Prof. Alexandru Suciu

MATH 3175 **Group Theory** **Spring 2024**

Solutions to the Midterm Exam

---

1. Let G be an abelian group with identity e, and let H be the set of all elements $a \in G$ that satisfy the equation $a^2 = e$. Prove that H is a subgroup of G.

- Let $a, b \in H$, so that $a^2 = e$ and $b^2 = e$. Then
$$(ab)^2 = abab = a(ba)b = a(ab)b = (aa)(bb) = ee = e,$$
where we used the fact that multiplication in G is both associative and commutative. Thus, $ab \in H$.
- Let $a \in H$. Then $a \cdot a = a^2 = e$; thus, $a^{-1} = a$, and so $a^{-1} \in H$.

This shows that H is a subgroup of G.

Remark: The assumption that G is an *abelian* group is essential for this to be true. For example, if $G = S_3$, then $H = \{(), (12), (13), (23)\}$, and this subset of G is not a subgroup, since, for instance, $|H| = 4$ does not divide $|G| = 6$.

2. Let $G = \langle a \rangle$ be a group generated by an element a of order 20.

(i) Find all elements of G which generate G.

The cyclic group G consists of all elements of the form a^k, with $0 \le k \le 19$. The generators of G are those elements of the form a^k, with $0 \le k \le 19$ and $\gcd(k, 20) = 1$. Thus, the set of generators of G is $\{a, a^3, a^7, a^9, a^{11}, a^{13}, a^{17}, a^{19}\}$, or, more succintly, $\{a^{\pm 1}, a^{\pm 3}, a^{\pm 7}, a^{\pm 9}\}$.

(ii) List all the elements in the subgroup $\langle a^5 \rangle$, together with their respective orders.

The cyclic subgroup $\langle a^5 \rangle$ consists of the elements e, a^5, a^{10}, a^{15}; their respective orders are $1, 4, 2, 4$.

(iii) What are the generators of the subgroup $\langle a^5 \rangle$?

a^5 and a^{15}.

(iv) Find an element in G that has order 4. Does this element generate G?

a^5 has order 4; it is not a generator of G.

3. Let $G = \mathrm{GL}(2, 2)$ be the group of all invertible 2×2 matrices with entries in $\mathbb{Z}_2$, with group operation given my matrix multiplication.

(i) List all the elements of G and find their orders.

The invertible 2×2 matrices with entries in $\mathbb{Z}_2 = \{0, 1\}$ are those which have non-zero determinant; in this case, those matrices with determinant equal to 1:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

The orders of these matrices are: $1, 2, 2, 2, 3, 3$.

(ii) Does G contain a subgroup of order 3? Why, or why not?

Yes, the cyclic subgroup of order 3 generated by any of the two matrices of order 3:

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

(iii) Is G an abelian group? Why, or why not?

No, G is not an abelian group, since it contains pairs of elements that do not commute (that is, $a, b \in G$ such that $ab \neq ba$). For instance:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{but} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

4. Let $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ be the multiplicative group of positive real numbers. Consider the map $f : \mathbb{R}^+ \to \mathbb{R}^+$ given by $f(x) = \sqrt{x}$.

(i) Show that f is an homomorphism.

For all $x_1, x_2 \in \mathbb{R}^+$, we have: $f(x_1x_2) = \sqrt{x_1x_2} = \sqrt{x_1}\sqrt{x_2} = f(x_1)f(x_2)$.

(ii) What is the kernel of f?

$\ker(f) = \{x \in \mathbb{R}^+ : f(x) = 1\} = \{x \in \mathbb{R} : x > 0 \text{ and } \sqrt{x} = 1\} = \{1\}$.

(iii) What is the image of f? For each $y \in \operatorname{im}(f)$ find an $x \in \mathbb{R}^+$ such that $f(x) = y$.

$\operatorname{im}(f) = \{y \in \mathbb{R}^+ : \exists x \in \mathbb{R}^+ \text{ such that } \sqrt{x} = y\} = \mathbb{R}^+$. Indeed, if $y \in \mathbb{R}^+$, take $x = y^2 \in \mathbb{R}^+$; then $f(x) = f(y^2) = \sqrt{y^2} = y$.

(iv) Show that f is an isomorphism, and find the inverse isomorphism.

The map f is injective: if $x_1, x_2 \in \mathbb{R}^+$ are such that $f(x_1) = f(x_2)$, then $f(x_1x_2^{-1}) = f(x_1)f(x_2)^{-1} = 1$, and so, by part (1), $x_1x_2^{-1} = 1$, i.e., $x_1 = x_2$.

The map f is also surjective, by part (2). Thus, f is a bijection. Moreover, by part (1), f is a homomorphism. Therefore, f is an isomorphism.

The inverse of f is the isomorphism $f^{-1} : \mathbb{R}^+ \to \mathbb{R}^+$ given by $f^{-1}(y) = y^2$.

5. List *all* the homomorphisms from the cyclic group of order 4 to itself. For each such homomorphism, $f : \mathbb{Z}_4 \to \mathbb{Z}_4$, indicate what the image of f and the kernel of f are (that is, list the elements of $\operatorname{im}(f)$ and $\ker(f)$).

Since the domain of f is a cyclic group (the group $\mathbb{Z}_4 = \langle 1 \rangle$), the homomorphism f is determined by the value $f(1)$ it assigns to the chosen generator of $\mathbb{Z}_4$. There are 4 such values (as many elements in the codomain, $\mathbb{Z}_4$). Therefore, there are 4 possibilities:

- $f(1) = 0$ and thus $f(x) = 0$ for all $x \in \mathbb{Z}_4$ (the trivial homomorphism). The kernel is $\mathbb{Z}_4$, the image is $\{0\}$.
- $f(1) = 1$ and thus $f(x) = x$ for all $x \in \mathbb{Z}_4$ (the identity homomorphism). The kernel is $\{0\}$, the image is $\mathbb{Z}_4$.
- $f(1) = 2$ and thus $f(x) = 2x$ for all $x \in \mathbb{Z}_4$. The kernel is $\{0, 2\}$, the image is $\{0, 2\}$.
- $f(1) = 3$ and thus $f(x) = 3x$ for all $x \in \mathbb{Z}_4$. The kernel is $\{0\}$, the image is $\mathbb{Z}_4$.

6. Let $\mathbb{Z}_n^\times$ be the group of units in the ring $\mathbb{Z}_n$, let Q_8 be the quaternion group of order 8, let D_n be the dihedral group of order $2n$, and let S_n be the group of permutations of $\{1, \dots, n\}$. Show that the following pairs of groups are *not* isomorphic. In each case, explain why.

(i) $\mathbb{Z}_{15}^\times$ and $\mathbb{Z}_8$.

Both groups are abelian of size 8, but $\mathbb{Z}_{15}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is not cyclic (its elements have orders $1, 4, 2, 4, 4, 2, 4, 2$, respectively, so no element of order 8), whereas $\mathbb{Z}_8$ is cyclic. Therefore, the two groups are not isomorphic.

(ii) Q_8 and D_4.

Both groups are non-abelian of size 8 and all their elements have order $1, 2$ or 4, but Q_8 has 6 elements of order 4, whereas D_4 has only 2 elements of order 4. Since isomorphisms must preserve the orders of elements, the two groups are not isomorphic.

(iii) $Q_8 \times \mathbb{Z}_3$ and $S_3 \times \mathbb{Z}_4$.

Both groups are non-abelian of size 24, and all their elements have order $1, 2, 3, 4$, or 12, but again not the same number of each type; e.g., $Q_8 \times \mathbb{Z}_3$ had 6 elements of order 12 (namely, $(\pm i, \pm 1), (\pm j, \pm 1), (\pm k, \pm 1)$), whereas $S_3 \times \mathbb{Z}_4$ has only 4 elements of order 12 (namely, $((1, 2, 3), \pm 1)$ and $((1, 3, 2), \pm 1)$). Therefore, the two groups are not isomorphic.

7. Let G be a finite group, H a subgroup of G, and K a subgroup of H.

(i) Show that $[G : K] = [G : H] \cdot [H : K]$.

By Lagrange's Theorem the index of the subgroup $H \leq G$ is given by $[G : H] = |G| \,/\, |H|$. Hence,

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H] \cdot [H : K].$$

(ii) Suppose $|K| = 10$ and $|G| = 240$. What are the possible values for $|H|$?

By Lagrange's Theorem, the order of H is divisible by $|K| = 10 = 2 \cdot 5$ and divides $|G| = 240 = 2^4 \cdot 3 \cdot 5$. Hence,

$$|H| \in \{10, 20, 30, 40, 60, 80, 120, 240\}.$$

8. Let $D_3 = \langle a, b \mid a^3 = b^2 = 1, ba = a^{-1}b \rangle$ be the dihedral group of order 6.

(i) Let $H = \langle a \rangle$ be the cyclic subgroup generated by a. Write down all the right cosets and all the left cosets of H in D_3. Is H a normal subgroup?

Right cosets of H in G:

$$H = \{1, a, a^2\}$$
$$Hb = \{b, ab, a^2b\}$$

Left cosets of H in G:

$$H = \{1, a, a^2, a^3\}$$
$$bH = \{b, ba, ba^2\}$$

Yes, H is a normal subgroup of G. Indeed, since $ba = a^2b$ and $ba^2 = ab$, we have that $bH = Hb$, and of course $H = H$, thus showing that the left and right cosets of H coincide. Alternatively, one may note that $bH = Hb = G \setminus H$, an argument which shows that any index 2 subgroup of an arbitrary group G is normal.

(ii) Let $K = \langle b \rangle$ be the cyclic subgroup generated by b. Write down all the right cosets and all the left cosets of K in D_3. Is K a normal subgroup?

Right cosets of K in G:

$$K = \{1, b\}$$
$$Ka = \{a, ba\}$$
$$Ka^2 = \{a^2, ba^2\}$$

Left cosets of K in G:

$$K = \{1, b\}$$
$$aK = \{a, ab\}$$
$$a^2K = \{a^2, a^2b\}$$

No, K is not a normal subgroup of G. Indeed, $Ka \neq aK$, since $ba \neq ab$. Alternatively, $aba^{-1} = a^2b \notin K$, although $b \in K$.