Revision Session

MAU22101 — Group Theory

Note. These are short notes to help you study for you upcoming exam. It contains blank spaces which you should fill in. Attempt all exercises! Solutions will be discussed during the revision session on January 6th.

---

1 Basic definitions

A *group* is a set G endowed with a binary operation $G \times G \longrightarrow G$, usually called a product, which we usually denote $(g,h) \longmapsto$_____(juxtaposition), that satisfies the following three axioms.

1. _____. There exists an element $e \in G$ such that for every $g \in G$, we have_____.
2. _____. For each $g \in G$ there exists another element g' such that_____$= e$. We call this the_____of g.
3. _____. For every three elements $g,h,k \in G$, we have that_____=_____.

Let us fix a group G. We say an element $g \in G$ has finite order if there exists some positive integer N for which $g^N = e$. The *order of* g is the_____and we denote it by $|g|$. If no such integer exists, we say that g has infinite order.
For example, the set of non-zero rational numbers $\mathbb{Q}^\times$ is a group under multiplication with identity 1. The only elements of finite order are 1 and -1. The integers $\mathbb{Z}$ under addition form a group, they contain no element of finite order. A group is *abelian* if for each $g,h \in G$ we have that_____=_____, in which case we say g and h_____. When G is abelian, we usually use additive notation as opposed to multiplicative notation, and write the product gh as $g+h$. A group G is cyclic if there exists an element $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\} := \langle g \rangle$, that is, every element of G is the power of a fixed element $g \in G$. Note there may exist *several* elements in G with this property!

> **Exercise 1.** Show that the additive group of integers $\mathbb{Z}$ is cyclic, but that the additive group of rational numbers $\mathbb{Q}$ is not cyclic.
>
> **Exercise 2.** Show that every cyclic group is abelian. Can you give an example of an abelian group that is not cyclic?
>
> **Exercise 3.** Let us fix a positive integer N. We define the group $C_N = \{z \in \mathbb{C} : z^N = 1\}$ of Nth roots of unit in $\mathbb{C}$. Show this a cyclic group of order N.
>
> **Exercise 4.** We say $\omega \in C_N$ is a primitive root of unity if $\langle \omega \rangle = C_N$. Show that these are precisely the elements of the form $\exp(2\pi i k/N)$ where $\gcd(k,N) = 1$.

2 The symmetric groups

Let us fix a positive integer n. The symmetric group, usually denoted by S_n is the set of bijections of the finite set $[n] = \{1, 2, \ldots, n\}$, where the group operation is given by_____. An element in S_n is called a_____. If $\sigma \in S_n$, we record the values of σ in matrix notation as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_n \end{pmatrix}$$

where we wrote σ_j instead of $\sigma(j)$. More simply, we also use one line notation $\sigma_1 \cdots \sigma_4$. For example, $2143 \in S_4$ is given in matrix notation by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

The *support* of a permutation σ is the set_____, which we write $\mathrm{supp}(\sigma)$. We say two permutations are *disjoint* if_____. A *cycle* is a permutation τin S_n with the following property: if $\mathrm{supp}(\tau) = \{i_1, \ldots, i_r\}$ then $\sigma(i_j) = i_{j+1}$ for $j < r$ and $\sigma(i_r) = i_1$. We write such elements in cycle notation $(i_1 \ldots i_r)$, noting that there are r ways of doing so, and say σ is an r-cycle.

> **Exercise 5.** Show that an r-cycle has order r, and that every element in S_n can be written as a product of disjoint cycles.

> **Exercise 6.** A 2-cycle is called a *transposition*. Show that every element in S_n can be written as a product of transpositions.

> **Exercise 7.** We say two permutations are disjoint if their supports are_____. Show that disjoint permutations commute.

Theorem 2.1. *Any permutation σ can be written uniquely as a product of disjoint cycles, which we call the*_____. *Moreover, if a permutation is written as a product of s transpositions and also as a product of r transpositions, then $s = t \mod 2$, and we call $(-1)^s$ the*_____ *and write it $(-1)^\sigma$ or $\mathrm{sgn}(\sigma)$.*

A permutation σ is_____if $\mathrm{sgn}(\sigma) = 1$ and it is_____if $\mathrm{sgn}(\sigma) = -1$. The sign of a permutation is multiplicative, in the sense that for any two permutations σ and τ, we have that $\mathrm{sgn}(\tau\sigma) =$_____. All transpositions are_____. More generally, a cycle of even length is_____, while a cycle of odd length is_____.

> **Exercise 8.** Show that the set of even permutations is a subgroup of S_n. We call it the _____and denote it by A_n.

> **Exercise 9.** Compute the order, the sign, and the cycle decomposition of the following permutation:
>
> $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 3 & 6 & 4 & 7 \end{pmatrix} \in S_7.$$

3 Subgroups, cosets and Lagrange's theorem

A subgroup of G is a subset H of G that satisfies the following three properties:

1. _____. The unit e of G belongs to H.
2. _____. For each $h \in H$ we have that the inverse h^{-1}_____
3. _____. For every $h, k \in H$, we have that the product hk_____.

In this case, the set H with the same product as the one in G is itself a group. We denote this situation by $H \leqslant G$. If S is a subset of G, let us write S^{-1} for the set $\{s^{-1} : s \in S\}$. The subgroup of G generated by S, which we denote by $\langle S \rangle$, is the set of products of the form $s_1 \dots s_n$ so that for each i we have that $s_i \in S \cup S^{-1}$. That is, it is the set of products of elements of S and of inverses of elements of S. We denote it by $\langle S \rangle$.

Exercise 10. Compute the subgroup generated by $\{(12), (123)\}$ in S_3. Do the same for $\{(12), (13)\}$ in S_3 and $\{(12), (34)\}$ in S_4.

Exercise 11. Compute the subgroup generated by i in C_8.

If H is a subgroup of G and $g \in G$, we call the set of products $\{gh : h \in H\}$ the_____ _____and write it gH. These sets have the following remarkable property: we have that $g_1 H = g_2 H$ if and only if_____, hence two left cosets are either equal or disjoint. Moreover, $|gH| = |H|$ for any $g \in G$, and the group G is a union of left cosets. In case G is finite, there exist finitely many disjoint cosets whose union is G, we call this number_____ and write it $[G : H]$.

Theorem 3.1 (Lagrange)**.** *Let H be a subgroup of G. Then $|G| = |H|[G : H]$, so that $|H|$ divides $|G|$.*

Lagrange's theorem is a cornerstone of group theory. It can be used to prove the following result.

Theorem 3.2. *Every finite group of prime order is cyclic.*

Proof. Let G be a finite group of prime order p, and choose an element $g \in G$ that is not the unit. The subgroup $H = \langle g \rangle$ must have order k that divides_____. Since g is not the unit, this subgroup is not trivial, so $k = p$ and thus $G = H$. It follows that G is generated by g, and hence that it is cyclic. □

Exercise 12. Find the left and the right cosets of $\langle (123) \rangle$ in S_3.

Exercise 13. (Difficult) Show that every group of order p^2, for p a prime, is abelian but not necessarily cyclic.

Exercise 14. Exhibit a finite group of order p^3, for p a prime, that is not abelian.

Exercise 15. Suppose that $g \in G$ has finite order $|g|$. Show that for any positive integer r, the element g^r has order $|g| / \gcd(r, |g|)$.

For G and H groups, the cartesian product $G \times H$ is again a group under the product $(g, h)(g', h') = (gg', hh')$. It is called the *direct product* of G and H.

4 Normal groups, quotient groups and Noether's isomorphism theorems

A group homomorphism is a function $\psi : G \longrightarrow H$ where G and H are groups, such that for each $g, g' \in G$ we have that_____. Group homomorphisms, which we can simply call morphisms or maps, satisfy the following properties:

1. If e is the unit of G and if e' is the unit of H, then_____.
2. If g is any element of G and g^{-1} is its invese, then_____.
3. If g is any element of G then the order of $\psi(g)$_____the order of g.
4. If K is a subgroup of G, then the set $\psi(K)$ is_____of H.

The *kernel* of a map $\psi : G \to H$ is the set $\psi^{-1}(e')$ where e' is the identity of H, and we denote it by $\ker\psi$. The kernel of ψ has the following remarkable property: ψ is injective if and only if_____. In this case we call ψ a monomorphism. A surjective morphism is called an epimorphism.

Exercise 16. Show that $N = \ker\psi$ is a subgroup of G and that for each $g \in G$ we have that $gN = Ng$.

Exercise 17. Show that if $\psi : G \longrightarrow H$ is an monomorphism then $|G|$ divides $|H|$.

Exercise 18. Show that if $\psi : G \longrightarrow H$ is an epimorphism then $|H|$ divides $|G|$.

A subgroup N of G with the property above, namely, that $gN = Ng$ for each $g \in N$ is called_____, and we denote this situation by $N \trianglelefteq G$. These subgroups are characterized by the following result, that says that normal subgroups of G are precisely given by kernels of maps with domain G:

Theorem 4.1. *Let N be a_____subgroup of G. Then the set of cosets G/N of N in G is a group under the operation_____. Moreover, the function $\pi : G \to G/N$ such that $g \mapsto gN$ is a group homomorphism with kernel N.*

We call G/N the quotient group of G by N, and usually read it 'G over N'. Note that in general G/H is merely a set of cosets, it is only when N is normal that we can make it into a group.

Exercise 19. Show that the operation on cosets of the last theorem is well defined if and only if N is normal.

Exercise 20. Show that the subgroup generated by (123) in S_4 is not normal. Show that the subgroup generated by (123) in S_3 is normal, and compute the quotient group.

Exercise 21. Show that A_n is normal in S_n for any $n \in \mathbb{N}$.

Exercise 22. Let $V_4 = \langle (12)(34), (14)(23) \rangle$. Show that V_4 is normal in S_4, and hence that it is normal in A_4.

Exercise 23. Show that, $C = \langle (12)(34) \rangle$ is normal in V_4, but not in A_4. Conclude that $C \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ but that "being normal' is not transitive.

The following result, due to Emmy Noether, is one of the most important results in basic group theory.

Theorem 4.2 (First isomorphism theorem)**.** *Let $\psi : G \longrightarrow H$ be a morphism with kernel $N = \ker \psi$. Then the map $\overline{\psi} : G/N \longrightarrow H$ such that $\overline{\psi}(gN) = \psi(g)$ is a well defined homomorphism with image $\psi(G)$, that restricts to an isomorphism of groups:*

$$G/N \longrightarrow \psi(G).$$

Moreover, if $\pi : G \longrightarrow G/N$ is the projection such that $\pi(g) = gN$, then ψ factors as $\overline{\psi}\pi = \psi$ where π is an epimorphism and $\overline{\psi}$ is a monomorphism.

Exercise 24. Consider the exponential function $\exp : \mathbb{R} \longrightarrow S^1$ (the unit circle in the complex plane) such that $r \longmapsto e^{2\pi i r}$. Find its kernel.

Exercise 25. Show that the map $\psi_n : \mathbb{Z} \longrightarrow \mathbb{R}$ such that $k \longmapsto k/n$ is a group monomorphism. Find the kernel and the image of the composite $\exp \circ \psi_n$.

Exercise 26. Conclude that the map $j_n : \mathbb{Z}/n \longrightarrow S^1$ such that $j_n(\overline{k}) = e^{2\pi i k/n}$ determines an isomorphism between $\mathbb{Z}/n$ and the group of nth roots of the unit.

Exercise 27. Conclude that the elements $\overline{k} \in \mathbb{Z}/n$ such that $\langle \overline{k} \rangle = \mathbb{Z}/n$ are precisely the classes of integers k coprime to n.

Exercise 28. Show that the group $\mathbb{G}_m = \{z \in \mathbb{C} : z^N \text{ for some } N \neq 0\}$ of **all** groups of unit is not finite, not cyclic, and isomorphic to the quotient group $\mathbb{Q}/\mathbb{Z}$. *Difficult:* show, however, that every proper subgroup of $\mathbb{G}_m$ is finite and cyclic.

5 Group actions

Let X be a set and G a group. An action of G on X is a group homomorphism $G \longrightarrow S_X$ where S_X is the group of permutations on X. In this case, we say X is a G-set and that G acts on X. Each $g \in G$ gives us a bijection on X, which we usually denote by $x \mapsto gx$. Alternatively, an action of G on X is a function $G \times X \longrightarrow X$ which we denote $(g, x) \longmapsto gx$ with the following properties:

1. If e is the identity of G, then for each $x \in X$ we have that_____.
2. For each $x \in X$ and for each $g, g' \in G$ we have that $g(g'x) =$_____.

If $x \in X$, then the subset of X of translates $Gx = \{gx : g \in G\}$ is called the_____, and the subset $G_x = \{g \in G : gx = x\}$ of G is called the_____. We say two elements $x, y \in X$ are G-equivalent if there is some $g \in G$ such that $gx = y$. This defines an equivalence relation on X, and it follows that the orbit Gx is the equivalence class of x. Moreover, the orbits form a partition of X, although they may have different sizes (unlike the case of cosets!). The following is one of the basic results regarding group actions:

Theorem 5.1 (Orbit-stabilizer theorem)**.** *Let X be a G-set and pick $x \in X$. The function $\alpha : G/G_x \longrightarrow X$ such that $gG_x \longmapsto gx$ defines a bijection between the set of left cosets of G_x in G and the orbit Gx of x in X. In particular, we have that $[G : G_x] = |Gx|$.*

Proof. First, α is well defined: if $gG_x = g'G_x$ then $g^{-1}g' \in G_x$, meaning that $g^{-1}g'x = x$ or, what is the same, $gx = g'x$. Thus $\alpha(gG_x)$ does not depend on the choice of representative g. It is clear that the image of α is Gx, so it suffices to check that α is injective. But if $gx = g'x$ then $g^{-1}g' \in G_x$ or, what is the same, the cosets gG_x and $g'G_x$ are equal, which means α is injective. □

Exercise 29. Suppose that $gx = y$. Show that $G_y = gG_xg^{-1}$, that is, the stabilizers of G-equivalent elements are conjugate.

Exercise 30. For each $g \in G$, let $\mathsf{Fix}(g)$ be the collection of elements $x \in X$ such that $gx = x$, and let $\mathsf{fix}(g)$ denote its cardinality. Consider the set $S = \{(g, x) \in G \times X : gx = x\}$.

1. Show that for each $g \in G$ there are $\mathsf{fix}(g)$ many pairs in S of the form (g, x).
2. Show that for each $x \in X$, there are $|G_x|$ many pairs in S of the form (g, x).
3. Conclude that $\sum_{g\in G} \mathsf{fix}(g) = \sum_{x\in X} |G_x|$.

Exercise 31. (Continued) Use the Orbit–Stabilizer theorem to show that $\frac{1}{|G|}\sum_{g\in G} \mathsf{fix}(g) = |X/G|$. That is, the average number of fixed points of G equals the number of orbits of the action.

Exercise 32. Let $G = O(2)$ be the set of 2×2 real orthogonal matrices, and define an action of $O(2)$ on $X = \mathbb{R}^2$ by $v \mapsto Av$. Show that the orbits of G on X are the sets of circles $B_r = \{(x, y) : x^2 + y^2 = r\}$ for $r \in [0, \infty)$. That is, there exists a matrix A such that $Av = w$ if and only if v and w have the same magnitude.

Exercise 33. Let X and Y be G-sets and consider the set Z of functions $\psi : Y \longrightarrow X$. Show this is a G-set under the rule $(g\psi)(x) = \psi(g^{-1}y)$.

Exercise 34. (Continued) Show that if $c(g)$ is the number of orbits of $\langle g \rangle$ on Y, then $\mathsf{fix}_Z(g) = |X|^{c(g)}$: a function $\psi : X \longrightarrow Y$ is fixed by g if and only if it is constant on the orbits of $\langle g \rangle$.

Exercise 35. (Continued) Let $Y = \mathbb{Z}/n$ be the cyclic group of order n and let $G = \mathbb{Z}/n$ act on Y by left multiplication. Show that $c(\overline{k}) = \gcd(k, n)$ and conclude that

$$\sum_{j=0}^{n-1} t^{\gcd(k,n)} = 0 \mod n$$

where $t = |X|$.

The class equation. Let X be a G-set. The set $X^G = \{x \in X : gx = x \text{ for all } g \in G\}$ is called the set of fixed points of X. It consists of those elements $x \in X$ such that $Gx = \{x\}$. Since the orbits of elements

of X partition it, we can find elements $x_1, \dots, x_r \in X$ such that $X = X^G \sqcup Gx_1 \sqcup \cdots \sqcup Gx_r$. By the Orbit-stabilizer Theorem, it follows that

$$|X| = |X^G| + \sum_{i=1}^{r} [G : G_{x_i}]$$

which we call the class equation of X. The following is are some standard exercises that use it:

Exercise 36. Let G be a p-group, that is, a group of order p^k for some $k \in \mathbb{N}$, and suppose that X is a G-set. Show that if $x \in X$ has a non-trivial orbit, then the size of its orbit is divisible by p.

Exercise 37. Use the previous exercise and the class equation to conclude that $|X| = |X^G| \mod p$. In particular, deduce that if $|X|$ is not divisible by p, then the action must have at least one fixed point.

Exercise 38. Let G be a group, and consider the action of G on itself by conjugation, that is, $g \cdot g'$ is the conjugate $gg'g^{-1}$. Show that the set of fixed points coincides with $Z(G) = \{g \in G : gh = hg \text{ for all } h \in H\}$, the center of G, and hence conclude that a non-trivial p-group has non-trivial center.