Chapter 13 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

March 3, 2014

Understanding Examples 5 and 6

Let us show that Z_n is an integral domain if and only if n is prime.

Suppose n is prime and let $a, b \in Z_n$ such that $ab = 0$. Then $n|ab$, and so, by Euclid's lemma, $n|a$ or $n|b$. It follows that $a = 0$ or $b = 0$, showing that Z_n is an integral domain, because there cannot be any zero divisors, 1 is the unity, and multiplication in Z_n is commutative.

Now suppose that for some $a, b \in Z_n$ with $ab = 0$, we have neither $a = 0$ nor $b = 0$. (That is, suppose Z_n is not an integral domain.) Then, by Euclid's Lemma one again, n is not prime.

Understanding Theorem 13.2 Better

Notice that no element in the sequence $a, a^2, a^3, \ldots$ is zero, because D is an integral domain. After seeing that there must be $i > j$ such that $a^i = a^j$, write $a^{i-j}a^j = a^j \implies a^j(a^{i-j}-1) = 0$. (Remember that D is a commutative ring.) We can now claim that $a^{i-j} = 1$ by the property that D has no zero divisors. The rest is easy.

Exercise 13

Let a belong to a ring R with unity and suppose that $a^n = 0$ for some positive integer n. (Such an element is called *nilpotent*.) Prove that $1-a$ has a multiplicative inverse in R. [*Hint*: Consider $(1-a)(1+a+a^2+\cdots+a^{n-1})$.]

Notice that $1 = 1 - a^n = (1-a)(1 + a + a^2 + \cdots + a^{n-1})$. Now realize that we cannot have $1 + a + a^2 + \cdots + a^{n-1} = 0$, because $0 \neq 1$.

Exercise 14

Show that the nilpotent elements of a commutative ring form a subgring.

Let R be a ring and let $N(R)$ denote the set of all nilpotents in R. Clearly $N(R) \subseteq R$. Notice that $0 \in N(R)$, since any power of zero is clearly zero. Now let $a, b \in N(R)$. Then if $a^m = 0$ and $b^n = 0$ for integers m and n, then clearly $a^k = 0$ and $b^k = 0$ if $k = \max\{m, n\}$. Then, by the commutativity of R, it follows that $(ab)^k = a^k b^k = 0$, showing that $ab \in N(R)$. Thus we have closure in $N(R)$ for the product of R. Now consider $a - b$. Notice that

$$(a-b)^{mn} = \sum_{k=0}^{mn} (-1)^k \binom{mn}{k} a^{mn-k} b^k,$$

and that $\min\{\max\{mn - k, k\}\}_{k=0}^{mn} \geq k$. It follows that $(a-b)^{mn} = 0$ and so $a - b \in N(R)$, showing that $N(R)$ is a subgroup of R. We can now claim that $N(R)$ is a subring by Theorem 12.3.

Exercise 16

A ring element a is called *idempotent* if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.

Let a be any element of an integral domain for which $a^2 = a$. We then see that $a(a-1) = 0$. It then follows that $a = 0$ or $a - 1 = 0 \implies a = 1$ by the non-existence of zero divisors in the domain.

Exercise 28

Prove that there is no integral domain with exactly six elements. Can your argument be adapted to show that there is no integral domain with exactly four elements? What about 15 elements? Use these observations to guess a general result about the number of elements in a finite integral domain.

Let D be the finite integral domain in question. Then by the proof of Theorem 13.3, the unity of D must have an additive order of $\operatorname{char} D$.

Furthermore, since any non-unity element $x \in D$ has the property that $(\text{char}\, D) \cdot x = 0$, it follows by Corollary 2 of Theorem 4.1 that the additive order of x divides $\text{char}\, D$. But by Theorem 13.4, we must have $\text{char}\, D$ prime. It follows that all non-zero elements of D have an additive order of $p = \text{char}\, D$. Thus, in considering the size of D, we are left to consider only those Abelian groups where all non-zero elements are of the same prime order p. By the Fundamental Theorem of Finite Abelian Groups, the only groups that fit our current description of D are isomorphic to, for some integer $k \geq 1$, $\bigoplus_{i=1}^{k} Z_p$. So far we can conclude that the size of D is always a power of some prime p. For example, Example 9 exhibits a field, (and therefore an integral domain) of size 3^2.

Back to the original question, we can easily rule out integral domains of size 6 and 15, but not 4. Hmmm...why not 4? By a careful examination of all possibilities for the multiplication table of such a field, it cannot exist. In any case, I'm not sure that I have reached the general result sought after by the author of this exercise's problem statement.

Exercise 38

Suppose that a and b belong to a commutative ring and ab is a zero-divisor. Show that eithe ra or b is a zero-divisor.

Since ab is a zero-divisor, $ab \neq 0$, so $a \neq 0$ and $b \neq 0$. Furthermore, there exists $c \neq 0$ in the ring such that $abc = 0$. Now if $bc \neq 0$, it follows that a is a zero-divisor. If $bc = 0$, then b is a zero-divisor.

Exercise 41

Let x and y belong to a commutative ring R with $\text{char}\, R = p \neq 0$. Show that $(x+y)^p = x^p + y^p$. Show that, for all positive integers n, $(x+y)^{p^n} = x^{p^n} + y^{p^n}$. Find elements x and y in a ring of characteristic 4 such that $(x+y)^4 \neq x^4 + y^4$.

Note that the case $n = 1$ is covered in the general case, so only the general case will be shown. Also, it is assumed that p is prime, although this was not specifically stated. (It must have been meant as it is needed.)

First note that

$$(x+y)^{p^n} = \sum_{i=1}^{p^n} \binom{p^n}{i} x^i y^{p^n - i}.$$

The crux of the proof then comes in realizing that only when p is prime is it true that p divides $\binom{p^n}{i}$ whenever $i > 0$ and $i < p^n$. To see this, we expand the binomial coeficient as

$$\binom{p^n}{i} = \frac{p^n(p^n-1)!}{i!(p^n-i)!} = p^n \frac{(p^n-1)(p^n-2)\dots(p^n-i+1)}{i!}.$$

Now notice that when $i > 0$ and $i < p^n$, a multiple of p always survives any cancellation that may occur in the fraction. (More rigor could be given here, but it is true.)

Returning to the expansion of $(x+y)^{p^n}$, we see that, for some integer s, the general term is of the form

$$psx^i y^{p^n-i} = (px)sx^{i-1}y^{p^n-i} = 0 \cdot sx^{i-1}y^{p^n-i} = 0,$$

whenever $i > 0$ and $i < p^n$, since for any $x \in R$, we must have $px = 0$. When $i = 0$ or $i = p^n$, the term survives, and we're left with $x^{p^n} + y^{p^n}$.

For the example, consider Z_4. Notice that $0 = (1+3)^4 \neq 1^4 + 3^4 = 2$.

Exercise 42

Let R be a commutative ring with unity 1 and prime characteristic. If $a \in R$ is nilpotent, prove that there is a positive integer k such that $(1+a)^k = 1$.

Let m be an integer such that $a^m = 0$. Now choose an integer n such that $(\operatorname{char} R)^n \geq m$. We then have, by Exercise 41, $(1+a)^k = 1$, if $k = (\operatorname{char} R)^n$.

Exercise 43

Show that any finite field has order p^n, where p is prime.

See Exercise 28 above.

Exercise 56

Suppose that a and b belong to a field of order 8 and that $a^2 + ab + b^2 = 0$. Prove that $a = 0$ and $b = 0$. Do the same when the field has order 2^n with n odd.

Notice that there must be an element of the field with an additive order equal to the characteristic of the field. Then, by Legrange's Theorem, this

characteristic must divide the order of the field. It follows that the characteristic is 2, because it must be finite and therefore prime by Theorem 13.4. It then follows by Exercise 41 that $ab = (a+b)^2 = a^2 + b^2$. So we have $0 = a^2 + ab + b^2 = 2ab$ which implies that $a = 0$ or $b = 0$. Suppose, without loss of generality, that $a = 0$. Then $b^2 = 0 \implies b = 0$ by Exercise 15.