Chapter 12 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

March 3, 2014

Exercise 14

Let a and b belong to a ring R and let m be an integer. Prove that $m\cdot(ab) = (m\cdot a)b = a(m\cdot b)$.

Notice that

$$m\cdot(ab) = \underbrace{ab+\cdots+ab}_{m} = a(\underbrace{b+\cdots+b}_{m}) = a(m\cdot b).$$

A proof that $m\cdot(ab) = (m\cdot a)b$ is similar. This is just repeated use of the distributive properties. We might have used induction, I suppose; but that seems like over-kill.

Exercise 15

Show that if m and n are integers and a and b are elements from a ring, then $(m\cdot a)(n\cdot b) = (mn)\cdot(ab)$.

Notice that

$$\begin{aligned}(m\cdot a)(n\cdot b) &= (m\cdot a)(\underbrace{b+\cdots+b}_{n})\\ &= \underbrace{(m\cdot a)b+\cdots+(m\cdot a)b}_{n}\\ &= \underbrace{m\cdot(ab)+\cdots+m\cdot(ab)}_{n} = (nm)\cdot(ab).\end{aligned}$$

Exercise 17

Show that a ring that is cyclic under addition is commutative.

Let $R = \langle g \rangle$ and let $a, b \in R$. Then there exist integers m and n such that $a = m \cdot g$ and $b = n \cdot g$. Now notice that

$$ab = (m \cdot g)(n \cdot g) = (mn) \cdot g^2 = (nm) \cdot g^2 = (n \cdot g)(m \cdot g) = ba$$

by Exercise 15.

Exercise 18

Let a belong to a ring R. Let $S = \{x \in R | ax = 0\}$. Show that S is a subgring of R.

Notice that $0 \in S$, which we must have if S is to be an Abelian group. Now let $x \in S$, and see that $a(-x) = -(ax) = -0 = 0$, showing that $-x \in S$. Now let $x, y \in S$, and see that $a(x + y) = ax + ay = 0 + 0 = 0$, showing that $x + y \in S$. Thus far we have shown that S is a group under the additive operation of R. Letting $x, y \in S$ once again, see that $axy = (ax)y = 0 \cdot y = 0$, showing that $xy \in S$. We can now claim by Theorem 12.3 that S is a subring of R.

Exercise 22

Let R be a commutative ring with unity and let $U(R)$ denote the set of units of R. Prove that $U(R)$ is a group under the multiplication of R. (This group is called the *group of units of* R.)

Seeing that the unity 1 of R is a unit, we have $1 \in U(R)$, so $U(R)$ is not empty. Now notice that $x \in U(R)$ if and only if $x^{-1} \in R$ exists, and clearly $(x^{-1})^{-1} = x$, so $x^{-1} \in U(R)$ too. Now let $x, y \in U(R)$. Then, seeing that $(xy)^{-1} = y^{-1}x^{-1} \in R$, we must have $xy \in U(R)$. Why did R need to be a commutative ring? Did I miss something?

Exercise 30

Suppose that there is an integer $n > 1$ such that $x^n = x$ for all elements x of some ring. If m is a positive integer and $a^m = 0$ for some a, show that $a = 0$.

If $m = 1$, we're done. So let $m > 1$.

If $n > m$, then let $n = m + k$ and we have $a = a^n = a^m a^k = 0 \cdot a^k = 0$. If $n = m$, then $0 = a^m = a^n = a$. If $n < m$, then let $m_1 = m$ and we have $0 = a^{m_1} = a^n a^{m_1 - n} = a^{m_1 - n + 1}$. If we then let $m_2 = m_1 - n + 1$, we're done if $m_2 \leq n$; otherwise, we have $m_2 < m_1$, and $0 = a^{m_2} = a^n a^{m_2 - n} = a^{m_2 - n + 1}$. Now let $m_3 = m_2 - n + 1$, and continue this process, which must terminate with the conclusion that $a = 0$.

Exercise 36

Let m and n be positive integers and let k be the least common multiple of m and n. Show that $mZ \cap nZ = kZ$.

If $x \in mZ \cap nZ$, then x is a multiple of m and n. But $\mathrm{lcm}(m, n)$ divides all such multiples, so there exists $z \in Z$ such that $x = zk \implies x \in kZ$. Now if $x \in kZ$, there exists $z \in Z$ such that $x = zk = z\mathrm{lcm}(m, n)$. So x is a multiple of n and m. But $mZ \cap nZ$, by construction, contains all such multiples. So $x \in mZ \cap nZ$.