

Math 519- Exam #1 Take Home problems Solutions

1. Let G be a finite group and let p be a prime which divides the order of G . Define X to be the set of all p -tuples of elements of G whose product is the identity, i.e.:

$$X = \{(g_1, g_2, \dots, g_p) \mid g_i \in G, g_1 g_2 \cdots g_p = e.\}$$

a. Show that X has $|G|^{p-1}$ elements. In particular the cardinality of X is divisible by p .

Given $(g_1, g_2, \dots, g_{p-1}, x) \in X$ then it is clear that $x = (g_1 g_2 \cdots g_{p-1})^{-1}$. Thus the first $p-1$ slots can be filled arbitrarily with an element of G , leaving only 1 choice for the last slot. Thus the total size of X is $|G|^{p-1}$.

b. Show that a cyclic permutation of an element of X is also an element of X , i.e. if $(g_1, g_2, g_3, \dots, g_p) \in X$ then so is $(g_2, g_3, \dots, g_p, g_1)$ and $(g_3, g_4, \dots, g_p, g_1, g_2)$, etc...

If $(g_1, g_2, g_3, \dots, g_p) \in X$ then $g_1 g_2 \cdots g_p = e$. Multiply both side of this equation by g_1^{-1} on the left and g_1 on the right gives $g_2 g_3 \cdots g_p g_1 = e$ so $(g_2, g_3, \dots, g_p, g_1) \in X$. Iterating this shows cyclic permutations of the p -tuple remain in X .

c. Define the relation \sim on X by setting $\alpha \sim \beta$ if β is a cyclic permutation of α . Prove that \sim is an equivalence relation on X .

Let $x = (g_1, g_2, g_3, \dots, g_p)$ and let σ denote the cyclic permutation so $\sigma(g_1, g_2, g_3, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1)$. So $\alpha \sim \beta$ if $\beta = \sigma^i(\alpha)$ for some $0 \leq i < p$ (Note $\sigma^p = id$). Clearly $\alpha \sim \alpha$ since $\alpha = \sigma^0(\alpha)$. If $\alpha = \sigma^i(\beta)$ then $\beta = \sigma^{p-i}(\alpha)$ so the relation is symmetric. Finally if $\alpha = \sigma^i(\beta)$ and $\beta = \sigma^j(\gamma)$ then $\alpha = \sigma^{i+j}(\gamma)$ so the relation is transitive.

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

Clearly such elements give an equivalence class with one element. Now if $x = (g_1, g_2, \dots, g_p) \in X$ has $g_i \neq g_j$ $\sigma^i(x) \neq \sigma^j(x)$ since they have different first entries. Thus the class has more than one element.

e. Prove that every equivalence class contains either 1 or p elements. (This requires p to be prime, be sure you make clear why!)

Let $x = (g_1, g_2, g_3, \dots, g_p)$. Consider the elements $\{x, \sigma x, \sigma^2 x, \dots, \sigma^{p-1} x\}$. If they are all distinct then the class of x has p elements. Suppose not, so assume, WLOG by shifting x cyclically, that $x = \sigma^i(x)$. Then $g_1 = g_i$. But $\sigma^i(\sigma^i(x)) = x$ so $g_1 = g_{2i}$ where $2i$ should be reduced mod p if it is $> p$. Continuing on we see that $g_1 = g_{ki}$ for any k . But p is prime so $(i, p) = 1$ so $\{ki\}$ runs over all the congruence classes mod p , and hence $g_1 = g_2 = \dots = g_p$. Thus either all the g_i are equal or there are p distinct elements in the equivalence class.

f. Since the equivalence classes partition the set X , conclude that:

$$|G|^{p-1} = k + pd$$

where k is the number of equivalence classes with one element and d is the number of equivalence classes with p elements.

This is immediate since equivalence classes are disjoint and partition the set X . Adding up their sizes gives the desired equation.

g. Since $\{(e, e, e, \dots, e)\}$ is an equivalence class of size 1, conclude from (f) that there must be a nonidentity element $g \in G$ with $g^p = e$. (show $p \mid k$).

Since $p \mid |G|$ and $p \mid pd$ then $p \mid k$. We already have $(e, e, \dots, e) \in X$ so k is at least one, thus k is at least p . Thus there are at least $p - 1$ other equivalence classes of size one. But these correspond to elements g with $g^p = e$. Thus we have shown G contains an element (actually at least $p - 1$ elements) of order p .

h. Conclude Cauchy's Theorem: Let G be a finite group and p a prime dividing the order of G . Then G contains an element of order p . (Cauchy's original 1845 proof was 9 pages, hopefully you have improved on this!)

Done! We have a nonidentity element such that $g^p = e$ so its order divides p so must equal p since p is prime.

i. Give an example of a finite group G and an integer d which divides $|G|$ such that G does not have an element of order d .

The Klein 4-group has no element of order 4.

2. Consider the group of order 16 with the following presentation:

$$QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = e, \sigma\tau = \tau\sigma^3 \rangle$$

(called the *quasidihedral or semidihedral group of order 16*).

a. Use the relations to explain why every element of QD_{16} can be put in the form $\tau^i\sigma^j$ with $0 \leq i \leq 1$ and $0 \leq j \leq 7$.

Given any product of σ 's and τ 's, the relation $\sigma\tau = \tau\sigma^3$ allows us to eventually bring all the τ 's to the left. Then the relation $\sigma^8 = \tau^2 = e$ allows the exponent of σ to be reduced mod 8 and of τ to be reduced mod 4.

b. Construct the Cayley Table for QD_{16} . Please order your elements $\{e, \sigma, \sigma^2, \dots, \sigma^7, \tau, \tau\sigma, \dots, \tau\sigma^7\}$.

Too big to type in!

c. This group has 3 subgroups of order 8. Prove that $\langle \sigma \rangle \cong Z_8$, $\langle \tau, \sigma^2 \rangle \cong D_4$ and $\langle \sigma^2, \sigma\tau \rangle$ is isomorphic to the Quaternion group whose Cayley table is given on page 90. In each case simply give an isomorphism, you don't have to prove it works.

The elements $\{e, \sigma, \sigma^2, \dots, \sigma^7\}$ form a subgroup isomorphic to Z_8 in the obvious way. The subgroup $\langle \tau, \sigma^2 \rangle$ has 8 elements, $\{e, \sigma^2, \sigma^4, \sigma^6, \tau, \tau\sigma^2, \tau\sigma^4, \tau\sigma^6\}$. The isomorphism can be given by sending τ to s and σ^2 to r in our usual notation for D_4 . The isomorphism of $\langle \sigma^2, \sigma\tau \rangle$ with Q_8 is given by taking σ^2 to a and $\tau\sigma^3 = \sigma\tau$ to b .

d. What is the center of QD_{16} ?

$$\{e, \sigma^4\}$$