

MATH 511A, SOLUTIONS 7

1. Since $H \cap K$ is a subgroup of H , we know from Lagrange's Theorem that $\#(H \cap K)$ divides $\#H$. Similarly $\#(H \cap K)$ divides $\#K$. Since the GCD of $\#H$ and $\#K$ is 1, we have $\#(H \cap K) = 1$.

2. There are many ways to solve this problem. One way is to note that D_{12} contains seven elements of order two (sr^i for $0 \leq i < 6$, and r^3) while A_4 has only three (the three 2, 2-cycles).

3.

- (i) $f(x)^k = f(x^k) = f(e) = e$, so $\text{ord}(f(x))$ divides k .
- (ii) By (i), $\text{ord}(f(x))$ divides k , which divides $\#G$. But $\text{ord}(f(x))$ divides $\#H$ because $f(x) \in H$. Since $\#G, \#H$ are relatively prime, $\text{ord}(f(x)) = 1$; therefore $f(x) = e$ for all x .

4. The inverse of an r -cycle is an r -cycle, and disjoint cycles commute; it follows that α and α^{-1} have the same cycle type. Since elements of S_n with the same cycle type are conjugate, the claim follows.

If G is abelian then conjugation is trivial, so any element of order greater than 2 in an abelian group will be an example of an element not conjugate to its inverse.

5.

- (i) Certainly $Z(GL_2(\mathbb{F}))$ contains the nonzero scalar matrices. Conversely, suppose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $Z(GL_2(\mathbb{F}))$. Then A must commute with all diagonal matrices $D_{x,y} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ with x, y nonzero, as well as with $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. But

$$D_{x,y}A = \begin{pmatrix} xa & xb \\ yc & yd \end{pmatrix}, \quad AD_{x,y} = \begin{pmatrix} xa & yb \\ xc & yd \end{pmatrix}$$

and when $x \neq y$ these are equal only when $b = c = 0$. Moreover

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

only when $a = d$. Hence A is scalar.

- (ii) Suppose $G/Z(G)$ is cyclic, generated by $bZ(G)$. Every element of G has the form $b^n z$ for some $z \in Z(G)$. If $g, h \in G$, say $g = b^n z$ and $h = b^m w$, then

$$gh = b^n z b^m w = b^{n+m} zw = b^{n+m} wz = hg$$

so G is abelian. (In this equation, the second equality uses the fact that z commutes with b^m , the third that w and z commute, and the last that w commutes with b^n .)

6. Observe that if $x \in Q$, then $x^2 = \pm 1$ (with $x^2 = -1$ unless $x = \pm 1$, in fact). It follows that in the quotient $Q/Z(Q)$, which has order 4, every element has order at most 2. Since every group of order 4 is isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or V , we conclude $Q/Z(Q) \cong V$. Alternately, apply problem #2.69: Q is not abelian, so $Q/Z(Q)$ cannot be cyclic; since it has order 4, the only other possibility is that it is isomorphic to V .

If Q had a subgroup isomorphic to V , then Q would contain at least three elements of order 2; however, it has only one.

7.

(i) We have

$$\gamma_g(xy) = gxyg^{-1} = (gxyg^{-1}) = \gamma_g(x)\gamma_g(y),$$

so γ_g is a homomorphism. It is injective because $gxyg^{-1} = e$ implies $x = g^{-1}eg = e$, and it is surjective because $\gamma_g(g^{-1}xg) = x$ for any $x \in G$.

(ii) We have

$$(\gamma_h \circ \gamma_g)(x) = \gamma_h(gxyg^{-1}) = hgxyg^{-1}h^{-1} = \gamma_{hg}(x)$$

and therefore $\gamma_h \circ \gamma_g = \gamma_{hg}$. This proves $\Gamma(h)\Gamma(g) = \Gamma(hg)$.

(iii) We have $g \in \ker(\Gamma)$ if and only if γ_g is trivial, i.e., if and only if $gxyg^{-1} = x$ for all $x \in G$. The latter is equivalent to $gx = xg$ for all $x \in G$, which by definition is what it means to have $g \in Z(G)$.

(iv) If $\phi \in \text{Aut}(G)$ and $\gamma_a \in \text{Inn}(G)$, we have to check that $\phi \circ \gamma_a \circ \phi^{-1}$ is an inner automorphism. To see this, we calculate

$$\begin{aligned} (\phi \circ \gamma_a \circ \phi^{-1})(x) &= (\phi \circ \gamma_a)(\phi^{-1}(x)) \\ &= \phi(a\phi^{-1}(x)a^{-1}) \\ &= \phi(a)\phi(\phi^{-1}(x))\phi(a)^{-1} \\ &= \phi(a)x\phi(a)^{-1}. \end{aligned}$$

So indeed $\phi \circ \gamma_a \circ \phi^{-1} = \gamma_{\phi(a)}$.

8. Solution 1: Write $V = \{e, a, b, c\}$ with a, b, c of order 2. Any automorphism of V fixes e and permutes a, b, c ; we therefore have an injection $\text{Aut}(V) \rightarrow S_{\{a,b,c\}}$ given by restriction to $\{a, b, c\}$. It is easy to see (directly, using the multiplication table for V) that this is surjective. Another approach is to note that $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so that $\text{Aut}(V)$ will be isomorphic to $\text{GL}_2(\mathbb{F}_2)$, which is isomorphic to S_3 .

Any automorphism of S_3 must send elements of order 2 to elements of order 2; in this case the only elements of order 2 are the transpositions, so an element of $\text{Aut}(S_3)$ permutes the transpositions: that is, we obtain a map $\varphi : \text{Aut}(S_3) \rightarrow S_{\{(12), (23), (13)\}}$. Since the transpositions generate S_3 , this map is injective. On the other hand $\#\text{Aut}(S_3) \geq 6$, since $\text{Aut}(S_3)$ contains the inner automorphisms and $Z(S_3)$ is trivial. Hence φ is an isomorphism.

If $\phi \in \text{Aut}(\mathbb{Z})$, then $\phi(n) = n\phi(1)$. In particular ϕ is determined entirely by $\phi(1)$. Since ϕ must be surjective, we have $1 = n\phi(1)$ for some n ; hence $\phi(1) = \pm 1$. So we have an injection from $\text{Aut}(\mathbb{Z}) \rightarrow \{\pm 1\}$ given by $\phi \mapsto \phi(1)$. Both $\phi(n) = n$ and $\phi(n) = -n$ are indeed automorphisms of \mathbb{Z} , so the map $\text{Aut}(\mathbb{Z}) \rightarrow \{\pm 1\}$ is a bijection.

Solution 2 (for $\text{Aut}(V)$): Observe that V , regarded as a subgroup of S_4 , is a normal subgroup. This means that inner automorphisms of S_4 map $V \rightarrow V$, and we get a map

$$\varphi : S_4 \cong \text{Inn}(S_4) \rightarrow \text{Aut}(V).$$

The kernel of φ is the centralizer

$$C_{S_4}(V) = \{x \in S_4 : xy = yx \text{ for all } y \in V\},$$

which you can check is simply V . By the first isomorphism theorem we have an injection $\phi : S_4/V \hookrightarrow \text{Aut}(V)$. As in Solution 1 we have an injection $\text{Aut}(V) \hookrightarrow S_{\{a,b,c\}}$, and by composing these maps we get an injection

$$S_4/V \hookrightarrow S_{\{a,b,c\}}.$$

Since both sides have order 6, this must be an isomorphism.

Alternately we may regard S_3 as a subgroup of S_4 in a number of ways, but the most natural is to allow each element in S_3 to act on $\{1, 2, 3, 4\}$ in the obvious way on $\{1, 2, 3\}$ and to fix 4. To put it another way, S_3 is identified with the stabilizer $\text{Stab}(4)$ in the natural action of S_4 on $\{1, 2, 3, 4\}$. In this manner we get $S_3 \hookrightarrow S_4 \rightarrow S_4/V \hookrightarrow \text{Aut}(V)$, which is injective because S_3 and V have trivial intersection in S_4 , and surjective since $\#\text{Aut}(V) \leq 6$.

9. Solution 1: Consider the natural homomorphism $\pi : G \rightarrow G/K$, and suppose $H \leq G$ with $\#H = \#K$. If $h \in H$, then the order of $\pi(h) \in G/K$ divides $\#(G/K)$; however, this order also divides $\#H = \#K$ (by Exercise #3(i)). Since $\#(G/K)$ and $\#K$ are relatively prime, $\pi(h)$ has order 1, and $h \in K$. Hence $H \subset K$, and therefore $H = K$. Alternately, consider the order of the whole subgroup $\pi(H)$.

Solution 2: If H is such a group, consider the second isomorphism theorem $HK/K \cong H/(H \cap K)$. The size of the left-hand side is a divisor of $[G : K]$; the size of the right-hand side is a divisor of $\#H = \#K$. Since $[G : K], \#K$ are relatively prime, we must have $H = H \cap K$, and so $H = K$.

10.

- (i) Clear.
- (ii) Note first that if $x \in G$, then nx has order dividing m , since $m(nx) = (mn)x = 0$. Similarly mx has order dividing n . Now since $(m, n) = 1$, we can write $1 = an + bm$ for some $a, b \in \mathbb{Z}$. If $x \in G$, then

$$x = 1 \cdot x = (an + bm)x = a(nx) + b(mx) \in G_m + G_n.$$

- (iii) **Solution 1:** G_m and G_n are normal subgroups of G , they have trivial intersection, and $G_m + G_n = G$; it follows from the proposition proved in class that $G \cong G_m \times G_n$.

Solution 2: Define a map $\phi : G_m \times G_n \rightarrow G$ by sending $(x, y) \mapsto x + y$. It is injective since $G_m \cap G_n = \{0\}$; it is surjective by (ii). Therefore it is an isomorphism. (Note: if you tried defining this map in the reverse direction, i.e., $G \rightarrow G_m \times G_n$, then you had to check that this is well-defined; you can avoid this by defining the map from $G_m \times G_n \rightarrow G$ instead!)

Solution 3: As in part (ii), map $\phi : G \rightarrow G_m \times G_n$ by sending $x \mapsto (anx, bmx)$. Map $\rho : G_m \times G_n \rightarrow G$ by sending (y, z) to $y + z$. Then

$$(\rho \circ \phi)(x) = \rho(anx, bmx) = (an + bm)x = x$$

and

$$\begin{aligned}(\phi \circ \rho)(y, z) &= \phi(y + z) = (an(y + z), bm(y + z)) = (any, bmoz) \\ &= ((an + bm)y, (an + bm)z) = (y, z)\end{aligned}$$

Therefore ϕ and ρ are inverse to one another, and must be isomorphisms.