Selected exercises from *Abstract Algebra* by *Dummit and Foote* (3rd edition).

Bryan Félix

Abril 12, 2017

Section 7.1

Exercise 5. *Decide which of the following are subrings of* $\mathbb{Q}$*:*

(a) the set of all rational numbers with odd denominators (when written in lowest terms)

Proof. Indeed, the set is a subring. First we show that it is a subgroup of $\mathbb{Q}$ by means of the subgroup criterion; i.e.
Let $\frac{a}{b}, \frac{c}{d}$ be in the set. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$$

is a rational number with odd denominator (since both b and d are odd). Furthermore

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

is in the set by the same argument. Hence, the set is closed under multiplication, proving itself a subring. □

(b) the set of all rational numbers with even denominators (when written in lowest terms)

Proof. The set is not a subring as it ain't a group. Observe that $\frac{1}{2}$ and $\frac{1}{6}$ are in the set, but

$$\frac{1}{2} - \frac{1}{6} = \frac{1}{3}$$

is not. □

(c) The set of nonnegative rational numbers

Proof. Again, the set is not a subring since it is not a subgroup. Note that 1 and 3 are in the set, but $1 - 3 = -2$ is not. □

(d) the set of squares of rational numbers

Proof. Again, the set is not a subring since it ain't a subgroup. Note that $\frac{1}{4}$ is in the set, but $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$ is not since $\frac{1}{2}$ is not the square of a rational number. □

(e) the set of all rational numbers with odd numerators (when written in lowest terms)

Proof. Again, the set is not a subring because it is not a group. Note that $\frac{1}{3}$ is in the set, but $\frac{1}{3} + \frac{1}{3} = \frac{2}{3}$ is not. □

(f) the set of all rational numbers with even numerators (when written in lowest terms)

Proof. The set is a subring. Note that the set is not empty ($\frac{2}{3}$ is an element). We show that the set is a subgroup by means of the subgroup criterion.
Let $\frac{2a}{b}$ and $\frac{2c}{d}$ be elements of the group. Note that both b and d are odd, otherwise the fraction is not written in lowest terms. Furthermore

$$\frac{2a}{b} - \frac{2c}{d} = \frac{2(ad - bc)}{bd}$$

is an element of the set, since the product bd is still odd and therefore, the factor 2 in the numerator survives. Then, the set is closed under multiplication, note that $\frac{2a}{b} \cdot \frac{2c}{d} = \frac{2(2ac)}{bd}$. □

Exercise 12. *Prove that any subring of a field which contains the identity is an integral domain.*

Proof. By construction, 1 is already in the set. Now we assume that the set is not an integral domain, and therefore, there exist two non-zero elements a and b, such that $ab = 0$. Since a and b are element of a field, they have multiplicative inverses and therefore the following holds

$$a^{-1}ab = a^{-1}0.$$

Equivalently $b = 0$, a contradiction to the assumption that both a and b were non-zero elements. □

Exercise 14. *Let x be a nilpotent element of a commutative ring R.*

(a) Prove that x is either zero or a zero divisor.

Proof. Assume that $x^n = 0$, where n is the least positive integer that satisfies the equation. Then $x \cdot x^{n-1} = 0$, and therefore x is a zero divisor. □

(b) Prove that rx is nilpotent for all $r \in R$.

Proof. Let n be defined as in part (a). Then, since the ring is commutative, $(rx)^n = r^n x^n = 0$ as desired. □

(c) Prove that $1 + x$ is a unit in R.

Proof. Note that

$$(1 + x)(1 - x + x^2 - \cdots \pm x^{n-1}) = (1 \pm x^n) = (1 + 0) = 1.$$

Therefore $1 + x$ has a multiplicative inverse, and hence, it is a unit. □

(d) Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. Let a be a unit and x be a nilpotent element with $x^n = 0$. Then, $a + x = a(1 + a^{-1}x)$ where $a^{-1}x$ is nilpotent by part (b). Then, by part (c), $(1 + a^{-1}x)$ is a unit, and therefore $a(1 + a^{-1}x$ has a n inverse, namely, $(1 + a^{-1}x)^{-1}a^{-1}$. □

Exercise 26. *Let K be a field. A* discrete valuation *on K is a function $v : K^\times \to \mathbb{Z}$ satisfying*

(i) $v(ab) = v(a) + v(b)$

(ii) v *is surjective, and*

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ *for all* $x, y \in K^\times$ *with* $x + y \neq 0$.

The set $R = \{x \in K^\times | v(x) \geq 0\} \cup \{0\}$ *is called the valuation ring of* v.

(a) Prove that R is a subring of K which contains the identity.

Proof. Note that the homomorphism characterization of v guarantees that 1 is in R as $v(1) = 0$. Now we will show that R is a subgroup of the field by means of the subgroup criterion.
Let a and b be elements of R. We want to prove that $a - b$ is also an element of R. Assume that $a - b \neq 0$ (otherwise $a - b$ is in R by construction) and observe that

$$v(a-b) = v(a+(-b)) \geq \min\{v(a), v(-b)\} = \min\{v(a), v(-1 \cdot b)\} = \min\{v(a), v(-1)+v(b)\}.$$

Note that $0 = v(1) = v(-1 \cdot -1) = v(-1) + v(-1) = 2v(-1)$, therefore $v(-1) = 0$ and $v(a - b) \geq \min\{v(a), v(b)\} \geq 0$ as both a and b are in R. It follows that $a - b$ is in R and therefore R is an subgroup of the field.
It is left to show that the group is closed under multiplication, to that end, note that for arbitrary a and b in R

$$v(ab) = v(a) + v(b) \geq 0 + 0 \geq 0.$$

We conclude that R is a subring that contains the multiplicative identity. □

(b) Prove that for each nonzero element $x \in K$ either x or x^{-1} is in R.

Proof. Observe that

$$v(x \cdot x^{-1}) = v(x) + v(x^{-1}) = v(1) = 0$$

and assume that x is not in R. Then $v(x) < 0$ and the previous identity forces $v(x) + v(x^{-1}) = 0$. It follows that $v(x^{-1}) = -v(x) > 0$. Hence x^{-1} is in R. □

(c) Prove that an element x is a unit of R if and only if $v(x) = 0$.

Proof. Assume x is a unit of R. Then, both $v(x) \geq 0$ and $v(x^{-1}) \geq 0$. Furthermore

$$v(x) + v(x^{-1}) = v(xx^{-1}) = v(1) = 0.$$

The previous equation is satisfied only if $v(x) = v(x^{-1}) = 0$.
Now assume that $v(x) = 0$, then $v(x^{-1}) = -v(x)$ (by part (b)) and it follows that $v(x^{-1}) = 0$. Therefore x^{-1} is in R and x is a unit in R. □

Section 7.2

Exercise 5. *Let F be a field and define the ring $F((x))$ of formal Laurent series with coefficients from F by*

$$F((x)) = \left\{ \sum_{n \geq N}^{\infty} a_n x^n \ ; \ a_n \in F \text{ and } N \in \mathbb{Z} \right\}.$$

(a) *Prove that $F((x))$ is a field.*

Proof. We prove the properties of a Field

i. $F((x))$ is an abelian group under addition.
Note that

$$\sum_{n \geq N}^{\infty} a_n x^n + \sum_{n \geq M}^{\infty} b_n x^n = \sum_{n \geq \min\{N,M\}}^{\infty} (a_n + b_n) x^n$$

where we extend the series by using 0 coefficients if necessary. Likewise

$$\sum_{n \geq M}^{\infty} b_n x^n + \sum_{n \geq N}^{\infty} a_n x^n = \sum_{n \geq \min\{N,M\}}^{\infty} (b_n + a_n) x^n.$$

Since a_i and b_i are elements of a field, the previous resulting sums are equal. Associativity and closure of $+$ follows from the properties of polynomials. Lastly, the additive inverse of the element $\sum a_n x^n$ for $n \geq N$ is the sum $\sum(-a_n)x^n$.

ii. Multiplication distributes over addition and is commutative.
Note that

$$\sum_{n \geq N}^{\infty} a_n x^n \left(\sum_{n \geq M}^{\infty} b_n x^n + \sum_{n \geq L}^{\infty} c_n x^n \right) = \sum_{n \geq N}^{\infty} a_n x^n \left(\sum_{n \geq \min\{M,L\}}^{\infty} (b_n + c_n) x^n \right)$$

To inspect the coefficients of the product we let $d_i = (b_i + c_i)$ and $K = \min\{M, L\}$ and we inspect the following multiplication table

	a_N	a_{N+1}	a_{N+2}	a_{N+3}	$\cdots$
d_K	$d_K a_N$	$d_K a_{N+1}$	$d_K a_{N+2}$	$d_K a_{N+3}$	$\cdots$
d_{K+1}	$d_{K+1} a_N$	$d_{K+1} a_{N+1}$	$d_{K+1} a_{N+2}$	$d_{K+1} a_{N+3}$	$\cdots$
d_{K+2}	$d_{K+2} a_N$	$d_{K+2} a_{N+1}$	$d_{K+2} a_{N+2}$	$d_{K+2} a_{N+3}$	$\cdots$
d_{K+3}	$d_{K+3} a_N$	$d_{K+3} a_{N+1}$	$d_{K+3} a_{N+2}$	$d_{K+3} a_{N+3}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$

Note that the coefficient of the term x^i are represented as diagonal sums of the entries of the table. Also, the order of multiplication is not important as all the entries come from a field. Furthermore, every coefficient is of the form $a_j \cdot (b_i + c_i) a_i$ and since the distributive property holds in F then every coefficient in our table can be rewritten as $a_j b_i + a_j c_i$ which proves the associative property. Commutativity follows in the same manner by rewriting $d_i a_j$ as $a_j d_i$.

iii. There is a multiplicative identity.
Our good ol' friend 1_F (the unit in F) satisfies.

iv. We have multiplicative inverses.
We claim that the multiplicative inverse of

$$\sum_{n\geq N}^{\infty} a_n x^n$$

exist and is of the form

$$\sum_{n\geq -N}^{\infty} b_n x^n.$$

This is clear from our multiplication table. The first term (in the upper left corner) is the coefficient $a_N b_{-N}$ of x^0. We can solve for b_{-N} explicitly as F is an integral domain and $a_N b_{-N} = 1_F$. A close inspection to the multiplicative table shows that the next coefficient, namely b_{-N+1}, is given in terms of a_N and b_{-N} and therefore can be solved explicitly. Analogously all the terms in $\sum_{n\geq -N}^{\infty} b_n x^n$ can be found so that the product evaluates to 1_F.

We conclude that $F((x))$ is a field. □

(b) *Define the map*

$$v : F((x))^\times \to \mathbb{Z} \quad \text{by} \quad v\left(\sum_{n\geq N}^{\infty} a_n x^n\right) = N$$

Prove that v is a discrete valuation on $F((x))$ whose discrete valuation ring is $F[[x]]$, the ring of formal power series.

Proof. We prove the properties of a discrete valuation

(i) $v(ab) = v(a) + v(b)$.
Note that the valuation is keeping track of the least exponent in the series. This property follows from the expansion of the product of two polynomial. It is also clear from the multiplication table in the first part,

(ii) v is surjective.
Trivial. take the element $\sum_{n\geq z}^{\infty} a_n x^n$ (defined for all $z \in \mathbb{Z}$). Then $v(x) = z$.

(iii) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K^\times$ with $x + y \neq 0$.
For this field in particular we have equality. This follows form part (a) of the exercise.

□

Section 7.3

Exercise 4. *Find all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/30\mathbb{Z}$. In each case describe the kernel and the image.*

Proof. Observe that since 1 is a generator for $\mathbb{Z}$ it suffices to define the homomorphism φ for 1. Furthermore note the following

$$\varphi(1) = \varphi(1 \cdot 1)\varphi(1)\varphi(1) = (\varphi(1))^2 .$$

In order to preserve the ring multiplicative structure $\varphi(1)$ has to be equal to $\varphi(1)^2$ modulo 30. Then we need to solve the equation $a = a^2 \mod 30$, or equivalently, $a(a-1) = 0 \mod 30$. Since $30 = 2 \cdot 3 \cdot 5$, we inspect the numbers such that either a or $a-1$ are multiples of 5, namely

$$\{0, 1, 5, 6, 10, 11, 15, 16, 20, 21, 25, 26\}.$$

Out of these possibilities is easy to do a check which ones satisfy the condition above. We get

$$a = \{0, 1, 6, 10, 15, 16, 21, 25\}.$$

Each of these defines an homomorphism by with $\varphi(1) = a$.
Now, for the kernel of $\varphi(1) = a$, note that

$$\varphi(n) = \varphi\left(\sum_{n=1}^{n} 1\right) = \sum_{i=1}^{n} \varphi(1) = n\varphi(1) = n \cdot a.$$

Then, n is in the kernel if $n \cdot a = 0 \mod 30$. Since a was constructed by having **some** of the factors of 30, the number n would have to make up for the other ones. Therefore

$$n = \frac{30}{\gcd(30, a)}.$$

We conclude that the kernel of φ is the set of all integer multiples of n as defined above. □

Exercise 13. *Prove that the ring $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.*

Proof. Let $\varphi : \mathbb{C} \to M_2(\mathbb{R})$ be given by

$$\varphi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Note that

$$\begin{aligned} \varphi((a_1 + b_1 i) + (a_2 + b_2 i)) &= \varphi((a_1 + a_2) + (b_1 + b_2)i) \\ &= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ -(b_1 + b_2) & a_1 + a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \\ &= \varphi(a_1 + b_1 i) + \varphi(a_2 + b_2 i) \end{aligned}$$

and

$$\begin{aligned} \varphi((a_1 + b_1 i) \cdot (a_2 + b_2 i)) &= \varphi((a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i) \\ &= \begin{pmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + a_2 b_1 \\ a_1 b_2 + a_2 b_1 & a_1 a_2 - b_1 b_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \\ \varphi(a_1 + b_1 i) \cdot \varphi(a_2 + b_2 i) \end{aligned}$$

Thus, φ is a ring homomorphism, and it's image is a subring of $M_2(\mathbb{R})$. To prove the isomorphic property, we need to show that the homomorphism, restricted to it's image, is bijective. Note that $\varphi(a+bi) = 0$ if and only if both a and b are zero. Therefore φ is injective and, furthermore, when restricted to its image is a surjection. Hence $\mathbb{C} \cong \mathrm{Im}\,(\varphi)$. □

Exercise 17. *Let R and S be nonzero rings with identity and denote their respective identities by 1_R and 1_S. Let $\varphi : R \to S$ be a nonzero homomorphism of rings.*

(a) Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is a zero divisor in S. Deduce that if S is an integral domain then every ring homomorphism from R to S sends the identity of R to the identity of S.

Proof. Let $\varphi(1_R) = s$. Observe that

$$s = \varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R) \cdot \varphi(1_R) = s^2.$$

Then we have $s = s^2$, and equivalently $s(1 - s) = 0$. Note that $s - 1 \neq 0$ by construction. Now suppose that $\varphi(1_R) = 0$, then, for any r in R

$$\varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\varphi(1_R) = \varphi(r) \cdot 0 = 0$$

and thus, φ is the zero homomorphism, a contradiction. We conclude that $s(s - 1) = 0$ holds for $s \neq 0$ and it follows that s is a zero divisor. Furthermore it follows that if S is an integral domain $\varphi(1_R) = 1_S$. □

(b) Prove that if $\varphi(1_R) = 1_S$ then $\varphi(u)$ is a unit in S and that $\varphi(u^{-1}) = \varphi(u)^{-1}$ for each unit u of R.

Proof. Assume u is a unit in R and suppose that $\varphi(1_R) = 1_S$. Then

$$1_S = \varphi(1_R) = \varphi(u \cdot u^{-1}) = \varphi(u)\varphi(u^{-1}).$$

It follows that $\varphi(u)$ is a unit in S with $(\varphi(u))^{-1} = \varphi(u^{-1})$. □

Exercise 26. *The characteristic of a ring R is the smallest possible integer n such that $1 + 1 + \cdots + 1 = 0$ (n times) in R; if no such integer exists the characteristic of R is said to be 0.*

(a) *Prove that the map $\mathbb{Z} \to R$ defined by*

$$k \mapsto \begin{cases} 1 + 1 + \cdots + 1 \ (k \text{ times}) & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -1 - 1 - \cdots - 1 \ (-k \text{ times}) & \text{if } k < 0 \end{cases}$$

is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R (this explains the use of terminology " characteristic 0" instead of the archaic phrase "characteristic ∞" for rings in which no sum of 1's is zero).

Proof. We prove the two homomorphism properties.
Observe that

$$\varphi(k_1 + k_2) = \begin{cases} 1 + 1 + \cdots + 1 \ (k_1 + k_2 \text{ times}) & \text{if } k_1 + k_2 > 0 \\ 0 & \text{if } k_1 + k_2 = 0 \\ -1 - 1 - \cdots - 1 \ (-(k_1 + k_2) \text{ times}) & \text{if } k_1 + k_2 < 0 \end{cases}$$

In the first case we have two scenarios. Either both k_1 and k_2 positive, or (without loss of generality) k_1 is positive and k_2 is negative, with $|k_1| > |k_2|$. In the former we see that

$$k_1 + k_2 = \underbrace{1 + 1 + \cdots 1}_{k_1 \text{ times}} \underbrace{+1 + 1 + \cdots + 1}_{k_2 \text{ times}}$$

and it follows that $\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2)$. On the latter we have

$$k_1 + k_2 = \underbrace{1 + 1 + \cdots 1}_{k_1 \text{ times}} \underbrace{-1 - 1 - \cdots - 1}_{-k_2 \text{ times}}$$

and then we have $\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2)$, as desired.
Now we inspect the second case where $k_1 + k_2 = 0$. It follows that

$$0 = \underbrace{1 + 1 + \cdots 1}_{k_1 \text{ times}} \underbrace{-1 - 1 - \cdots - 1}_{-k_1 = k_2 \text{ times}}$$

and therefore $\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2)$.
The third case, when $k_1 + k_2 < 0$ is analogous to the first one by replacing $+1$ by -1 when necessary.
Now we prove the multiplicative property. Observe that

$$\varphi(k_1 k_2) = \begin{cases} 1 + 1 + \cdots + 1 \ (k_1 k_2 \text{ times}) & \text{if } k_1 k_2 > 0 \\ 0 & \text{if } k_1 k_2 = 0 \\ -1 - 1 - \cdots - 1 \ (k_1 k_2 \text{ times}) & \text{if } k_1 k_2 < 0 \end{cases},$$

again, we proceed by looking at the three cases separately.
In the first instance either both k_1 and k_2 are negative or positive. If both are positive

$$\begin{aligned} \varphi(k_1 k_2) &= 1 + 1 + \cdots + 1 \ (k_1 k_2 \text{ times}) \\ &= 1 \cdot (\underbrace{1 + 1 + \cdots + 1}_{k_1 \text{ times}}) + 1 \cdot (\underbrace{1 + 1 + \cdots + 1}_{k_1 \text{ times}}) + \cdots + 1 \cdot (\underbrace{1 + 1 + \cdots + 1}_{k_1 \text{ times}}) \ (k_2 \text{ times}) \\ &= \underbrace{(1 + 1 + \cdots + 1)}_{k_1 \text{ times}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{k_2 \text{ times}} \\ &= \varphi(k_1) \cdot \varphi(k_2) \end{aligned}$$

as desired. On the other hand, if both k_1 and k_2 are negative, then

$$\begin{aligned} \varphi(k_1 k_2) &= 1 + 1 + \cdots + 1 \ (k_1 k_2 \text{ times}) \\ &= -1 \cdot (\underbrace{-1 - 1 - \cdots - 1}_{-k_1 \text{ times}}) - 1 \cdot (\underbrace{-1 - 1 - \cdots - 1}_{-k_1 \text{ times}}) - \cdots - 1 \cdot (\underbrace{-1 - 1 - \cdots - 1}_{-k_1 \text{ times}}) \ (-k_2 \text{ times}) \\ &= \underbrace{(-1 - 1 - \cdots - 1)}_{-k_1 \text{ times}} \cdot \underbrace{(-1 - 1 - \cdots - 1)}_{-k_2 \text{ times}} \\ &= \varphi(k_1) \cdot \varphi(k_2). \end{aligned}$$

In the second case, where $k_1 k_2 = 0$ we have that either k_1 or k_2 is equal to zero (ans these elements operate in the integral domain $\mathbb{Z}$). Then, without loss of generality, assume $k_1 = 0$ and see that

$$\varphi(k_1 k_2) = 0 = 0 \cdot \varphi(k_2) = \varphi(k_1) \cdot \varphi(k_2)$$

as desired.
Lastly we inspect the case where $k_1 k_2 < 0$. Without loss of generality assume that $k_1 > 0$ and $k_2 < 0$. Then we have

$$\begin{aligned} \varphi(k_1 k_2) &= -1 - 1 - \cdots - 1 \ (-k_1 k_2 \text{ times}) \\ &= -1 \cdot (\underbrace{1 + 1 + \cdots + 1}_{k_1 \text{ times}}) - 1 \cdot (\underbrace{1 + 1 + \cdots + 1}_{k_1 \text{ times}}) - \cdots - 1 \cdot (\underbrace{1 + 1 + \cdots + 1}_{k_1 \text{ times}}) \ (-k_2 \text{ times}) \\ &= \underbrace{(1 + 1 + \cdots + 1)}_{k_1 \text{ times}} \cdot \underbrace{(-1 - 1 - \cdots - 1)}_{-k_2 \text{ times}} \\ &= \varphi(k_1) \cdot \varphi(k_2). \end{aligned}$$

We conclude that φ is a ring homomorphism.
Observe that an element z in $\mathbb{Z}$ will be in the kernel whenever $z = 0$ or $1 + 1 + \cdots + 1 = 0$. By definition of R, the latter is zero whenever $z = n$. Likewise (by the product property of the homomorphism) $\varphi(n \cdot z) = \varphi(n)\varphi(z) = 0$ for all $z \in \mathbb{Z}$. Hence z is in the kernel of φ whenever z is an integer multiple of n. □

(b) *Determine the characteristics of the rings* $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Z}/n\mathbb{Z}[x]$.

Proof. Observe that, over $\mathbb{Q}$, $1 + 1 + \cdots + 1$ (n times) is equal to n and therefore the sums is 0 only if $n = 0$. We conclude that the characteristic of Q is 0.
Over $\mathbb{Z}[x]$, the multiplicative identity is 1. Like the previous part, $1 + 1 + \cdots + 1$ (n times) is equal to the constant polynomial n. which is 0 only if $n = 0$. We conclude that the characteristic of $\mathbb{Z}[x]$ is 0.
Lastly, over $\mathbb{Z}/n\mathbb{Z}[x]$, $1 + 1 + \cdots + 1$ (m times) equals the constant polynomial $m \mod n$. This polynomial is zero wherever m is a positive multiple of n. Therefore the smallest m that agrees with the definition of the characteristic is $m = n$. □

(c) *Prove that if* p *is a prime and if* R *is a commutative ring of characteristic* p*, then* $(a+b)^p = a^p + b^p$ *for all* $a, b \in R$.

Proof. Using the binomial theorem we see that

$$(a + b)^p = \sum_{n=0}^{p} \frac{p!}{n!(p-n)!} a^{p-k} b^k.$$

Note that p is a factor of the coefficient whenever $n < p$ and $p - n < p$, or equivalently, whenever $0 < n < p$. Since our ring has characteristic p, all the coefficients with p as a factor will be 0 and therefore only the first and last term survive. It is to say that

$$(a + b)^p = \sum_{n=0}^{p} \frac{p!}{n!(p-n)!} a^{p-k} b^k = a^p + 0 + 0 + \cdots + 0 + b^p = a^p + b^p.$$

□

Exercise 28. *Prove that an integral domain has characteristic* p*, where* p *is either a prime or* 0.

Proof. Let n be composite of the form $n = n_1 n_2$ (where n_1 and n_2 are numbers less than n) and let $\varphi : \mathbb{Z} \to R$ be the homomorphism prescribed in exercise 26. Then we have,

$$0 = \varphi(n) = \varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$$

Observe that $\varphi(n_1)$ and $\varphi(n_2)$ are non zero elements in R as otherwise, the characteristic of R is smaller than n. Therefore $\varphi(n_1)\varphi(n_2)$ are two non zero elements whose product is zero, and therefore R is not an integral domain, a contradiction. □

Section 7.4

Exercise 8. *Let R be an integral domain. Prove that $(a) = (b)$ for some elements $a, b \in R$, if and only if $a = ub$ for some unit u of R.*

Proof. We begin by proving the trivial case, when either a or b are the zero element. Assume, without loss of generality that $a = 0$. Then, $(a) = 0$ and $(a) = (b)$ if and only if $b = 0$. Here, $u = 1$.
Now assume that a and b are non zero elements and that $(a) = (b)$. Since R is an integral domain, it is commutative and therefore (a) is the collection of multiples of a, likewise (b) is the set of multiples of b. It follows that $a = ub$ and $b = va$ for some elements u and v in the ring. Combining both equalities we have $ab = (ub)(va) = (uv)ab$ and since the ring is an integral domain is follows that $1 = uv$. Hence, u is a unit in R.
Now assume that $a = ub$ for some unit in R. We show that $(a) \subset (b)$. Take an arbitrary element $\bar{a} \in (a)$. Then $\bar{a} = ra$ for some element r in the ring. It follows that $\bar{a} = r(ub) = (ru)b$. The later is an element of (b) as desired. The inclusion $(b) \subset (a)$ follows analogously by writing b as $u^{-1}a$.

□

Exercise 11. *Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ (for example, if P contains $I \cap J$). Prove either I or J is contained in P.*

Proof. We prove the contrapositive argument. Assume that neither I nor J are contained in P, then there exist elements i and j such that $i \notin P$ and $j \notin P$. It follows that the product $ij \notin P$ otherwise, either $i \in P$ or $j \in P$ and we get a contradiction. Hence $IJ \not\subset P$ as it lacks the element ij. □

Exercise 15. *Let $x^2 + x + 1$ be an element of the polynomial ring $E = \mathbb{F}_2[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{F}_2[x]/(x^2 + x + 1)$.*

(a) *Prove that $\overline{E}$ has 4 elements: $\overline{0}, \overline{1}, \overline{x}$ and $\overline{x+1}$.*

Proof. We note that $\mathbb{F}_2[x]$ is an euclidean domain and therefore every element in the ring can be written as $q(x)(x^2 + x + 1) + r(x)$ where $q(x)$ and $r(x)$ are elements in the ring and with $r(x)$ being a polynomial of degree less than 2. It follows that under the quotient, all the polynomial have degree less than or equal to 1 for which the only possibilities are $\overline{0}, \overline{1}, \overline{x}$ and $\overline{x+1}$. □

(b) *Write out the 4×4 addition table for $\overline{E}$ and deduce that the additive group $\overline{E}$ is isomorphic to the Klein 4-group.*

Proof. The addition table is the following

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

One sees that this is the same multiplication table as the Klein 4-group. □

(c) *Write out the* 4×4 *multiplication table for* $\overline{E}$ *and prove that* $\overline{E}^\times$ *is isomorphic to the cyclic group of order* 3. *Deduce that* $\overline{E}$ *is a field.*

Proof. The multiplication table is as follows

$\times$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

One sees that the group of units, $\overline{E}^\times$, is given at the lower right 3×3 sub-table. It's structure is the same as $\mathbb{Z}/3\mathbb{Z}$ as desired. □

Exercise 19. *Let* R *be a finite commutative ring with identity. Prove that every prime ideal of* R *is a maximal ideal.*

Proof. It suffices to show to that the quotient ring R/P is a field. Let P be a prime ideal of the ring. By **Proposition 13** (Dummit and Foote ch. 7.4) the quotient R/P is an integral domain, and furthermore is finite (since R is finite). **Corollary 3** of section 7.1 asserts that a finite integral domain is a field. Hence R/P is a field as desired. □

Exercise 26. *Prove that a prime ideal in a commutative ring* R *contains every nilpotent element. Deduce that the nilradical of* R *is contained in the intersection of all the prime ideals of* R.

Proof. Let x be a nilpotent element in R with $x^n = 0$ and $n < \infty$. We proceed by induction over n. For $n = 1$ we have that x is the zero element and it is necessarily on P. Assume that for finite n the statement is true. Now, see that $x^{n+1} = (x)(x^n) = 0$ is in P and therefore, either $x \in P$ and we are done, or $x^n \in P$ and we are done by the induction hypothesis.
It follows that for every prime ideal P, the ideal consisting of all nilpotent elements (the nilradical) is a subset of P. Then

$$\text{nilradical ideal} \subseteq \bigcap_{P \text{ a prime ideal}} P$$

□

Exercise 37. *A commutative ring* R *is called a* local ring *if it has a unique maximal ideal. Prove that if* R *is a local ring with maximal ideal* M *then every element of* $R - M$ *is a unit. Prove conversely that if* R *is a commutative ring with* 1 *in which the set of nonunits forms an ideal* M, *then* R *is a local ring with unique maximal ideal* M.

Proof. Since M is the unique maximal ideal, every other ideal is contained in M. In particular, consider the ideal (r) generated by a nonzero element $r \in R - M$. Since $r \notin M$, (r) is not contained in M. Therefore $(r) = R$ and furthermore (r) contains a unit u, but since (r) is a principal ideal the only choice for the multiplicative inverse of u is r. Hence r is a unit.
Now assume that M is the set of non units in R. First we show that the ideal is maximal. Consider the quotient ring R/M and observe that for every unit in R (let it be u) there exist v such that $(u + M)(v + M) = uv + M = 1 + M$. Thus, every non zero element in R/M is a

unit and therefore R/M is a field. We conclude that M is maximal. Now we show uniqueness. Assume N is a maximal ideal with $N \neq M$ then, there exist n such that $n \in N$ but $n \notin M$. This implies that n is a unit and therefore $N = R$ by **Proposition 9.** It follows that N is not maximal as it is not proper. □

Section 7.5

Exercise 3. *Let F be a field. Prove that F contains a unique smallest subfield F_0 and that F_0 is somorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p (F_0 is called the prime subfield of F).*

Proof. The following proof is outlined by *Dummit* and/or *Foote* in the textbook (Chaper 13.1 {Field Theory}).
Lemma. *the characteristic of a field F is either 0 or a prime p.*

Proof. Let n be the characteristic of the field. Then $n \cdot 1 = 0$. If n is composite with $n = ab$, then $(ab)1 = (a1)(b1) = 0$. By the properties of the field, either $a1 = 0$ or $b1 = 0$. Therefore the smallest such integer is prime. □

Let φ be the homomorphism from $\mathbb{Z}$ to F defined by

$$\varphi(n) = n \cdot 1$$

and observe that $\ker(\varphi) = \mathrm{ch}(F)\mathbb{Z}$. Thus, the quotient $F/\ker(\varphi)$ gives an injection to either $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ depending on the characteristic of F. Since F is a field, we see that it contains a subfield isomorphic to either $\mathbb{Q}$ or the field of fractions of $\mathbb{Z}/p\mathbb{Z}$, and in either case it is the smallest subfield as it is generated by 1 in F. □

Section 7.6

Exercise 1. *An element $e \in R$ is called idempotent if $e^2 = e$. Assume e is an idempotent in R and $er = re$ for all $r \in R$. Prove that Re and $R(1-e)$ are two-sided ideals of R and that $R \cong Re \times R(1-e)$ Show that e and $1-e$ are identities for the subrings Re and $R(1-e)$ respectively.*

Proof. First, we prove that Re and $R(1-e)$ are two sided ideals.

1. Re is a two sided ideal.
   Let re be an arbitrary element in Re and let $\bar{r}$ be an arbitrary element in R. Then $(\bar{r})re = (\bar{r}r)e$ where $\bar{r}r \in R$ and thus $(\bar{r}r)e \in Re$. In the same manner, with re and $\bar{r}$ as above, note that $re(\bar{r}) = (er)\bar{r} = e(r\bar{r}) = (r\bar{r}e) \in Re$ (recall that $re = er$ for all $r \in R$). It follows that Re is a two sided ideal.

2. $R(1-e)$is a two sided ideal.
   Let $r(1-e)$ be an arbitrary element in $R(1-e)$ and let $\bar{r}$ be an arbitrary element in R. Then $(\bar{r})r(1-e) = (\bar{r}r)(1-e)$ where $\bar{r}r \in R$ and thus $(\bar{r}r)(1-e) \in R(1-e)$. In the same manner, with re and $\bar{r}$ as above, note that $r(1-e)\bar{r} = r(\bar{r} - e\bar{r}) = r(\bar{r} - \bar{r}e) = r\bar{r}(1-e) \in R(1-e)$ (recall that $re = er$ for all $r \in R$). It follows that $R(1-e)$ is a two sided ideal.

Now we show that $R \cong Re \times R(1-e)$.
Let $\varphi : R \to Re \times R(1-e)$ be given by $\varphi(r) = (re, r(1-e))$. Let a and b be arbitrary elements in R. Now, observe the following with awe:

i)

$$\begin{aligned}\varphi(a+b) &= ((a+b)e, (a+b)(1-e)) \\ &= ((ae+be, a(1-e)+b(1-e)) \\ &= (ae, a(1-e)) + (be, b(1-e)) \\ &= \varphi(a) + \varphi(b), \text{ and}\end{aligned}$$

ii)

$$\begin{aligned}\varphi(ab) &= (abe, ab(1-e)) \\ &= (abee, ab(1-e)(1-e)) \\ &= (aebe, a(1-e)b(1-e)) \\ &= (ae, a(1-e))(be, b(1-e)).\end{aligned}$$

Thus φ is a homomorphism. Furthermore φ is surjective as it has a well defined inverse $\varphi^{-1}(re, s(1-e)) = re + s(1-e)$. Injectivity follows form $\varphi(a) = \varphi(b)$ if and only if $ae = be$ and $a(1-e) = b(1-e)$ (equivalently $a - ae = b - be$). Combining the two we see that $a = b$. Therefore φ is an isomorphism as desired.
For the last part see that for an arbitrary element $re \in Re$, $e(re) = r(ee) = re$ and $(re)e = r(ee) = re$. Hence the identity of Re is e. The proof for $R(1-e)$ is analogous by replacing e by $(1-e)$. □

Exercise 2. *Let R be a finite Boolean ring with identity $1 \neq 0$. Prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \mathbb{Z}/2\mathbb{Z}$.*

Proof. We proceed by induction over the size of R. Observe that $|R| \geq 2$ as $1 \neq 0$. Therefore, for the base case, consider the Boolean ring of two elements, namely $R = \{1, 0\}$. Clearly this ring is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and we assume the hypothesis is satisfied for all Boolean rings R with $|R| < n$. Proceed by letting R be a Boolean ring of size n and note that there must be a nonzero nonidentity element x with $x^2 = x$ (by definition of the Boolean ring), in other words, x is nilpotent. By the previous exercise R is isomorphic to $Rx \times R(1-x)$, where Rx and $R(1-x)$ are ideals. Observe that in Rx we have $x = (1)x = (x)x$ and, analogously, in $R(1-x)$ we have $(1-x) = (1)(1-x) = (1-x)(1-x)$. Thus, by the closure property of ideals and the injectivity of $r \mapsto r(x)$ and $r \mapsto r(1-x)$, the size of Rx and $R(1-x)$ is less than n. It follows form the induction hypothesis that $Rx \cong (\mathbb{Z}/2\mathbb{Z})^a$ and $R(1-x) \cong (\mathbb{Z}/2\mathbb{Z})^b$ for some a and b. It follows that $R \cong Rx \times R(1-x) \cong (\mathbb{Z}/2\mathbb{Z})^a \times (\mathbb{Z}/2\mathbb{Z})^b \cong (\mathbb{Z}/2\mathbb{Z})^{a+b}$. □