# Chapter 14 Exercises
# Gallian's Book on Abstract Algebra

Spencer T. Parkin

March 4, 2014

## Understanding Example 7

Let $R$ be the ring of all real-valued functions of a real variable. The subset $S$ of all differentiable functions is a subgring of $R$ but not an ideal of $R$.

Let $f$ be any real-valued function of a real variable that is not differential and let $g$ be such a function that is differentiable. Now notice that the function $h(x) = f(x)g(x)$ is not differentiable.

## Understanding Example 15

If it can be shown that $A$ contains a non-zero real number $c$, then, by virtue of being an ideal, it absorbs all elements of $R[x]$, so all $f(x)c$ with $f(x) \in R[x]$ is all of $R[x]$, showing that $A = R[x]$.

## Exercise 3

Verify that the set $I$ in Example 5 is an ideal and that if $J$ is any ideal of $R$ that contains $a_1, a_2, \ldots, a_n$, then $I \subseteq J$. (Hence, $\langle a_1, a_2, \ldots, a_n \rangle$ is the smallest ideal of $R$ that contains $a_1, a_2, \ldots, a_n$.)

For reference, note that

$$I = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n | r_i \in R\}.$$

Clearly $0 \in I$. If $x, y \in I$, then for elements $x_1, x_2, \ldots, x_n \in R$ and elements $y_1, y_2, \ldots, y_n \in R$, we have

$$\begin{aligned} x - y &= x_1 a_1 + x_2 a_2 + \cdots + x_n a_n - (y_1 a_1 + y_2 a_2 + \cdots + y_n a_n) \\ &= (x_1 - y_1)a_1 + (x_2 - y_2)a_2 + \cdots + (x_n - y_n)a_n \in I, \end{aligned}$$

since each $x_i - y_i \in R$. Letting $r \in R$, we have

$$rx = rx_1 a_1 + rx_2 a_2 + \cdots + rx_n a_n \in I,$$

since each $rx_i \in R$.

Now let $J$ be an ideal of $R$ containing $a_1, a_2, \ldots, a_n$, and let $x$ be any element of $I$. As before, let $x = x_1 a_1 + x_2 a_2 + \cdots + x_n a_n$. Now by the definition of what an ideal is, it is clear that each $x_i a_i \in J$, because $x_i \in R$ and $a_i \in J$. Furthermore, $x \in J$, because each $x_i a_i \in J$ and $J$ is a group.

# Exercise 7

Let $a$ belong to a commutative ring $R$. Show that $aR = \{ar | r \in R\}$ is an ideal of $R$. If $R$ is the ring of even integers, list the elements of $4R$.

Clearly the additive identity is in $aR$, since $0 = a \cdot 0$. Let $x, y \in aR$. Then there exist elements $r_x, r_y \in R$ such that $x = ar_x$ and $y = ar_y$. We then have $x - y = ar_x - ar_y = a(r_x - r_y) \in aR$ since $r_x - r_y \in R$. Now let $r \in R$ and see that $rx = rar_x = arr_x \in aR$ since $rr_x \in R$. It follows that $aR$ is an ideal of $R$.

In that case, $4R = \{0, \pm 8, \pm 16, \pm 24, \pm 32, \ldots\}$, I think.

# Exercise 9

If $n$ is an integer greater than 1, show that $\langle n \rangle = nZ$ is a prime ideal of $Z$ if and only if $n$ is prime.

Notice that $nZ$ is an ideal of $Z$ by Exercise 7.

Suppose $n$ is prime. Let $a, b \in Z$ such that $ab \in nZ$. Then there exists $z \in Z$ such that $ab = nz$. It follows that $n | ab$ which implies that $n | a$ or $n | b$ by Euclid's Lemma. So there exists $z' \in Z$ such that $a = nz' \in nZ$ or $b = nz' \in nZ$, showing that $nZ$ is a prime ideal of $Z$.

Now suppose $nZ$ is a prime ideal of $Z$. Then if $a, b \in Z$ such that $ab = nz$ for some $z \in Z$, we must have, for some $z' \in Z$, $a = nz'$ or $b = nz'$. In other words, if $n|ab$, we must have $n|a$ or $n|b$ in every case. There is no composite number that can do this, so $n$ must be prime. (We can also conclude $n$ is prime by continually factoring what $n$ divides, and then know that $n$ divides one of the factors. Repeating, we're eventually left with only one prime factor.)

# Exercise 10

If $A$ and $B$ are ideals of a ring $R$, show that the sum of $A$ and $B$, $A + B = \{a + b | a \in A, b \in B\}$, is an ideal.

Notice that $0 \in A + B$. Then, if $x, y \in A + B$, then there exist elements $a_x, a_y \in A$ and $b_x, b_y \in B$ such that $x = a_x + b_x$ and $y = a_y + b_y$. Then $x - y = a_x - a_y + b_x - b_y \in A + B$ since $a_x - a_y \in A$ and $b_x - b_y \in B$. Now letting $r \in R$, we see that $rx = ra_x + rb_x \in A + B$, since each one of $A$ and $B$ is a left ideal so that $ra_x \in A$ and $rb_x \in B$. Similarly, $xr = a_x r + b_x r \in A + B$, since each one of $A$ and $B$ is a right ideal so that $a_x r \in A$ and $b_x r \in B$. We can now claim that $A + B$ is an ideal by Theorem 14.1.

# Exercise 12

If $A$ and $B$ are ideals of a ring $R$, show that the product of $A$ and $B$, $AB = \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n | a_i \in A, b_i \in B, n \text{ a positive integer}\}$, is an ideal.

Clearly $0 \in AB$. Let $x, y \in AB$. Then there exist elements $a_i, u_i \in A$ and $b_i, v_i \in B$ such that $x = a_1 b_1 + \cdots + a_m b_m$ and $y = u_1 v_1 + \cdots + u_n v_n$ for positive integers $m$ and $n$. Now realize that $x - y \in AB$, since $-u_i \in A$ and $m + n$ is a positive integer. Now for any $r \in R$, notice that $rx \in AB$ since $A$ is an ideal, and $xr \in AB$ since $B$ is an ideal. So $AB$ is an ideal by the Ideal Test (Theorem 14.1).

# Exercise 14

Let $A$ and $B$ be ideals of a ring. Prove that $AB \subseteq A \cap B$.

Let $x \in AB$. Then for $a_i \in A$, $b_i \in B$ and a positive integer $n$, we have $x = a_1 b_1 + \cdots + a_n b_n$. Now notice that for each integer $i$, $a_i b_i \in A$ since $A$ is an ideal, and $a_i b_i \in B$ since $B$ is an ideal. Then since $A$ and $B$ are groups, $x \in A \cap B$.

## Exercise 15

If $A$ is an ideal of a ring $R$ and 1 belongs to $A$, prove that $A = R$.

Since $A$ is an ideal of $R$ and $1 \in A$, we have, for all $r \in R$, $r = 1r \in A$, showing that $A = R$.

## Exercise 21

Verify the claim made in Example 10 about the size of $R/I$.

For reference,

$$R = \left\{ \left[ \begin{array}{cc} a_1 & a_2 \\ a_3 & a_4 \end{array} \right] \middle| a_i \in Z \right\}$$

and $I$ is the subset of $R$ consisting of matrices with even entries.

The example in the text helps make the verification easy. Let $M \in R$. Then the coset $M+I = B+I$, where $B$ is a matrix consisting of just ones and zeros. Since the matrices have 4 possible entries, there are $2^4 = 16$ possible elements in $R/I$.

## Exercise 23

Show that the set $B$ in the latter half of the proof of Theorem 14.4 is an ideal of $R$.

For reference, $B = \{br + c | r \in R, a \in A\}$ with $b \in R - A$. The subset $A$ is an ideal of $R$, and $R$ is a commutative ring with unity.

Letting $x \in R$, we must show that for any $y \in B$, that $xy \in B$ and $yx \in B$. Let $y = br + a$ for elements $r \in R$ and $a \in A$. Then $xy = bxr + xa \in B$ since $xr \in R$ and $xa \in A$. (Remember that $A$ is an ideal of $R$.) And we have $yx = bry + ay \in B$ since $ry \in R$ and $ay \in A$.

# Exercise 30

Let $R = Z_8 \oplus Z_{30}$. Find all maximal ideals of $R$, and for each maximal ideal $I$, identify the size of the field $R/I$.

Let's start by looking for all maximal subgroups of $R$. By inspection, but mostly by reasoning, I believe these are $2Z_8 \oplus Z_{30}$, $Z_8 \oplus 2Z_{30}$, $Z_8 \oplus 3Z_{30}$ and $Z_8 \oplus 5Z_{30}$. Which of these are ideals? In part, Exercise 7 can be used to say that all of them are, so they're all maximal ideals. (The other part is realizing that the other cyclic group taken in the product is just "along for the ride" when performing the ideal test.) Being maximal, the factor rings generated by these ideas are fields of orders $8/2 \cdot 30$, $8 \cdot 30/2$, $8 \cdot 30/3$ and $8 \cdot 30/5$, respectively. Have I missed something? Alas, no one but me will ever view this.

# Exercise 34

Let $R$ be a ring and let $I$ be an ideal of $R$. Prove that the factor ring $R/I$ is commutative if and only if $rs - sr \in I$ for all $r$ and $s$ in $R$.

For any two elements $a, b \in R$, two elements of $R/I$ are $a + I$ and $b + I$. Now realize that $ab + I = (a + I)(b + I) = (b + I)(a + I) = ba + I$ if and only if $ab - ba \in I$ by Property 4 on Page 138, (6th Ed.)

# Exercise 38

Let $R$ be a ring and let $p$ be a fixed prime. Show that $I_p = \{r \in R|$ additive order of $r$ is a power of $p\}$ is an ideal of $R$.

Notice that the additive identity is in $I_p$. Now for any pair of elements $x, y \in I_p$, let them have additive orders $p^m$ and $p^n$, respectively. Now notice that if $k = mn$, then $p^k \cdot (x - y) = p^k \cdot x - p^k \cdot y = 0$, showing that the additive order of $x - y$ divides $p^k$ by Corollary 2 of Theorem 4.1. So since $p$ is prime, we have $x - y \in I_p$. Similarly, letting $r \in R$ be any element, notice that $p^m \cdot xr = (p^m \cdot x)r = 0 \cdot r = 0$, showing that the additive order of $xr$ divides $p^m$. Also, $p^m \cdot rx = r(p^m \cdot x) = r \cdot 0 = 0$, showing that the additive order of $rx$ divides $p^m$ also. So $xr$ and $rx$ are in $I_p$.

## Exercise 42

Let $R$ be a commutative ring and let $A$ be any ideal of $R$. Show that the nil radical of $A$, $N(a) = \{r \in R | r^n \in A$ for some positive integer $n$ ($n$ depends on $r$)$\}$, is an ideal of $R$. [$N(\langle 0 \rangle)$ is called the nil radical of $R$.]

Clearly $0 \in N(A)$. Then if $x, y \in N(A)$, then there exist integers $m$ and $n$ such that $x^m \in A$ and $y^m \in A$. Now choose an integer $k$ so that for all integers $i \in [0, k]$, we have $i \geq m$ or $k - i \geq n$. It then follows that

$$(x-y)^k = \sum_{i=1}^{k} \binom{k}{i} x^i y^{k-i} \in A,$$

since $A$ is a left and right ideal. So $x - y \in N(A)$. Now notice that $(rx)^m = r^m x^m \in A \implies rx \in N(A)$, since $R$ is commutative and $A$ is an ideal. We need not check that $xr \in N(A)$, since $R$ is commutative.

## Exercise 43

Let $R = Z_{27}$ Find $N(\langle 0 \rangle), N(\langle 3 \rangle), N(\langle 9 \rangle)$.

By inspection, we have

$$N(\langle 0 \rangle) = N(\langle 3 \rangle) = N(\langle 9 \rangle) = \langle 3 \rangle,$$

if I didn't make a mistake. Is there a general result these observations could lead us to?

## Exercise 44

Let $R = Z_{36}$. Find $N(\langle 0 \rangle), N(\langle 4 \rangle), N(\langle 6 \rangle)$.

I think we have $N(\langle 0 \rangle) = \langle 6 \rangle$, $N(\langle 4 \rangle) = \langle 2 \rangle$ and $N(\langle 6 \rangle) = \langle 6 \rangle$. Exercise 46 seems to agree.

## Exercise 46

Let $A$ be an ideal of a commutative ring. Prove that $N(N(A)) = N(A)$.

Notice that $x \in N(N(A)) \implies x^n \in N(A) \implies x^{nm} = (x^n)^m \in A \implies x \in N(A)$. Then see that $x \in N(A) \implies x^n \in A \implies x^n \in N(A) \implies x \in N(N(A))$. This can seem a bit tricky, but it all falls out.

# Exercise 56

Let $R$ be a commutative ring with unity and let $I$ be a proper ideal with the property that every element of $R$ that is not in $I$ is a unit of $R$. Prove that $I$ is the unique maximal ideal of $R$.

Suppose $J$ is an ideal of $R$ properly containing $I$. Let $x \in J - I$. Then $x^{-1} \in J$ and $1 = xx^{-1} \in J$, so $J = R$, (since it absorbs all of $R$ through the unity.) This proves that $I$ is maximal. Suppose now that $J$ is any other maximal ideal of $R$. Then $J \cap (R - I)$ is non-empty. So, letting $x \in J \cap (R - I)$, we see that $1 = xx^{-1} \in J$ and $J = R$, which is a contradiction. It follows that there is no other maximal ideal of $R$. This proves that $I$ is unique.