Prof. Alexandru Suciu

MATH 3175 **Group Theory** **Summer 2, 2022**

Solutions to Midterm Exam

---

1. Prove the following statements.

(i) All cyclic groups are abelian.

Let $G = \langle a \rangle = \{a^s \mid s \in \mathbb{Z}\}$ be a cyclic group. Then $a^s \cdot a^t = a^{s+t} = a^t \cdot a^s$ for all $s, t \in \mathbb{Z}$. Thus, G is abelian.

(ii) All groups of prime order are cyclic.

Let G be a group of order p, where p is a prime. If G is trivial, then $G = \langle e \rangle$ and we are done. Otherwise, there is $a \in G$ with $a \neq e$. Set $k = \operatorname{ord} a$. Then $k \neq 1$ (since $a \neq e$) and $k \mid p$ (by Lagrange's theorem). Since p is prime, this implies $k = p$, and so $G = \langle a \rangle = \{e, a, \dots, a^{p-1}\}$.

(iii) Any two cyclic groups of the same size are isomorphic.

Let $G = \langle a \rangle = \{a^s \mid s \in \mathbb{Z}\}$ and $H = \langle b \rangle = \{b^s \mid s \in \mathbb{Z}\}$ be two cyclic groups of the same size. Then the map $\varphi\colon G \to H$, $a^s \mapsto b^s$ is an isomorphism. Indeed, $\varphi(a^s a^t) = \varphi(a^s)\varphi(a^t)$, and so φ is a homomorphism, and since the groups are both infinite or both finite (of the same order), the map φ is a bijection (with inverse $\varphi^{-1}\colon H \to G$, $b^s \mapsto a^s$).

2. 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.

There are $2^4 = 16$ matrices of size 2×2 with entries in $\mathbb{Z}_2 = \{0, 1\}$; of those, 6 have determinant 1, and thus belong to G; the remaining 8 have determinant 0, and thus do not belong to G. Explicitly,

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

Their respective orders are: $\{1, 2, 2, 2, 3, 3\}$.

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

Yes, the subgroup generated by one of the matrices of order 3, say, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.

(iii) Is G a cyclic group? Why, or why not?

No, since it has no elements of order 6.

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

No, since $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, is different from $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

3. Consider the cyclic group $\mathbb{Z}_8 = \{[0]_8, \dots, [7]_8\}$ and the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. For each of these two groups:

(i) List all the subgroups, and display the information as a lattice of subgroups.

Subgroups of $\mathbb{Z}_8$: $\{0\}$, $\{0, 4\}$, $\{0, 2, 4, 6\}$, $\mathbb{Z}_8$.

Subgroups of $\mathbb{Q}_8$: $\{1\}$, $\{\pm 1\}$, $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, $\{\pm 1, \pm k\}$, $\mathbb{Q}_8$.

(ii) In each case, how many *distinct* subgroups are there?

$\mathbb{Z}_8$ has 4 subgroups, while Q_8 has 6 subgroups.

(iii) In each case, how many *isomorphism classes* of subgroups are there?

There are 4 isomorphism classes of subgroups of $\mathbb{Z}_8$; up to isomorphism, those subgroups are: $\{0\}$, $\mathbb{Z}_2$, $\mathbb{Z}_4$, and $\mathbb{Z}_8$.

There are 4 isomorphism classes of subgroups of $\mathbb{Q}_8$; up to isomorphism, those subgroups are: $\{0\}$, $\mathbb{Z}_2$, $\mathbb{Z}_4$, and Q_8.

(iv) In each case, how many *cyclic* subgroups are there?

$\mathbb{Z}_8$ has 4 cyclic subgroups (all subgroups of a cyclic group are cyclic!), while Q_8 has 5 cyclic subgroups (which fall into 3 isomorphism classes).

4. Let G be a group, and let $H \leq G$ be a subgroup.

(i) Show that, for every element $a \in G$, the right coset Ha coincides (up to inversion in G) with the left coset $a^{-1}H$.

$$g \in Ha \iff ga^{-1} \in H \iff (ga^{-1})^{-1} \in H \iff ag^{-1} \in H \iff g^{-1} \in a^{-1}H.$$

(ii) Use part (i) to construct a bijection between the set of right cosets of H and the set of left cosets of H.

By part (i), the inversion map $G \to G$, $g \mapsto g^{-1}$ (which is a bijection) induces a bijection

$$\{\text{right cosets of } H \text{ in } G\} \to \{\text{left cosets of } H \text{ in } G\}$$

given by $Ha \mapsto a^{-1}H$; its inverse is given by $aH \mapsto Ha^{-1}$.

(iii) Assume now that G is finite. Use part (ii) to show that the number of left cosets of H is equal to the number of right cosets of H.

Since the sets of right and left cosets are in bijection (by part (ii)), and since they are both finite sets (since G is finite), the two sets must have the same number of elements.

5. Let $\mathbb{C}^\times$ be the multiplicative group of non-zero complex numbers, and let $T = \{z \in \mathbb{C}^\times : |z| = 1\}$ be the subset of complex numbers with absolute value equal to 1.

(i) Show that T is a subgroup of $\mathbb{C}^\times$.

First note that $|zw| = |z| \cdot |w|$, and so $|z^{-1}| = |z|$, for every $z, w \in \mathbb{C}^\times$. Thus, if $z, w \in T$, that is, $|z| = |w| = 1$, then

$$\left|zw^{-1}\right| = |z| \cdot \left|w^{-1}\right| = |z| \cdot |w| = 1 \cdot 1 = 1.$$

(ii) Sketch T in the x-y plane (where recall $z = x + iy \in \mathbb{C}$ corresponds to the point in $\mathbb{R}^2$ with coordinates (x, y).)

Since $|z| = \sqrt{x^2 + y^2}$, we have that $T = \{(x, y) \mid x^2 + y^2 = 1\}$ is the unit circle in the plane.

(iii) Describe the (right) cosets of T in geometric terms and sketch at least 4 of these cosets, labelling each one accordingly.

The right cosets of T are of the form $T \cdot r = \{z \in \mathbb{C}^\times \mid |z| = r\}$ for all r real, $r > 0$. That is, they are concentric circles of arbitrary positive radius r.

6. Let G be a group of order 21. Suppose that G has precisely one subgroup of order 3, and one subgroup of order 7. Show that G is cyclic.

Let H be the unique subgroup of order 3 and K the unique subgroup of order 7. Then $|H \cup K| \leq |H| + |K| - |\{e\}| = 3 + 7 - 1 = 9$. [In fact, $H \cap K$ is the trivial subgroup, since any nontrivial element of H must have order 3, and any non-trivial element of K must have order 7; thus, $|H \cup K| = 9$.] Therefore, there must be an element $g \in G \setminus (H \cup K)$. Note that

- $|g| \neq 1$, since $g \neq e$.
- $|g| \neq 3$, since otherwise $\langle g \rangle$ would be a subgroup of order 3 distinct from H.
- $|g| \neq 7$, since otherwise $\langle g \rangle$ would be a subgroup of order 7 distinct from K.

On the other hand, we know from Lagrange's theorem that $\operatorname{ord}(g)$ divides $|G| = 21$. Hence, we must have $\operatorname{ord}(g) = 21$, and so $G = \langle g \rangle$ is cyclic.

7. Let $\varphi\colon G \to H$ be a homomorphism. Prove the following:

(i) If φ is injective, then $|G|$ divides $|H|$.

Since the problem asks about divisibility of orders, the groups G and H must be finite. In general, we know that $\operatorname{im}(\varphi) \coloneqq \varphi(G)$ is always a subgroup of H, and that the co-restriction $\varphi\colon G \to \operatorname{im}(\varphi)$ is a surjective homomorphism. Now, since φ is assumed to be injective, the map $\varphi\colon G \to \operatorname{im}(\varphi)$ is an isomorphism. Consequently, $|G| = |\operatorname{im}(\varphi)|$. But, by Lagrange's theorem, $|\operatorname{im}(\varphi)|$ must divide $|H|$, and so $|G| \mid |H|$.

(ii) If φ is surjective, and G is abelian, then H is also abelian.

Let $h_1, h_2 \in H$. Then, by surjectivity of φ, there exist $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Hence, since φ is a homomorphism and G is abelian, we have:

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) = \varphi(g_2 g_1) = \varphi(g_2)\varphi(g_1) = h_2 h_1.$$

(iii) If φ is surjective, and G is cyclic, then H is also cyclic.

Suppose $G = \langle a \rangle$, and let $b = \varphi(a)$. Then, since φ is a surjective homomorphism, we have that $H = \langle b \rangle$. Indeed, if $h \in H$, then $h = \varphi(g)$ for some $g \in G$; but $g = a^s$ for some $s \in \mathbb{Z}$, and so $h = \varphi(a^s) = \varphi(a)^s = b^s$, and so $h \in \langle b \rangle$.

8. For each of the following pairs of groups, decide whether they are isomorphic or not. In each case, give a brief reason why.

(i) $\mathbb{Z}_9^\times$ and $\mathbb{Z}_8$.

No: $\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$ has order $\phi(9) = 6$, which is different from $|\mathbb{Z}_8| = 8$.

(ii) $\mathbb{Z}_{16}^\times$ and $\mathbb{Z}_8$.

No: Both $\mathbb{Z}_{16}^\times = \{1, 3, 5, 7, 9, 11, 13, 15\}$ have the same order (8), but $\mathbb{Z}_{16}^\times$ is not cyclic (it has no element of order 8), whereas $\mathbb{Z}_8$ is cyclic.

(iii) $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_6$.

Yes: The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic of order 6, generated by $([1]_2, [1]_3)$, and so the map $\varphi\colon \mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6$, $([1]_2, [1]_3) \mapsto [1]_6$ is an isomorphism.

(iv) $\mathbb{Z}_2 \times \mathbb{Z}_8$ and $\mathbb{Z}_4 \times \mathbb{Z}_4$.

No: Both groups are abelian and have the same order (16), but the first has elements of order 8 (for instance, $([0]_2, [1]_8)$), whereas the second has no such elements (all its elements have order 1, 2, or 4).