Debra Griffin
Math 210A
HW #5, 2.6 p. 95 #67, 68, 69, 71, 76

2.67 **(i)** Prove that Aut($\boldsymbol{V}$) ≅ S_3 and that Aut (S_3) ≅ S_3. Conclude that nonisomorphic groups can have isomorphic automorphism groups.

Proof:
$S_3 = \{1, a, b, c, ab, bc\} = \{\alpha_1, \alpha_2, ..., \alpha_6\}$.
We first show that Aut($\boldsymbol{V}$) ≅ S_3.
Let ψ : Aut($\boldsymbol{V}$) → S_3 where $\forall\ \phi \in$ Aut($\boldsymbol{V}$) , $\psi(\phi) = \phi(\boldsymbol{V})$.
We know $\boldsymbol{V} = \{1, a', b', c'\}$ and $\forall\ \phi \in$ Aut($\boldsymbol{V}$), $\phi(1) = 1$.
Since $\boldsymbol{V}$ consists of 3 nonidentity elements, a', b', c' of the same order, then every $\phi \in$ Aut($\boldsymbol{V}$) permutes these 3 elements and there are 6 distinct permutations of 3 elements.
Then we can let Aut($\boldsymbol{V}$) = $\{\phi_1, \phi_2, ..., \phi_6\}$.
One permutation, ϕ_1, is the identity permutation.
Three permutations, ϕ_2, ϕ_3, ϕ_4, permute only 2 elements and fix the other, hence have order 2.
And two permutations, ϕ_5, ϕ_6, permute all 3 elements, and thus have order 3.
Define ψ : Aut($\boldsymbol{V}$) → S_3 by $\psi(\phi_i) = \alpha_i$. Clearly, ψ is an isomorphism.
We now show that Aut (S_3) ≅ S_3.
Let $S_3 = \{1, a, b, c, ab, bc\}$ where a, b, c have order 2; and ab and bc have order 3.
Since S_3 consists of 3 elements of order 2, 2 elements of order 3 and 1, then every $\phi \in$ Aut(S_3) permutes the 3 elements of order 2 and there are 6 distinct permutations of the 3 elements. By homormorphism properties, $\phi(ab) = \phi(a)\phi(b)$, thus each permutation of the order 2 elements determines the assignment of the order 3 elements.
Thus Aut(S_3) has exactly 6 distinct elements. Let Aut(S_3) = $\{\phi_1, \phi_2, ..., \phi_6\}$.
One permutation, ϕ_1, is the identity permutation.
Three permutations, ϕ_2, ϕ_3, ϕ_4, permute only 2 of the order 2 elements, a, b, and c, and fix the other, hence have order 2.
And two permutations, ϕ_5, ϕ_6, permute all 3 of a, b, and c, and thus have order 3.
Define ψ : Aut(S_3) → S_3 by $\psi(\phi_i) = \alpha_i$; hence ψ is an isomorphism from Aut(S_3) → S_3.

(ii) Prove that Aut($\mathbb{Z}$) ≅ $\mathbb{Z}_2$. Conclude that an infinite group can have a finite automorphism group.

Proof:
Since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, then if $\phi \in$ Aut ($\mathbb{Z}$), $\phi(1)$ and $\phi(-1)$ must be generators of the group.
Since 1 and –1 are the only generators of $\mathbb{Z}$, then there are only 2 automorphisms of $\mathbb{Z}$.
Hence Aut($\mathbb{Z}$) ≅ $\mathbb{Z}_2$.

2.68 If G is a group for which Aut $(G) = \{1\}$, prove that $|G| \leq 2$.
Proof:
From an online source—

Assume that the only automorphism of G is the identity mapping. Then all inner automorphisms of G are trivial, so G must be abelian. Next, the function $\mu : G \to G$ defined by $\mu(x) = x^{-1}$, for all x in G, is an automorphism, so by hypothesis it must be trivial. This forces $x = x^{-1}$ for all x in G. If G is written additively, then G has a vector space structure over the field $\mathbf{Z}_2$. (Since every element of G has order 2, it works to define $0 \cdot x = 0$ and $1 \cdot x = x$, for all x in G.) With this vector space structure, any group homomorphism is a linear transformation (and vice versa), so the automorphism group of G is a group of invertible matrices. Therefore Aut (G) is nontrivial, unless G is zero or one-dimensional.

For $|G| = 1$, the result holds trivially.
For $|G| = 2$, $G = \{e, a\}$. Since $\forall\ \varphi \in \text{Aut}(G)$, $\varphi(e) = e$, then the bijection forces $\varphi(a) = a$. Thus we have only the identity map.
$(*)$ Suppose $|G| \geq 3$ and $\text{Aut}(G) = \{1\}$.
We will show that over the field $\mathbb{Z}_2$, G satisfies the axioms of a vector space.
We start with the commutativity axiom.
$\forall\ g \in G$, the inner automorphism φ: $G \to G$ defined by $\varphi(g) = gxg^{-1}$ is the identity map.
So then $\forall\ g, x \in G$, $gx = xg$, hence G is abelian.
The automorphism μ: $G \to G$ defined by $\mu(x) = x^{-1}$ must be the identity map, hence $\forall\ x \in \text{G}$, $x = x^{-1}$. This gives us that every nonidentity element of G has order 2.
So then we can define $0_{\mathbb{Z}2} \bullet x = 0_G$ and $1_{\mathbb{Z}2} \bullet x = x$ (If x has order > 2, the distributive law fails; for example, if x has order 3, then $(1 + 1) \bullet x = 0 \bullet x = 0 \neq x + x = 1 \bullet x + 1 \bullet x$.)
So now we can assume G satisfies the axioms of a vector space.
Consider G^*, the set of all linear transformations from G to itself. The set of all automorphisms of G is a subgroup of G^*. Since automorphisms are bijective linear transformations, then $\text{Aut}(G)$ is a group of invertible matrices (that is matrix representations of the change of bases). Since $|G| \geq 3$, then $\text{Aut}(G)$ is a group of $n \times n$ matrices with entries from $\mathbb{Z}_2$ where $n \geq 2$. Since more than 1 invertible matrix exists for any $n \geq 2$, then $|\text{Aut}(G)| \neq 1$, a contradiction to our assumption $(*)$.
$\therefore |G| \leq 2$.

2.69 Prove that if G is a group for which $G/Z(G)$ is cyclic, where $Z(G)$ denotes the center of G, then G is Abelian.
Hint: If $G/Z(G)$ is cyclic, prove that a generator gives an element that is possibly outside of $Z(G)$ which commutes with each element of G.
Proof:
Assume $G/Z(G)$ is cyclic. Then for some $a \in G$, $G/Z(G) = \langle aZ(G) \rangle = \{Z(G), aZ(G), (aZ(G))^2, \ldots\}$. And since $Z(G) \lhd G$, then $(aZ(G))^n = a^n(Z(G))^n = a^nZ(G)$.

Let $x, y \in G$.

Then for some integers i and j, $xZ(G) = (aZ(G))^i = a^iZ(G)$ and $yZ(G) = (aZ(G))^j = a^jZ(G)$. Since $1 \in Z(G)$ and $x = x \bullet 1$, then $x \in xZ(G)$. Thus, $x = a^ic$ and $y = a^jd$ where c, d are elements in $Z(G)$. As $c, d \in Z(G)$, then

$$xy = (a^ic)(a^jd) = a^i(ca^j)d = a^i(a^jc)d = (a^ia^j)(cd) = (a^{i+j})(cd)$$
$$= (a^{j+i})(dc) = (a^ja^i)(dc) = a^j(a^id)c = a^j(da^i)c = (a^jd)(a^ic) = yx.$$

$\therefore$ G is Abelian.

2.71 Let G be a finite group with $K \lhd G$. If $(|K|, [G:K]) = 1$, prove that K is the unique subgroup of G having order $|K|$.

Proof:

Let $|K| = m$, then by Lagrange's Theorem, $|G| = mn$ for some positive integer n

and $[G:K] = n$. Assume $(m, n) = 1$.

Suppose G has another subgroup H that has order m.

Let $h \in H, h \neq 1$. Then $\circ(hK) \mid n$ since $hK \in G/K$ and $|G/K| = n$.

Let $d = \circ(h)$. Then $K \lhd G \Rightarrow K = h^dK = (hK)^d$, hence $\circ(hK) \mid m$ as $\circ(h) \mid |H|$.

By assumption, $(m, n) = 1$. So $\circ(hK) = 1$.

$\therefore\ hK \in K.\ \therefore H \subseteq K$ and $|H| = |K|.\ \therefore\ H = K.$

$\therefore K$ is the unique subgroup of G having order $|K|$.

2.76 If H and K are normal subgroups of a group G with $HK = G$, prove that $G/(H \cap K) \cong (G/H) \times (G/K)$.
Hint: If $\phi: G \to (G/H) \times (G/K)$ is defined by $x \mapsto (xH, xK)$, then $\ker \phi = H \cap K$; moreover, we have $G = HK$ so that $\bigcup_a aH = HK = \bigcup_b bK$.

Proof:
Define $\phi: G \to (G/H) \times (G/K)$ by $x \mapsto (xH, xK)$. We will show (1) ϕ is a homomorphism, (2) $\phi(G) = (G/H) \times (G/K)$, and (3) $\ker \phi = H \cap K$.

(1) Let $x, y \in G$, and note that normalcy gives us that $xHyH = xyH$ and $xKyK = xyK$.

Then $\phi(x)\phi(y) = (xH, xK)(yH, yK) = (xHyH, xKyK) = (xyH, xyK) = \phi(xy)$.

$\therefore$ ϕ is a homomorphism.

(2) We will show containment in both directions.

Let $(X, Y) \in \phi(G)$. Then $X = xH$ and $Y = xK$ for some $x \in G$.

$\therefore$ $\phi(x) = (xH, xK) = (X, Y) \in (G/H) \times (G/K)$. $\therefore$ $\phi(G) \subseteq (G/H) \times (G/K)$.

Let $(X, Y) \in (G/H) \times (G/K)$. Then $X = aH$ and $Y = bK$ for some $a, b \in G$.

Note that since $HK = G$, then $a = hk$ and $b = h'k'$ for some $h \in H$, $h' \in H$, $k \in K$, and $k' \in K$.

Also note that normalcy gives us that $hkH = h(Hk) = (hH)k = Hk = kH$.

$(aH, bK) = (hkH, h'k'K) = (hkH, h'K) = (kH, h'K)$.

Let $x = h'k$, then $(xH, xK) = (h'kH, h'kK) = (kH, h'K) = (aH, bK)$.

$\therefore$ $(X, Y) \in \phi(G)$. $\therefore$ $(G/H) \times (G/K) \subseteq \phi(G)$, as desired.

$\therefore$ $\phi(G) = (G/H) \times (G/K)$.

(3) Again, we will show containment in both directions.

Let $x \in \ker \phi$. Then $\phi(x) = (xH, xK) = (H, K)$.

$\therefore$ $xH = H$ and $xK = K$.

$\therefore$ $x \in H$ and $x \in K$, hence $x \in H \cap K$.

Let $x \in H \cap K$. Then $x \in H$ and $x \in K$. $\therefore$ $\phi(x) = (H, K)$.

$\therefore$ $\ker \phi = H \cap K$.

And by the 1st Isomorphism Theorem, $G/(H \cap K) \cong (G/H) \times (G/K)$.
