Math 430 – Problem Set 4 Solutions

Due March 18, 2016

6.18. If $[G : H] = 2$, prove that $gH = Hg$.

Solution. Since there are only two left cosets of H, which are disjoint, and one of them is H itself, the left cosets are H and $G - H$. The same holds for the right cosets. Moreover, $gH = H$ iff $g \in H$ iff $Hg = H$, and $gH = G - H$ iff $g \notin H$ iff $Hg = G - H$. Thus $Hg = gH$ for all $g \in G$.

9.8. Prove that $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$.

Solution. Suppose that $\phi : \mathbb{Q} \to \mathbb{Z}$ is an isomorphism. Since ϕ is surjective, there is an $x \in \mathbb{Q}$ with $\phi(x) = 1$. Then $2\phi(x/2) = \phi(x) = 1$, but there is no integer n with $2n = 1$. Thus ϕ cannot exist.

9.12. Prove that S_4 is not isomorphic to D_{12}.

Solution. Note that D_{12} has an element of order 12 (rotation by 30 degrees), while S_4 has no element of order 12. Since orders of elements are preserved under isomorphisms, S_4 cannot be isomorphic to D_{12}.

9.23. Prove or disprove the following assertion. Let G, H, and K be groups. If $G \times K \cong H \times K$, then $G \cong H$.

Solution. Take $K = \prod_{i=1}^{\infty} \mathbb{Z}$ and $G = \mathbb{Z}$ and $H = \mathbb{Z} \times \mathbb{Z}$. Then

$$G \times K \cong K \cong H \times K$$

but $G \ncong H$. Thus the assertion is false.

Note that the assertion is true if K is finite, but it's difficult to show. Many people tried to used an isomorphism $\phi : G \times K \to H \times K$ to construct an isomorphism $G \to H$. The difficulty is that ϕ does not necessarily map $G \times \{1\}$ to $H \times \{1\}$ (and if it does, it may not be surjective).

9.29. Show that S_n is isomorphic to a subgroup of A_{n+2}.

Solution. Let $\tau = (n+1, n+2) \in S_{n+2}$. Identifying S_n with the subgroup of S_{n+2} that fix $n+1$ and $n+2$, we define

$$\begin{aligned} \phi : S_n &\to A_{n+2} \\ \sigma &\mapsto \begin{cases} \sigma & \text{if } \sigma \text{ even} \\ \sigma\tau & \text{if } \sigma \text{ odd} \end{cases} \end{aligned}$$

We check that ϕ is an injective homomorphism. Note that $\sigma\tau = \tau\sigma$ for all $\sigma \in S_n$. Then

$$\phi(\sigma_1\sigma_2) = \begin{cases} \sigma_1\sigma_2 = \phi(\sigma_1)\phi(\sigma_2) & \text{if } \sigma_1 \text{ even, } \sigma_2 \text{ even,} \\ \sigma_1\sigma_2\tau = \phi(\sigma_1)\phi(\sigma_2) & \text{if } \sigma_1 \text{ even, } \sigma_2 \text{ odd,} \\ \sigma_1\tau\sigma_2 = \phi(\sigma_1)\phi(\sigma_2) & \text{if } \sigma_1 \text{ odd, } \sigma_2 \text{ even,} \\ \sigma_1\sigma_2\tau^2 = \phi(\sigma_1)\phi(\sigma_2) & \text{if } \sigma_1 \text{ odd, } \sigma_2 \text{ odd.} \end{cases}$$

Thus ϕ is a homomorphism. Moreover, since $\sigma\tau$ is never 1 and ϕ is the identity on A_n, ϕ is injective. Thus it defines an isomorphism with its image, a subgroup of A_{n+2}.

9.40. Find two nonisomorphic groups G and H such that $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

Solution. The simplest example is the trivial group and $\mathbb{Z}_2$, both of which have trivial automorphism group. Other examples include $G = \mathbb{Z}_3$ and $H = \mathbb{Z}_6$ (both of which have automorphism group isomorphic to $\mathbb{Z}_2$), $G = \mathbb{Z}_7$ and $H = \mathbb{Z}_{18}$ (both of which have isomorphism group isomorphic to $\mathbb{Z}_6$). A more interesting example is $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $H = S_3$, both of which have automorphism group isomorphic to S_3.

9.41. Let G be a group and $g \in G$. Define a map $i_g : G \to G$ by $i_g(x) = gxg^{-1}$. Prove that i_g defines an automorphism of G.

Solution. Since $i_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(y)$, we see that i_g is a homomorphism. It is injective: if $i_g(x) = 1$ then $gxg^{-1} = 1$ and thus $x = 1$. And it is surjective: if $y \in G$ then $i_g(g^{-1}yg) = y$. Thus it is an automorphism.

9.48 Prove that $G \times H$ is isomorphic to $H \times G$.

Solution. The map $\phi : G \times H \to H \times G$ defined by $\phi(g, h) = (h, g)$ is an isomorphism. It is surjective since, given $(h, g) \in H \times G$, $\phi(g, h) = (h, g)$. It is injective since if $\phi(g, h) = \phi(g', h')$ then $(h, g) = (h', g')$ and therefore $h = h'$ and $g = g'$. Finally, it is a homomorphism since $\phi((g, h)(g', h')) = \phi(gg', hh') = (hh', gg') = (h, g)(h', g') = \phi(g, h)\phi(g', h')$.

9.55 We classify groups of order $2p$ for an odd prime p.

(a) Assume G is a group of order $2p$, where p is an odd prime. If $a \in G$, show that a must have order 1, 2, p, or $2p$.

Solution. This is Lagrange's theorem.

(b) Suppose that G has an element of order $2p$. Prove that G is isomorphic to $\mathbb{Z}_{2p}$. Hence, G is cyclic.

Solution. Let $g \in G$ have order $2p$ and define $\phi : \mathbb{Z}_{2p} \to G$ by $n \mapsto g^n$. This is well defined and surjective since g has order $2p$, and thus also injective since G and $\mathbb{Z}_{2p}$ have the same size. Finally, it is a homomorphism since $g^{m+n} = g^n g^m$.

(c) Suppose that G does not contain an element of order $2p$. Show that G must contain an element of order p.

Solution. Suppose for contradiction that every element of G had order 1 or 2. Take two distinct elements a, b of order 2. Then $ab = ba$ (by 3.31 in a previous homework), and thus $\{1, a, b, ab\}$ forms a subgroup of G. But the order of G is not divisible by 4, contradicting Lagrange's theorem.

(d) Suppose that G does not contain an element of order $2p$. Show that G must contain an element of order 2.

Solution. Now suppose that every element has order 1 or p. We first show that the following relation is an equivalence relation on the set of non-identity elements of G: $a \sim b$ if there is an n so that $a = b^n$. It is reflexive (taking $n = 1$) and transitive (if $b = c^m$ then $a = c^{mn}$). In the equation $a = b^n$ we must have n relatively prime to p since a is not the identity. Taking m to be the inverse of n modulo p and raising both sides of $a = b^n$ to the mth yields $b = a^m$, so it is symmetric.

Each equivalence class under this relation has size $p - 1$. But there are $2p - 1$ elements of G, which is not divisible by $p - 1$. This provides the desired contradiction.

(e) Let P be a subgroup of G with order p and $y \in G$ have order 2. Show that $yP = Py$.

Solution. Since P has index 2, this is problem 6.18.

(f) Suppose that G does not contain an element of order $2p$ and $P = \langle z \rangle$ is a subgroup of order p generated by z. If y is an element of order 2, then $yz = z^k y$ for some $2 \leq k < p$.

Solution. Since $yP = Py$, we must have $yz = z^k y$ for some k, so we need only show that $k \neq 0, 1$. The case $k = 0$ is ruled out since $z \neq 1$. If $k = 1$, then z and y would commute, and the order of yz would be $2p$, contradicting the assumption.

(g) Suppose that G does not contain an element of order $2p$. Prove that G is not abelian.

Solution. This follows immediately from the previous part, since y and z do not commute.

(h) Suppose that G does not contain an element of order $2p$ and $P = \langle z \rangle$ is a subgroup of order p generated by z and y is an element of order 2. Show that we can list the elements of G as $\{z^i y^j | 0 \leq i < p, 0 \leq j < 2\}$.

Solution. The elements $z^i y^0$ for $0 \leq i < p$ are an enumeration of $P = \langle z \rangle$, and $z^i y^1$ for $0 \leq i < p$ are then an enumeration of Py. These are the two cosets of P in G, giving all the elements.

(i) Suppose that G does not contain an element of order $2p$ and $P = \langle z \rangle$ is a subgroup of order p generated by z and y is an element of order 2. Prove that the product $(z^i y^j)(z^r y^s)$ can be expressed uniquely as $z^m y^n$ for some non negative integers m, n. Thus, conclude that there is only one possibility for a non-abelian group of order $2p$, it must therefore be the one we have seen already, the dihedral group.

Solution. In the relation $yz = z^k y$, the number of ys does not change, so we must have $n \equiv j + s \pmod 2$. Furthermore, when $j = 0$ we have $z^{i+r} y^s$ directly, so we need only consider the case $j = 1$. Since we are interested in putting results in the form $z^m y^n$, the case $s = 1$ can be handled from the case $s = 0$ by just multiplying on the right by y, so it suffices to consider $z^i y z^r$. It must be of the form $z^m y$ for some m, but we need to show that there is only one possible value m can take.

Consider the expression yzy. Since $yz = z^k y$, we must have $yzy = z^k$. But then $z = yyzyy = yz^k y = (yzy)^k = (z^k)^k = z^{k^2}$. Thus $k^2 \equiv 1 \pmod 2$, for which there are only two solutions: $k = 1$ and $k = -1$. The case $k = 1$ corresponds to abelian G, which we have ruled out. Thus there is only a single possible group: the dihedral group D_p.