

250A Homework 2

prepared by Jaejeong Lee

Exercise 3.2.8. Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

Solution $H \cap K$ is a common subgroup of H and K . By Lagrange's theorem $|H \cap K|$ divides $\gcd(|H|, |K|) = 1$, hence $|H \cap K| = 1$. Therefore, $H \cap K = 1$.

Exercise 3.2.9. Let G be a finite group and let p be a prime dividing $|G|$. Let \mathcal{S} denote the set of p -tuples of elements of G the product of whose coordinates is 1:

$$\mathcal{S} = \{(x_1, x_2, \dots, x_p) \mid x_i \in G \text{ and } x_1 x_2 \cdots x_p = 1\}.$$

Define the relation \sim on \mathcal{S} by letting $\alpha \sim \beta$ if β is a cyclic permutation of α .

(a) Show that \mathcal{S} has $|G|^{p-1}$ elements, hence has order divisible by p .

Solution Once x_1, x_2, \dots, x_{p-1} are chosen arbitrarily, then x_p is uniquely determined as $(x_1 x_2 \cdots x_{p-1})^{-1}$.

(b) Show that a cyclic permutation of an element of \mathcal{S} is again an element of \mathcal{S} .

Solution Each $0 \leq k \leq p-1$ corresponds to a cyclic permutation ϕ_k given by

$$\phi_k(x_1, x_2, \dots, x_p) = (x_{k+1}, x_{k+2}, \dots, x_p, x_1, \dots, x_k).$$

Let $(x_1, x_2, \dots, x_p) \in \mathcal{S}$ and denote $a = x_1 \cdots x_k$ and $b = x_{k+1} x_{k+2} \cdots x_p$. Then $ab = 1$ and we have $(x_{k+1} x_{k+2} \cdots x_p)(x_1 \cdots x_k) = ba = (a^{-1}a)ba = a^{-1}(ab)a = 1$. Thus $(x_{k+1}, x_{k+2}, \dots, x_p, x_1, \dots, x_k) \in \mathcal{S}$. Therefore, $\phi_k \in \text{Perm}(\mathcal{S})$ for each k .

(c) Prove that \sim is an equivalence relation on \mathcal{S} .

Solution Reflexivity follows from the existence of ϕ_0 , symmetry from the pair of ϕ_k and $\phi_{p-k(\text{mod } p)}$, and transitivity from the equality $\phi_{k'} \circ \phi_k = \phi_{k+k'(\text{mod } p)}$, which one can easily check.

(d) Prove that an equivalence class contains a single element if and only if it is of the form (x, x, \dots, x) with $x^p = 1$.

Solution (\Leftarrow) Clear. (\Rightarrow) Denote the single element by $\alpha = (x_1, x_2, \dots, x_p)$. Because $\phi_1(\alpha) \sim \alpha$, we must have $\phi_1(\alpha) = \alpha$, namely, $(x_2, \dots, x_p, x_1) = (x_1, x_2, \dots, x_p)$. It follows that $x_1 = x_2 = \cdots = x_p$.

(e) Prove that every equivalence class has order 1 or p (this uses the fact that p is a prime). Deduce that $|G|^{p-1} = k + pd$, where k is the number of classes of size 1 and d is the number of classes of size p .

Solution First off, for any $0 < k \leq p-1$, we have $\{\phi_0, \phi_1, \dots, \phi_{p-1}\} = \{\phi_{ik(\text{mod } p)} \mid 0 \leq i \leq p-1\}$. For if $ik \equiv jk(\text{mod } p)$ for some $0 \leq i, j \leq p-1$, then $(i-j)k \equiv 0(\text{mod } p)$. Since p is prime and $k < p$, we must have $i = j$.

Now let E be an equivalence class and $\alpha \in E$. Then $E = \{\phi_0(\alpha), \phi_1(\alpha), \dots, \phi_{p-1}(\alpha)\}$ and $1 \leq |E| \leq p$. If $|E| \neq p$, then $\phi_i(\alpha) = \phi_j(\alpha)$ for some $i < j$. Applying ϕ_{p-i} on both sides and denoting $k = j - i$, we get $\alpha = \phi_{p(\text{mod } p)} = (\phi_{p-i} \circ \phi_i)(\alpha) = (\phi_{p-i} \circ \phi_j)(\alpha) = \phi_{p+(j-i)(\text{mod } p)}(\alpha) = \phi_k(\alpha)$. Again applying ϕ_k repeatedly, we have $\alpha = \phi_k(\alpha) = \phi_{2k(\text{mod } p)}(\alpha) = \cdots = \phi_{(p-1)k(\text{mod } p)}(\alpha)$. From the discussion at the beginning, it follows that all cyclic permutations of α are equal to α and hence $|E| = 1$.

(f) Since $\{(1, 1, \dots, 1)\}$ is an equivalence class of size 1, conclude from (e) that there must be a nonidentity element x in G with $x^p = 1$, i.e., G contains an element of order p . [Show $p \mid k$ and so $k > 1$.]

Solution Since $|G|^{p-1} = k + pd$ and p divides $|G|^{p-1}$, p also divides k . Because $\{(1, 1, \dots, 1)\}$ is an equivalence class of size 1, the number k of classes of size 1 is not zero. Therefore, $k > 1$ and there is another equivalence class of size 1, which is, by (d), of the form $\{(x, x, \dots, x)\}$ for some $x \neq 1$. Thus $x^p = 1$.