Université Gustave Eiffel
M2 – Semester 1 – 2025/2026

Algebra - Exercises

CHAU Dang Minh

Exercise 9. Prove Lagrange's theorem. Deduce that a group of prime order is cyclic.

Let G be a finite group and H be a subgroup of G. Recall that the left coset of H in G with respect to an element $x \in G$ is the set $xH = \{xh : h \in H\}$. Suppose that there is $h_1, h_2 \in H$ such that $xh_1 = xh_2$. Multiplying both sides on the left by x^{-1}, we get $h_1 = h_2$. So we must have that $\operatorname{card}(xH) = \operatorname{card}(H)$.

Since G is finite, there are only finitely many distinct left cosets of H in G. Let all of them be $x_1H, x_2H, \ldots, x_mH$, where $m \leq \operatorname{card}(G)$. We claim that

1. The cosets are pairwise disjoint i.e. for every $i, j \in \{1, \ldots, m\}$ and $i \neq j$, we have $x_iH \cap x_jH = \varnothing$. Indeed, if there is $y \in x_iH \cap x_jH$, then $y \in x_iH$. Hence, there is $h \in H$ such that $y = x_ih$. Therefore, $yH = (x_ih)H = x_i(hH) = x_iH$. Similarly, $yH = x_jH$. So, $x_iH = x_jH$, contradicting the assumption that they are distinct.
2. $G = x_1H \cup x_2H \cup \ldots \cup x_mH$. Indeed, for any $x \in G$, there is $i \in \{1, \ldots, m\}$ such that $xH = x_iH$. If not, then xH is a new left coset, contradicting the maximality of m.

Therefore, we have $\operatorname{card}(G) = \operatorname{card}(x_1H) + \ldots + \operatorname{card}(x_mH) = m \times \operatorname{card}(G)$, or $\operatorname{card}(H)$ divides $\operatorname{card}(G)$.

To deduce that a group of prime order is cyclic, let G be a group of prime order p. Let $x \in G$ and $x \neq e$. Since $e, a \in \langle x \rangle$, we have $\operatorname{card}(\langle x \rangle) > 1$. By Lagrange's theorem, the order of x divides the order of G. Since p is prime, we must have $\operatorname{card}(\langle x \rangle) = p = \operatorname{card}(G)$. Hence, $\langle x \rangle = G$, or G is cyclic.

Exercise 11. Prove that a subgroup H of a group G is normal if and only if for all $x \in G$ and $h \in H$ one has $xhx^{-1} \in H$ and also if and only if for all $x \in G$, $xHx^{-1} = H$.

Suppose that H is a normal subgroup of G. Then, for every $x \in G$, we have $xH = Hx$. Therefore, for every $h \in H$, there is $h' \in H$ such that $xh = h'x$. Multiplying both sides on the right by x^{-1}, we get $xhx^{-1} = h' \in H$. Conversely, suppose that for every $x \in G$ and $h \in H$, we have $xhx^{-1} \in H$. Then, for every $x \in G$ and $h \in H$, there is $h' \in H$ such that $xh = h'x$. Therefore, $xH \subseteq Hx$. Similarly, we can show that $Hx \subseteq xH$. Hence, $xH = Hx$, or H is a normal subgroup of G.

The other equivalence is proved as follows.

$$\begin{aligned} H \text{ is normal} &\iff \forall x \in G, xH = Hx \\ &\iff \forall x \in G, xHx^{-1} = Hxx^{-1} = H. \end{aligned}$$

Exercise 18. (Permutation Group) Let $\mathcal{S}^n$ be the permutation group of the set $\{1, 2, \ldots, n\}$.

1. Show that for every $\sigma \in \mathcal{S}^n$ and every cycle $(i_1, \ldots, i_k)$ one has $\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$.
2. Show that every element of $\mathcal{S}^3$ is a product of transpositions. Let $n \geq 2$ and $\sigma \in \mathcal{S}^n$. Show that if $\sigma(n) \neq n$, then there exists a transposition such that $\tau \circ \sigma(n) = n$. Conclude that for every $n \in \mathbb{N}^*$, every element of $\mathcal{S}^n$ is a product of transpositions.
3. Show that every $\sigma \in \mathcal{S}^n$ can be written as a product of cycles with disjoint supports.
4. We want to show that for $n \geq 3$, $Z(\mathcal{S}^n) = \{I\}$. Let $\sigma \in Z(\mathcal{S}^n)$. Show that for every $i \neq j$ one has $(\sigma(i), \sigma(j)) = (i, j)$. Deduce that $\sigma = I$.
5. Let us consider the subset H of $\mathcal{S}^4$ defined by

   $$H = \{I, (12)(34), (13)(24), (14)(23)\}.$$

   Show that H is an abelian normal subgroup of $\mathcal{S}^4$.

1. Let $c = (i_1, \ldots, i_k)$. For convenience, let $i_{k+1} = i_1$. Consider $x \in [n]$.
   - If $x = \sigma(i_r)$ for some $r \in [k]$, then
   $$\sigma c \sigma^{-1}(\sigma(i_j)) = \sigma c(i_j) = \sigma(i_{j+1}).$$
   - If $x \notin \{\sigma(i_1), \ldots, \sigma(i_k)\}$, then $\sigma^{-1}(x) \notin \{i_1, \ldots, i_k\}$, so $c\sigma^{-1}(x) = \sigma^{-1}(x)$. Therefore,
   $$\sigma c \sigma^{-1}(x) = \sigma(\sigma^{-1}(x)) = x.$$

   Therefore, $\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$.

2. We have $\mathcal{S}^3 = \{I, (12), (13), (23), (123), (132)\}$. The identity I is the product of zero transpositions, or we may write differently as $I = (12)(12)$. Also, $(123) = (13)(12)$ and $(132) = (12)(13)$.

   Let $\tau = (\sigma(n), n)$, we have $(\tau \circ \sigma)(n) = \tau(\sigma(n)) = n$.

   Now we use induction to show that for every $n \in \mathbb{N}^*$ every element of $\mathcal{S}^n$ is a product of transpositions. The base case $n = 2$ is trivial. Suppose that the statement is true for some $n \geq 2$. Let $\sigma \in \mathcal{S}^{n+1}$. If $\sigma(n+1) = n+1$, then $\sigma \in \mathcal{S}^n$ and by the induction hypothesis, σ is a product of transpositions. If $\sigma(n+1) \neq n+1$, then there exists a transposition τ such that $(\tau \circ \sigma)(n+1) = n+1$. Therefore, $\tau \circ \sigma \in \mathcal{S}^n$. By the induction hypothesis, $\tau \circ \sigma$ is a product of transpositions. Hence, $\sigma = \tau \circ (\tau \circ \sigma)$ is also a product of transpositions.

3. Let $\sigma \in \mathcal{S}^n$. If $\sigma = I$, then we are done. Suppose that $\sigma \neq I$. Then, there is $i_1 \in [n]$ such that $\sigma(i_1) \neq i_1$. Let $i_2 = \sigma(i_1)$. If $\sigma(i_2) = i_1$, then we have found a cycle (i_1, i_2). Otherwise, let $i_3 = \sigma(i_2)$. If $\sigma(i_3) = i_1$, then we have found a cycle (i_1, i_2, i_3). Otherwise, we continue this process. Since $[n]$ is finite, there must be $k \in \{2, \ldots, n\}$ such that $\sigma(i_k) = i_1$. Therefore, we have found a cycle $(i_1, i_2, \ldots, i_k)$.

   Now, let $\sigma' = (i_1, i_2, \ldots, i_k)^{-1} \circ \sigma$. We have $\sigma'(i_j) = i_j$ for every $j \in [k]$. If $\sigma' = I$, then we are done. Otherwise, we repeat the above process to find another cycle with disjoint support. Since $[n]$ is finite, this process must end after finitely many steps. Therefore, we can write σ as a product of cycles with disjoint supports.

4. Since $\sigma \in Z(\mathcal{S}^n)$, for every $i \neq j$, we have $(i,j)\sigma = \sigma(i,j)$. Multiplying both sides on the right by σ^{-1}, we get
   $$(i,j) = \sigma(i,j)\sigma^{-1} = (\sigma(i), \sigma(j)).$$
   Suppose that $\sigma \neq I$, or that there is $i \in [n]$ such that $\sigma(i) = j \neq i$. Since $n \geq 3$, there is $k \in [n]$ such that $k \neq i$ and $k \neq j$. Therefore, we have
   $$(i,k) = (\sigma(i), \sigma(k)) = (j, \sigma(k)).$$
   Hence $\{j, \sigma(k)\} = \{i, k\}$. But $j \neq i$ and $j \neq k$, which is a contradiction. Therefore $Z(S^n) = \{I\}$.

5. We have
   $$((12)(34))^2 = I, (12)(34)(13)(24) = (14)(23), (12)(34)(14)(23) = (13)(24),$$
   and similarly for other two double transpositions. Therefore, H is a subgroup of $\mathcal{S}^4$. From these equalities, we also have $(12)(34)(13)(24) = (13)(24)(12)(34)$ (equal to $(14)(23)$) and equalities of the same forms. Hence, H is abelian. Finally, for every $\sigma \in \mathcal{S}^4$, by question 1, we have
   $$\sigma((12)(34))\sigma^{-1} = \sigma((12)\sigma^{-1}\sigma(34))\sigma^{-1} = (\sigma(12)\sigma^{-1})(\sigma(34)\sigma^{-1}) = (\sigma(1), \sigma(2))(\sigma(3), \sigma(4)) \in H.$$
   Similarly for other two double transpositions. Therefore, H is normal.