Group Theory

Solutions to Problem Set 3 November 2, 2001

1. According to Lagrange's theorem, the order of a subgroup H of a group G must be a divisor of $|G|$. Since the divisors of a prime number are only the number itself and unity, the subgroups of a group of prime order must be either the unit element alone, $H = \{e\}$, or the group G itself, $H = G$, both of which are *improper* subgroups. Therefore, a group of prime order has no *proper* subgroups.

2. From a group G of prime order, select any element g, which is not the unit element, and form its period:

$$g, g^2, g^3, \ldots, g^n = e\,,$$

where n is the order of g (Sec. 2.4). The period *must* include every element in G, because otherwise we would have constructed a subgroup whose order is neither unity nor $|G|$. This contradicts the conclusion of Problem 1. Hence, a group of prime order is necessarily cyclic (but a cyclic group need not necessarily be of prime order).

3. For a group G with $|G| = pq$, where p and q are both prime, we know from Lagrange's theorem that the only proper subgroups have order p and q. Since these subgroups are of prime order, the conclusion of Problem 2 requires these subgroups to be cyclic.

4. Since the period of an element g of a group G forms a subgroup of G (this is straightforward to verify), Lagrange's theorem requires that $|g|$ must be a divisor of $|G|$, i.e., $G = k|g|$ for some integer k. Hence,

$$g^{|G|} = g^{k|g|} = (g^{|g|})^k = e^k = e\,.$$

5. The identity e of a group G has the property that for every element g in G, $ag = ge = g$. We also have that different cosets either have no common elements or have only common elements. Thus, in the factor group G/H of G generated by a subgroup H, the set which contains the unit element corresponds to the unit element of the factor group, since

$$\{e, h_1, h_2, \ldots\}\{a, b, c, \ldots\} = \{a, b, c, \ldots\}\,.$$

6. The class of an element a in a group G is defined as the set of elements gag^{-1} for all elements g in G. If G is Abelian, then we have

$$gag^{-1} = gg^{-1}a = a$$

for all g in G. Hence, in an Abelian group, every element is in a class by itself.

7. Let H be a subgroup of a group of G of index 2, i.e., H has two left cosets and two right cosets. If H is self-conjugate, then $gHg^{-1} = H$ for any g in G. Therefore, to show that H is self-conjugate, we must show that $gH = Hg$ for any g in G, i.e., that the left and right cosets are the same. Since H has index 2, and H is itself a right coset, all of the elements in Hg must either be in H or in the other coset of H, which we will call A. There two possibilities: either g is in H or g is not in H. If g is an element of H, then, according to the Rearrangement Theorem,

$$Hg = gH = H\,.$$

If g is not in H, then it is in A, which is a right coset of H. Two (left or right) cosets of a subgroup have either all elements in common or no elements in common. Thus, since the unit element must be contained in H, the set Hg will contain g which, by hypothesis, is in A. We conclude that

$$Hg = gH = A\,.$$

Therefore,

$$Hg = gH$$

for all g in G and H is, therefore, a self-conjugate subgroup.

8. The subgroup $H = \{e, a^2\}$ of the group $G = \{e, a, a^2, a^3, a^4 = e\}$ has index 2. Therefore, according to Problem 7, H *must* be self-conjugate. Therefore, the elements of the factor group G/H are the subgroup H, which corresponds to the unit element, so we call it $\mathcal{E}$, and the set consisting of the elements $\mathcal{A} = \{a, a^3\}$: $G/H = \{\mathcal{E}, \mathcal{A}\}$.

9. Let ϕ be an isomorphism between a group G and a group G', i.e. ϕ is a one-to-one mapping between all the elements g of G and g' of G'. From the group properties we have that the identity e of G must obey the relation

$$e = ee\,.$$

Since ϕ preserves all products, this relation must in particular be preserved by ϕ:

$$\phi(e) = \phi(e)\phi(e)\,.$$

The group properties require that, for any element g of G,

$$\phi(g) = e'\phi(g)\,,$$

where e' is the identity of G'. Setting $g = e$ and comparing with the preceding equation yields the equality

$$\phi(e)\phi(e) = e'\phi(e)\,,$$

which, by cancellation, implies

$$e' = \phi(e)\,.$$

Thus, an isomorphism maps the identity in G onto the identity in G'.