# Chapter 15 Exercises
# Gallian's Book on Abstract Algebra

Spencer T. Parkin

March 6, 2014

## Exercise 1

Prove Theorem 15.1.

For the theorem, we let $\phi$ be a ring homomorphism from a ring $R$ to a ring $S$, and we let $A$ be a subring of $R$ and let $B$ be an ideal of $S$.

The first part of the theorem states that for any $r \in R$ and any positive integer $n$, that $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.

Proof: That $\phi(nr) = n\phi(r)$ follows from Property 2 of Theorem 10.1 for group homomorphisms. Similarly,

$$\phi(r^n) = \phi(\underbrace{r \cdot \cdots \cdot r}_{n}) = \underbrace{\phi(r) \cdot \cdots \cdot \phi(r)}_{n} = (\phi(r))^n.$$

The second part of the theorem states that $\phi(A) = \{\phi(a) | a \in A\}$ is a subgring of $S$.

Proof: That $\phi(A)$ is an Abelian group follows from Properties 1 and 3 of Theorem 10.2 for group homomorphisms. Then, if $a, b \in \phi(A)$, then there exist $x, y \in A$ such that $\phi(x) = a$ and $\phi(y) = b$. Then, since $xy \in A$ and $\phi(xy) = \phi(x)\phi(y) = ab$, we see that $ab \in \phi(A)$. Having now shown closure of the ring multiplication of $S$ in $\phi(A)$, we can claim that $\phi(A)$ is a subring of $S$.

The third part of the theorem states that if $A$ is an ideal and $\phi$ is onto $S$, then $\phi(A)$ is an ideal.

Proof: By the second part of this theorem, $\phi(A)$ is a subring, so we need only prove now that it is an ideal of $S$. Let $s \in S - \phi(A)$ and $y \in \phi(A)$.

Then since $\phi$ is onto, there exists $r \in R$ such that $\phi(r) = s$. Let $x \in A$ such that $\phi(x) = y$. Then since $rx \in A$, (because $A$ is an ideal of $R$), and $\phi(rx) = \phi(r)\phi(x) = sy$, we have $sy \in \phi(A)$. Similarly, since $xr \in A$, (again, because $A$ is an ideal of $R$), and $\phi(xr) = \phi(x)\phi(r) = ys$, we have $ys \in \phi(A)$. We can now claim that $\phi(A)$ is an ideal of $S$.

The fourth part of the theorem states that $\phi^{-1}(B) = \{r \in R | \phi(r) \in B\}$ is an ideal of $R$.

Proof: By Property 7 of Theorem 10.2, $\phi^{-1}(B)$ is a subgroup of $R$. It must be an Abelian group since all subgroups of rings are Abelian. Now let $r \in R$ and $x \in \phi^{-1}(B)$. Then $\phi(r) \in S$ and $\phi(x) \in B$ and since $B$ is an ideal of $S$, $\phi(rx) = \phi(r)\phi(x) \in B$, showing that $rx \in \phi^{-1}(B)$. Similar reasoning shows that $xr \in \phi^{-1}(B)$, so $\phi^{-1}(B)$ is an ideal of $R$.

The fifth part of the theorem states that if $R$ is commutative, then $\phi(R)$ is commutative.

Proof: Letting $a, b \in R$, notice that

$$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a).$$

The sixth part of the theorem states that if $R$ has a unity 1, $S \neq \{0\}$, and $\phi$ is onto, then $\phi(1)$ is the unity of $S$.

Proof: Notice that for all $r \in R$, we have $\phi(1)\phi(r) = \phi(r)$. Then since $\phi$ is onto, it follows that $\phi(1)s = s$ for all $s \in S$. This shows that $\phi(1)$ is either the unity of $S$, or that $\phi(r) = 0$ for all $r \in R$. Now if $S \neq \{0\}$ and $\phi$ is onto, then we can't have $\phi(r) = 0$ for all $r \in R$. So $\phi(1) = 1$.

The seventh part of the theorem states that $\phi$ is an isomorphism if and only if $\phi$ is onto and $\ker \phi = \{r \in R | \phi(r) = 0\} = \{0\}$.

Proof: This follows immediately from Property 9 of Theorem 10.2. We need only look at the statement from a purely group-theoretic stand-point and also realize that $\phi$ will preserve the multiplication product of the ring.

The eighth and last part of the theorem states that if $\phi$ is an isomorphism from $R$ onto $S$, then $\phi^{-1}$ is an isomorphism from $S$ onto $R$.

Proof: Realize that $\ker \phi^{-1}$ is the trivial subring of $R$. This part of the theorem then follows from the seventh part of the theorem.

# Exercise 2

Prove Theorem 15.2.

Let $\phi$ be a homomorphism from a ring $R$ to a ring $S$. Then $\ker\phi = \{r \in R | \phi(r) = 0\}$ is an ideal of $R$.

Proof: From group theory, we already know that $\ker\phi$ is a normal subgroup of $R$. Now let $r \in R$ and $x \in \ker\phi$. Then $\phi(rx) = \phi(r)\phi(x) = \phi(r)\cdot 0 = 0 \implies rx \in \ker\phi$. Similarly, we have $xr \in \ker\phi$, so $\ker\phi$ is an ideal of $R$.

# Exercise 3

Prove Theorem 15.3.

Let $\phi$ be a ring homomorphism from $R$ to $S$. Then the mapping from $R/\ker\phi$ to $\phi(R)$, given by $r + \ker\phi \to \phi(r)$, is an isomorphism. In symbols, $R/\ker\phi \approx \phi(R)$.

Proof: By Theorem 10.3, $\phi$ is a group isomorphism from $R/\ker\phi$ to $\phi(R)$. Now since $\ker\phi$ is an ideal, $R/\ker\phi$ is a factor ring by Theorem 14.2. What remains to be shown is that the mapping preserves multiplication in $\phi(R)$. To that end, see that for any pair of elements $x, y \in R$, we have

$$\Psi(x + \ker\phi)\Psi(y + \ker\phi) = \phi(x)\phi(y) = \phi(xy) = \Psi(rs + \ker\phi),$$

where $\Psi : R/\ker\phi \to \phi(R)$ is the mapping given in the theorem's statement.

# Exercise 4

Prove Theorem 15.4.

Every ideal of a ring $R$ is the kernel of a ring homomorphism of $R$. In particular, an ideal $A$ is the kernel of the mapping $r \to r + A$ from $R$ to $R/A$.

Proof: Define $\phi(r) = r + A$ as the natural homomorphism from $R$ to $R/A$. It is not hard to see that $\phi$ preserves both operations of $R$ in $R/A$. Clearly, $\phi(r) = A$ if and only if $r \in A$, so $\ker\phi = A$.

# Exercise 18

Determine all ring isomorphisms from $Z_n$ to itself.

We know that all such isomorphisms $\phi : Z_n \to Z_n$ are of the form $\phi(x) = x\phi(1)$. Then, by Property 6 of Theorem 15.1, we must have $\phi(1) = 1$. So $\phi(x) = x$ is the only isomorphism from $Z_n$ to itself.

# Exercise 24

Recall that a ring element $a$ is called an idempotent if $a^2 = a$. Prove that a ring homomorphism carries an idempotent to an idempotent.

Let $\phi$ be a ring homomorphism and let $a$ be an idempotnent in the domain of $\phi$. Then $\phi(a)^2 = \phi(a^2) = \phi(a)$ by Property 1 of Theorem 15.1.

# Exercise 36

Determine all ring homomorphisms from $Q$ to $Q$.

By Exercise 40 of Chapter 6, all such homomorphisms are of the form $\phi(x) = x\phi(1)$. (A ring homomorphism must also be a group homomorphism.) Furthermore, since we must have $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$, $\phi(1)$ must be an idempotent of $Q$. But the only idempotents are 0 and 1. So $\phi(x) = x$ and $\phi(x) = 0$ are the only two homomorphisms of $Q$ to itself.

# Exercise 48

Suppose that $n$ divides $m$ and that $a$ is an idempotent of $Z_n$ (that is, $a^2 = a$). Show that the mapping $x \to ax$ is a ring homomorphism from $Z_m$ to $Z_n$. Show that the same correspondence need not yield a ring homomorphism if $n$ does not divide $m$.

Let $\phi : Z_m \to Z_n$ be defined as $\phi(x) = ax$ for an idempotent $a$ of $Z_n$. In considering whether $\phi$ is well defined, we have to ask ourselves: for $x, y \in Z_m$, if $x \equiv y \pmod{m}$, then do we have $\phi(x) \equiv \phi(y) \pmod{n}$? Well, if $n|m$ and $m|(x-y)$, then $n|(x-y) \implies n|a(x-y) = ax - ay$. So $\phi$ is well defined. We can now go on to show the $\phi$ preserves addition and multiplication. We have

$$\phi(x + y) = a(x + y) = ax + ay = \phi(x) + \phi(y),$$

and since $a$ is an idempotent of $Z_n$, we have

$$\phi(xy) = axy = a^2xy = axay = \phi(x)\phi(y).$$

Suppose now that $m = 2$ and $n = 3$. Let $a = 1$. Notice that while $0 \equiv 2 \pmod{2}$, we have $\phi(0) = 0 \not\equiv 2 = \phi(2) \pmod{3}$.

# Exercise 53

Let $D$ be an integral domain and let $F$ be the field of quotients of $D$. Show that if $E$ is any field that contains $D$, then $E$ contains a subfield that is ring-isomorphic to $F$. (Thus, the field of quotients of an integral domain $D$ is the smallest field containing $D$.)

Let $\phi : F \to E$ be a function defined as $\phi(a/b) = ab^{-1}$, where $a, b \in D$ with $b \neq 0$. To see that this is a well defined function, let $a', b' \in D$ such that $a/b = a'/b'$. It follows that $ab' = a'b$, so $ab^{-1} = a'b(b')^{-1}b^{-1} = a'(b')^{-1}$, showing that $\phi$ is indeed well defined. Now let $x, y \in D$ with $y \neq 0$ and see that

$$\begin{aligned}
\phi\left(\frac{a}{b} + \frac{x}{y}\right) &= \phi\left(\frac{ay + bx}{by}\right) \\
&= (ay + bx)(by)^{-1} \\
&= ab^{-1} + xy^{-1} \\
&= \phi\left(\frac{a}{b}\right) + \phi\left(\frac{x}{y}\right),
\end{aligned}$$

showing that $\phi$ preserves addition. We then see that

$$\phi\left(\frac{ax}{by}\right) = (ax)(by)^{-1} = ab^{-1}xy^{-1} = \phi\left(\frac{a}{b}\right)\phi\left(\frac{x}{y}\right),$$

showing that $\phi$ preserves multiplication. It follows that $\phi$ is a homomorphism from $F$ to $E$.

Now see that $\ker \phi = \{0/1\}$, since if $ab^{-1} = 0$ and $b^{-1} \neq 0$, we must have $a = 0$. Then since $\phi$ is clearly onto $\phi(F)$, it follows from Property 7 of Theorem 15.1 that $\phi(F)$ is ring-isomorphic to $F$. Now realize that $\phi(F)$ is a subfield of $E$.