(12)^2 = (34)^2 = (12)^2(34)^2 = e$.

5. (a) If n is odd, consider $H = \langle r^2, s\rangle$. Write $n = 2k-1$, then $(r^2)^k = r^{2k} = r \in H$, therefore $D_n = \langle r,s\rangle \leq H$. So $H = D_n$ and $|H| = 2n$.

   (b) If n is even, write $n = 2k$, since $D_n = \{e,r,r^2,...,r^{2k-1},s,sr,...,sr^{2k-1}\}$. It is obvious that $\{e,r^2,r^4,...,r^{2k-2},s,sr^2,...,sr^{2k-2}\} \subset \langle r^2,s\rangle$. On the other hand, a general element in $\langle r^2,s\rangle$ is a product of s and r^{2i}. In D_n, we have the relation $r^2 s = sr^{-2}$. In particular, given a general element in $\langle r^2,s\rangle$, we can move all of the r^{2i}'s together, so that it has the form $r^{\sum_j 2i_j}s^l$, now s^l is either s or e, and $r^{\sum_j 2i_j}$ is an even power of r. This shows that the element lies in $\{e,r^2,r^4,...,r^{2k-2},s,sr^2,...,sr^{2k-2}\}$. So $|\langle r^2,s\rangle| = n$.

6. See the solution to Tutorial 3 Q10.