Solutions to

TOPICS IN ALGEBRA

I.N. HERSTEIN

Part III: Ring Theory

Version: 1.1
Release: Jan 2013
Author: Rakesh Balhara

Preface

These solutions are meant to facilitate deeper understanding of the book, *Topics in Algebra*, second edition, written by I.N. Herstein. We have tried to stick with the notations developed in the book as far as possible. But some notations are extremely ambiguous, so to avoid confusion, we resorted to alternate commonly used notations.

The following notation changes will be found in the text:

1. use of *unity element* or simply *unity* instead of *unit element*.
2. use of *unit element* or simply *unit* in place of only *unit*.
3. an ideal generated by a is denoted by $\langle a \rangle$ instead of (a).
4. use of $gcd(a, b)$ instead of (a, b) for greatest common divisor of a, b.

Also following symbols are used in the text without any description, unless some other symbol is specifically described in the problem statement for the same:

1. $\mathbb{N}$ is used for natural numbers, i.e. $1, 2, 3, \cdots$.
2. $\mathbb{Z}$ is used for integers, i.e. $\cdots, -2, -1, 0, 1, 2, \cdots$.
3. $\mathbb{W}$ is used for whole numbers, i.e. $0, 1, 2, \cdots$.
4. $\mathbb{Z}_p$ is used for ring of integers with addition modulo p and multiplication modulo p as its addition and multiplication respectively.

Any suggestions or errors are invited and can be mailed to: rakeshbalhara@gmail.com

Problems (Page 130)

R is a ring in all the problems.

1. If $a, b, c, d \in R$, evaluate $(a+b)(c+d)$.
Solution: We have

$$\begin{aligned}(a+b)(c+d) &= a(c+d) + b(c+d) \\ &= ac + ad + bc + bd\end{aligned}$$

So $(a+b)(c+d) = ac + ad + bc + bd$. ∎

2. Prove that if $a, b \in R$, then $(a+b)^2 = a^2 + ab + ba + b^2$, where by x^2 we mean xx.
Solution: We have

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) \\ &= a(a+b) + b(a+b) \\ &= aa + ab + ba + bb \\ &= a^2 + ab + ba + b^2\end{aligned}$$

Hence the result. ∎

3. Find the form of the binomial theorem in a general ring; in other words, find an expression for $(a+b)^n$, where n is a positive integer.
Solution: We claim

$$(a+b)^n = \sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_n$$

We establish our claim by induction over n. For base case $n = 1$, we have $(a+b)^1 = a + b = \sum_{x_1 = a \text{ or } b} x_1$. So for $n = 1$, expression is valid. Suppose the expression $(a+b)^n = \sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_n$ is valid for $n = m - 1$, we will show the expression is then valid for $n = m$ too. We have

$$\begin{aligned}(a+b)^m &= (a+b)^{m-1}(a+b) \\ &= \left(\sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_{m-1} \right)(a+b) \\ &= \left(\sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_{m-1} \right) a + \left(\sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_{m-1} \right) b \\ &= \left(\sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_{m-1} a \right) + \left(\sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_{m-1} b \right)\end{aligned}$$

$$= \sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_{m-1} x_m$$

Thus the expression is equally valid for $n = m$. So we have for all $n \in \mathbb{N}$,

$$(a+b)^n = \sum_{x_i = a \text{ or } b} x_1 x_2 \cdots x_n \quad \blacksquare$$

4. If every $x \in R$ satisfies $x^2 = x$, prove that R must be commutative. (A ring in which $x^2 = x$ for all elements is called a *Boolean* ring.)
Solution: We are given $x^2 = x \quad \forall\, x \in R$. So for all x, $x^2 = 0 \Rightarrow x = 0$ as $x^2 = x$. But we have $\forall\, x, y \in R$,

$$\begin{aligned}(xy - xyx)^2 &= (xy - xyx)(xy - xyx) \\ &= xyxy - xyxyx - xyx^2y + xyx^2yx \\ &= xyxy - xyxyx - xyxy + xyxyx \text{ Using } x^2 = x \\ &= 0\end{aligned}$$

But

$$(xy - xyx)^2 = 0 \Rightarrow xy - xyx = 0 \tag{1}$$

Similarly, we can see $(yx - xyx)^2 = 0$. Therefore

$$yx - xyx = 0 \tag{2}$$

Using (1) and (2) we have $xyx = xy = yx$. So $xy = yx \quad \forall\, x, y \in R$. Hence R is commutative. $\blacksquare$

5. If R is a ring, merely considering it as an abelian group under its addition, we have defined, in Chapter 2, what is meant by na, where $a \in R$ and n is an integer. Prove that if $a, b \in R$ and n, m are integers, then $(na)(mb) = (nm)(ab)$.
Solution: We have

$$\begin{aligned}(na)(mb) &= (\underbrace{a + \cdots + a}_{n \text{ times}})(\underbrace{b + \cdots + b}_{m \text{ times}}) \\ &= \underbrace{a(\underbrace{b + \cdots + b}_{m \text{ times}}) + \cdots + a(\underbrace{b + \cdots + b}_{m \text{ times}})}_{n \text{ times}} \\ &= \underbrace{(\underbrace{ab + \cdots + ab}_{m \text{ times}}) + \cdots + (\underbrace{ab + \cdots + ab}_{m \text{ times}})}_{n \text{ times}} \\ &= \underbrace{m(ab) + \cdots + m(ab)}_{n \text{ times}}\end{aligned}$$

$$= (nm)(ab)$$

Hence the result. ∎

6. If D is an integral domain and D is of finite characteristic, prove that characteristic of D is a prime number.
Solution: Let the characteristic of D be p, therefore $pa = 0 \quad \forall\, x \in D$ and p is the smallest such positive integer. Suppose p is not a prime, therefore $p = rs$ for some positive integers r and s, with both not equal to 1. Let some $a \neq 0 \in D$, therefore $a^2 \in D$ too. So we have

$$\begin{aligned} pa^2 &= 0 \\ \Rightarrow (rs)(aa) &= 0 \\ \Rightarrow (ra)(sa) &= 0 \end{aligned}$$

D being an integral domain, implies $ra = 0$ or $sa = 0$. When $ra = 0$, we have $\forall\, x \in D$

$$\begin{aligned} (ra)x &= 0 \\ \Rightarrow (\underbrace{a + a + \cdots + a}_{r \text{ times}})x &= 0 \\ \Rightarrow (\underbrace{ax + ax + \cdots + ax}_{r \text{ times}}) &= 0 \\ \Rightarrow a(\underbrace{x + x + \cdots + x}_{r \text{ times}}) &= 0 \\ \Rightarrow a(rx) &= 0 \qquad (1) \end{aligned}$$

But $a \neq 0$ and D an integral domain, therefore (1) implies $rx = 0$. So we have $rx = 0 \quad \forall\, x \in D$ with $1 < r < p$, which is a contradiction as p is the smallest such integer. Similarly, when $sa = 0$ we have contradiction. Thus $p = rs$ is not possible, thereby proving p is a prime. ∎

7. Give an example of an integral domain which has an infinite number of elements, yet is of finite characteristic.
Solution: We define $\mathbb{Z}_p[x] = \{a_m x^m + a_{m-1}x^{m-1} + \cdots a_1 x + a_0 \mid a_i \in \mathbb{Z}_p, m \in \mathbb{W}\}$, where $\mathbb{Z}_p$ is a field of integers modulo p, p being prime. Clearly $pf(x) = 0 \quad \forall\, f(x) \in \mathbb{Z}_p[x]$. Also $\mathbb{Z}_p[x]$ has infinite number of elements. So $\mathbb{Z}_p[x]$ is the desired example. ∎

8. If D is an integral domain and if $na = 0$ for some $a \neq 0$ in D and some integer $n \neq 0$, prove that D is of finite characteristic.
Solution: We are given $na = 0$ for some $a \in D$ with $a \neq 0$ and $n \in \mathbb{N}$. We

have $\forall x \in D$

$$\begin{aligned}
(na)x &= 0 \\
\Rightarrow (\underbrace{a + a + \cdots + a}_{n \text{ times}})x &= 0 \\
\Rightarrow (\underbrace{ax + ax + \cdots + ax}_{n \text{ times}}) &= 0 \\
\Rightarrow a(\underbrace{x + x + \cdots + x}_{n \text{ times}}) &= 0 \\
\Rightarrow a(nx) &= 0 \qquad (1)
\end{aligned}$$

With $a \neq 0$ and D being integral domain, (1) implies $nx = 0$. So we have $nx = 0 \quad \forall\, x \in D$, showing D is of finite characteristic. ∎

9. If R is a system satisfying all the conditions for a ring with unit element with possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring. (*Hint:* Expand $(a+b)(1+1)$ in two ways.)
Solution: We have for $a, b \in R$

$$\begin{aligned}
(a + b)(1 + 1) &= a(1 + 1) + b(1 + 1) \\
&= a + a + b + b \qquad (1)
\end{aligned}$$

Also we have

$$\begin{aligned}
(a + b)(1 + 1) &= (a + b)1 + (a + b)1 \\
&= a + b + a + b \qquad (2)
\end{aligned}$$

From (1) and (2) we have $a + a + b + b = a + b + a + b$, or $a + b = b + a$. Thus axiom $a + b = b + a$ holds true in R, thereby proving R is a ring. ∎

10. Show that the commutative ring D is an integral domain if and only if for $a, b, c \in D$ with $a \neq 0$ the relation $ab = ac$ implies that $b = c$.
Solution: Suppose D is an integral domain. Now for $a \neq 0$, the relation

$$\begin{aligned}
ab = ac &\Rightarrow ab - ac = 0 \\
&\Rightarrow a(b - c) = 0
\end{aligned}$$

But $a \neq 0$ and D an integral domain, imply $b - c = 0$, or $b = c$. Thus the relation $ab = ac$ with $a \neq 0$ implies $b = c$.

Conversely, suppose D is a commutative ring with $a \neq 0$ and $ab = ac$ implying $b = c$. Now suppose $xy = 0$ for some $x, y \in D$. If $x \neq 0$, then $xy = 0 = x.0$. But $xy = x0$ with $x \neq 0$ implies $y = 0$. So $xy = 0$ and $x \neq 0$ implies $y = 0$. Similarly, $xy = 0$ and $y \neq 0$ implies $x = 0$. Therefore $xy = 0$ implies $x = 0$ or

$y = 0$. Hence D is an integral domain. ∎

11. Prove that Lemma 3.3.2 is false if we drop the assumption that the integral domain is finite.
Solution: When D is infinite, $Da = \{da \mid d \in D\}$ might not be equal to D for some $a \in D$, the fact which we had used to prove the Lemma 3.3.2. For example in the ring of integers $\mathbb{Z}$, which is an infinite integral domain, $2\mathbb{Z} \neq \mathbb{Z}$. Also $\mathbb{Z}$ is not a field. Thus an infinite integral domain might not be a field. ∎

12. Prove that any field is an integral domain.
Solution: Let F be some field and $xy = 0$ for some $x, y \in F$. If $x \neq 0$, then there must exist x', multiplicative inverse of x in F. So we have

$$\begin{aligned} xy = 0 &\Rightarrow x'(xy) = x'(0) \\ &\Rightarrow (x'x)y = 0 \\ &\Rightarrow (1)y = 0 \\ &\Rightarrow y = 0 \end{aligned}$$

Similarly, when $y \neq 0$, we have $x = 0$. So $xy = 0$ implies $x = 0$ or $y = 0$. Therefore F is an integral domain. Hence any field is an integral domain. ∎

13. Useing the pigeonhole principle, prove that if m and n are relatively prime integers and a and b are any integers, there exist an integer x such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$. (*Hint:* Consider the remainders of $a, a + m, a + 2m, \ldots, a + (n - 1)m$ on division by n.)
Solution: Consider the remainders of $a, a + m, a + 2m, \ldots, a + (n - 1)m$ on division by n. We claim no two remainder is same. Suppose if $(a + im) \bmod n = (a + jm) \bmod n$, then $(a + im) \equiv (a + jm) \bmod n \Rightarrow m(i - j) \equiv 0 \bmod n$. But $gcd(m, n) = 1$ implies $m \bmod n \neq 0$. Therefore, $(i - j) \equiv 0 \bmod n$, or $i \equiv j \bmod n$. Also $0 \leqslant i, j < n$ forces $i = j$. Thus no two remainders are same. But we have n terms in the sequence $a, a + m, a + 2m, \ldots, a + (n - 1)m$ and also for any y, $y \bmod n$ can have n values, i.e. $0 \leq y \bmod n \leq n - 1$. Therefore invoking pigeonhole principle, we have $b \bmod n$ must be a remainder for some i, that is $a + im \equiv b \bmod n$. Now let $x = a + im$, therefore $x \equiv a \bmod m$. Also then $x = a + im \equiv b \bmod n$. Thus we have shown there must exist some x, satisfying $x \equiv a \bmod m$ and $x \equiv b \bmod n$. ∎

14. Using the pigeonhole principle, prove that decimal expansion of a rational number must, after some time, become repeating.
Solution: Suppose $\frac{p}{q}$ be some rational number. We have $p = a_0 q + r$ where

$0 \leq r < q$. So dividing by q, we have

$$\frac{p}{q} = a_0 + \frac{r}{q} \text{ with } 0 \leq \frac{r}{q} < 1 \tag{1}$$

Again $10r = b_1 q + r_1$ with $0 \leq r_1 < q$. Dividing by $10q$, we have $\frac{r}{q} = \frac{b_1}{10} + \frac{r_1}{10q}$ with $0 \leq \frac{r_1}{10q} < \frac{1}{10}$. Thus we have

$$\frac{p}{q} = a_0 + \frac{b_1}{10} + \frac{r_1}{10q} \text{ with } 0 \leq \frac{r_1}{10q} < \frac{1}{10} \tag{2}$$

Continuing in the similar fashion, we have

$$\frac{p}{q} = a_0 + \frac{b_1}{10} + \frac{b_2}{10^2} + \cdots + \frac{b_n}{10^n} + \frac{r_n}{10^n q} \text{ with } 0 \leq \frac{r_n}{10^n q} < \frac{1}{10^n} \tag{3}$$

Note that $10r_{n-1} = b_n q + r_n$ with $0 \leq r_n < q$. Also (3) implies that decimal expression of $\frac{p}{q}$ is $a_0.b_1 b_2 \cdots$. So we have $0 \leq r_i < q \quad \forall\ i$. Now consider the set $\{r_1, r_2, \cdots, r_{q+1}\}$. This set has $q+1$ elements with values between -1 and q. Applying pigeonhole principle, we have $r_{q+1} = r_i$ for some $i \leq q$. Thus the sequence r_i must have repetition. Let $r_m = r_n$ for some $m < n$. But $10r_n = b_{n+1} q + r_{n+1}$ and $10r_m = b_{m+1} q + r_{m+1}$. Unique decomposition of integers by the Euclidean algorithm implies $b_{n+1} = b_{m+1}$ and $r_{n+1} = r_{m+1}$. Again $r_{n+1} = r_{m+1}$ will imply $b_{n+2} = b_{m+2}$ and $r_{n+2} = r_{m+2}$. Continuing the same we get $b_{m+i} = b_{n+i}$ for all $i \geq 0$. Thus the decimal expression of $\frac{p}{q}$ is repeating. ∎

Problems (Page 135)

1. If U is an ideal of R and $1 \in U$, prove that $U = R$.
Solution: Since we have $ur \in U \quad \forall\ u \in U\ \&\ r \in R$, so if $1 \in U$, we have $1r \in U \quad \forall\ r \in R$, or $r \in U \quad \forall\ r \in R$. Therefore $R \subset U$. But by definition $U \subset R$. Hence $U = R$. ∎

2. If F is a field, prove its only ideals are (0) and F itself.
Solution: Suppose U be some ideal of F. Now either $U = \{0\}$ or $U \neq \{0\}$. Clearly $U = \{0\}$ is an ideal of F. But when $U \neq \{0\}$, then there exists some $a \in U$ such that $a \neq 0$. But F being a field and $a \neq 0$, therefore there exists a', inverse of a in F. Now $a \in U$ and $a' \in F$, therefore $a.a' \in U$, or $1 \in U$. Again $1 \in U$ and any $r \in F$, therefore $1.r \in U$, or $r \in U$. Thus $F \subset U$. But $U \subset F$. So $U = F$. Thus the only possible ideals of F are $\{0\}$ or F. ∎

3. Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.
Solution: Let F be some field and R be some ring. Let $\phi : F \longrightarrow R$ be some homomorphism. Let K_ϕ be kernel of homomorphism ϕ. We know K_ϕ is an ideal of F. But the only ideals of F are $\{0\}$ or F itself. When $K_\phi = \{0\}$, we claim ϕ is one-to-one mapping. Suppose $\phi(x) = \phi(y)$ for some $x, y \in F$, then we have for $\overline{0}$ as an additive identity of R

$$\begin{aligned}\phi(x) = \phi(y) &\Rightarrow \phi(x) - \phi(y) = \overline{0} \\ &\Rightarrow \phi(x - y) = \overline{0} \\ &\Rightarrow x - y \in K_\phi \\ &\Rightarrow x - y = 0 \\ &\Rightarrow x = y\end{aligned}$$

So when $K_\phi = \{0\}$, ϕ is an one-to-one homomorphism (or isomorphism). But when $K_\phi = F$, then $\phi(x) = \overline{0} \quad \forall\ x \in F$, or ϕ takes every element of F into 0. Hence any homomorphism of a field is either an isomorphism or takes each element into 0. ∎

4. If R is a commutative ring and $a \in R$,
(a) Show that $aR = \{ar \mid r \in R\}$ is a two-sided ideal of R.
(b) Show by an example that this may be false if R is not commutative.
Solution:
(a) First we will show aR is subgroup of R. Suppose $x, y \in aR$, therefore $x = ar_1$ and $y = ar_2$ for some $r_1, r_2 \in R$. But then $x - y = ar_1 - ar_2 = a(r_1 - r_2) = ar_3$ for some $r_3 \in R$. So $x - y \in aR$. Thus aR is subgroup of R under addition. Next if some $x \in aR$ and $r \in R$, then we have $x = ar_4$ for some $r_4 \in R$. Also $rx = xr = ar_4r = a(r_4r) = ar_5$ for some $r_5 \in R$. So for all $x \in aR$ and $r \in R$,

we have $rx, xr \in aR$. Thus aR is an ideal(or two-sided ideal) of R.

(b) Consider $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$. We left it to the reader to check R is a non-commutative ring. Let $a = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. Again we can easily check $aR = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$. Clearly, aR is not a two-sided ideal as for $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \in aR$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in R$, we have $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin aR$. Thus in a non-commutative ring R, aR need not to be an ideal. ∎

5. If U, V are ideals of R, let $U + V = \{u + v \mid u \in U, v \in V\}$. Prove that $U + V$ is also an ideal.
Solution: Suppose some $x, y \in U + V$, therefore $x = u_1 + v_1$ and $y = u_2 + v_2$ for some $u_1, u_2 \in U$ and $v_1, v_2 \in V$. But then $x - y = (u_1 + v_1) - (u_2 + v_2) = (u_1 - u_2) + (v_1 - v_2) = u_3 + v_3$ for some $u_3 \in U$ and $v_3 \in V$ as U, V are the ideals of R. So $x - y \in U + V$. Thus $U + V$ is a subgroup of R under addition. Next suppose some $x \in U + V$ and $r \in R$, then we have $x = u_4 + v_4$ for some $u_4 \in U$ and $v_4 \in V$. Now we have $xr = (u_4 + v_4)r = u_4r + v_4r = u_5 + v_5$ for some $u_5 \in U$ and $v_5 \in V$ as U, V are the ideals of R. So $xr \in U + V$. Similarly $rx \in U + V$. Thus we have $xr, rx \in U + V \quad \forall\, x \in U + V \;\&\; r \in R$. So $U + V$ is an ideal of R.
Remark: We left it to the reader to check $U + V$ is the smallest ideal of R containing U and V. In other words, $\langle U \cup V \rangle = U + V$. ∎

6. If U, V are ideals of R let UV be the set of all the elements that can be written as finite sums of elements of the form uv where $u \in U$ and $v \in V$. Prove that UV is an ideal of R.
Solution: We first introduce a change in notation. We assume

$$UV = \{uv \mid u \in U \;\&\; v \in V\}$$

Let $I = \{\sum_{i \in \Lambda} u_i v_i \mid u_i \in U \;\&\; v_i \in V$ and Λ being some finite index set$\}$. So we need to show I is an ideal of R. Suppose some $x, y \in I$, therefore $x = \sum_{i \in \Lambda} u_i v_i$ and $y = \sum_{i \in \Gamma} u_i v_i$ for $u_i \in U$ and $v_i \in V$ for all $i \in \Lambda \cup \Gamma$, where Λ, Γ are some finite index sets. But then we have $x - y = \sum_{i \in \Lambda} u_i v_i - \sum_{i \in \Gamma} u_i v_i = \sum_{i \in \Lambda} u_i v_i + \sum_{i \in \Gamma} (-u_i) v_i = \sum_{i \in \Lambda \cup \Gamma} u_i' v_i$, for some $u_i' \in U$. So $x - y \in I$ showing I is a subgroup of R under under addition. Also if some $x \in I$ and $r \in R$, then $x = \sum_{i \in \Delta} u_i v_i$ for all $i \in \Delta$, where Δ is some finite index set. We have $xr = (\sum_{i \in \Delta} u_i v_i) r = \sum_{i \in \Delta} u_i v_i r = \sum_{i \in \Delta} u_i v_i'$ for some $v_i' \in V$. So $xr \in I$ for all $x \in I$ and $r \in R$. Similarly, $rx \in I$ for all $x \in I$ and $r \in R$. Thus I is an ideal of R.

Remark: We left it to the reader to check I is the smallest ideal of R containing UV. In other words, $I = \langle UV \rangle$ ∎

7. In Problem 6 prove that $UV \subset U \cap V$.
Solution: In terms of the notations, we developed in previous problem, we need to show

$$\langle UV \rangle \subset U \cap V$$

Suppose some $x \in \langle UV \rangle$, therefore $x = \sum_{i \in \Gamma} u_i v_i$ for $u_i \in U$ and $v_i \in V$ for all $i \in \Gamma$, where Γ is some finite index set. But $u_i v_i \in U \quad \forall\, i \in \Gamma$ as U is an ideal of R. Therefore $\sum_{i \in \Delta} u_i v_i \in U$. Similarly, $\sum_{i \in \Delta} u_i v_i \in V$ as V too is an ideal of R. Thus $x \in U$ and $x \in V$. Therefore $x \in U \cap V$. So $\langle UV \rangle \subset U \cap V$ ∎

8. If R is the ring of integers, let U be the ideal consisting of all multiples of 17. Prove that if V is an ideal of R and $R \supset V \supset U$ then either $V = R$ or $V = U$. Generalize!
Solution: We have $U = 17R$ and V ideal of R with $U \subset V \subset R$. Now either $V = U$ or $U \subsetneq V$. If $U \subsetneq V$, then there is some $x \in V$ such that $x \notin U$. But $x \notin U$ implies $x \neq 17k$ for some $k \in R$. But that means $17 \nmid x$. Also 17 being a prime, therefore $gcd(17, x) = 1$. Therefore $17i + xj = 1$ for some $i, j \in R$. But $17i \in U \subset V$ and $xj \in V$, therefore $17i + xj \in V$, or $1 \in V$. But $1 \in V$ implies $V = R$. Hence either $V = U$ or $V = R$.

We can generalize our result that if p is an irreducible element in R then whenever for some ideal V we have $pR \subset V \subset R$, implies either $V = pR$ or $V = R$. ∎

9. If U is an ideal of R, let $r(U) = \{x \in R \mid xu = 0 \text{ for all } u \in U\}$. Prove that $r(U)$ is an ideal of R.
Solution: Let some $x, y \in r(U)$, therefore $xu = 0 \quad \forall\, u \in U$ and $yu = 0 \quad \forall\, u \in U$. But then $(x - y)u = xu - yu = 0 - 0 = 0 \quad \forall\, u \in U$, therefore implying $x - y \in r(U)$. Thus $r(U)$ is a subgroup of R under addition. Next suppose some $x \in r(U)$ and $r \in R$. Therefore $x.u = 0 \quad \forall\, u \in U$. We have $(xr)u = x(ru) = x(u_1)$ for some $u_1 \in U$. Therefore $(xr)u = xu_1 = 0 \quad \forall\, u \in U$. So $xr \in r(U)$. Similarly, we can see $rx \in r(U)$. So $r(U)$ is an ideal of R. ∎

10. If U is an ideal of R let $[R : U] = \{x \in R \mid rx \in U \text{ for every } r \in R\}$. Prove that $[R : U]$ is an ideal of R and that it contains U.
Solution: Suppose some $x, y \in [R : U]$, therefore $rx \in U \quad \forall\, r \in R$ and $ry \in U \quad \forall\, r \in R$. But since U being an ideal, we have $rx - ry = r(x - y) \in U \quad \forall\, r \in R$, showing $x - y \in [R : U]$. Thus $[R : U]$ is a subgroup of R under addition. Next suppose $x \in [R : U]$ and $r_1 \in R$. Therefore $rx \in U \quad \forall\, r \in R$. Also $r(xr_1) = (rx)r_1 = u_1 r_1$ for some $u_1 \in U$. But U being an ideal, there-

fore $u_1 r_1 \in U$. So $r(xr_1) \in U \quad \forall\, r \in R$, implying $xr_1 \in [R : U] \quad \forall\, r_1 \in R$. Again, $r(r_1 x) = (rr_1)x = r_2 x$ for some $r_2 \in R$. So $r(r_1 x) = r_2 x \in U$, implying $r_1 x \in [R : U]$. So $r_1 x \in [R : U] \quad \forall\, r_1 \in R$. Hence $[R : U]$ is an ideal of R.

Also if $x \in U$, therefore $rx \in U \quad \forall\, r \in R$ as U is an ideal of R. But $rx \in U \quad \forall\, r \in R$ implies $x \in [R : U]$. Thus $U \subset [R : U]$. ∎

11. Let R be a ring with unit element. Using its elements we define a ring $\tilde{R}$ by defining $a \oplus b = a + b + 1$, and $a \cdot b = ab + a + b$, where $a, b \in R$ and where the addition and multiplication on the right-hand side of these relations are those of R.
(a) Prove that $\tilde{R}$ is a ring under the operations $\oplus$ and $\cdot$.
(b) What act as the zero-element of $\tilde{R}$?
(c) What acts as the unit-element of $\tilde{R}$?
(d) Prove that R is isomorphic to $\tilde{R}$.
Solution:
(a) First note that the both binary operations $\oplus$ and $\cdot$ are well-defined.

Closure under addition: Since $a + b + 1 \in R = \tilde{R}$, therefore $a \oplus b \in \tilde{R}$ for all $a, b \in \tilde{R}$. So $\tilde{R}$ is closed under addition.

Associativity under addition: We have

$$\begin{aligned} a \oplus (b \oplus c) &= a \oplus (b + c + 1) \\ &= a + (b + c + 1) + 1 \\ &= (a + b + 1) + c + 1 \\ &= (a \oplus b) + c + 1 \\ &= (a \oplus b) \oplus c \end{aligned}$$

Hence associativity under addition holds good.

Existence of additive identity: Suppose e be the additive identity, if it exists. But then $a \oplus e = a \quad \forall\, a \in \tilde{R}$. So $a + e + 1 = a \Rightarrow e = -1 \in \tilde{R}$. So the additive identity exists and is equal to -1.

Existence of additive inverses: Suppose some $a \in \tilde{R}$. If its inverse exists, let it be a'. So We have $a \oplus a' = -1 \Rightarrow a + a' + 1 = -1 \Rightarrow a' = -2 - a \in \tilde{R}$. So the inverse element exists for all elements.

Closure under multiplication: We have $a \cdot b = ab + a + b \in R = \tilde{R}$. So $\tilde{R}$ is closed under multiplication.

Associativity under multiplication: We have

$$a \cdot (b \cdot c) = a \cdot (bc + b + c)$$

$$
\begin{aligned}
&= a(bc+b+c)+a+(bc+b+c)\\
&= abc+ab+ac+a+bc+b+c\\
&= (ab+a+b)c+(ab+a+b)+c\\
&= (a\cdot b)c+(a\cdot b)+c\\
&= (a\cdot b)\cdot c
\end{aligned}
$$

Hence $\tilde{R}$ is a ring with $\oplus$ and $\cdot$ as addition and multiplication respectively.

(b) Already found in part(a), -1 acts as zero-element of $\tilde{R}$.

(c) If exists, let the unity element be u. So we have $a\cdot u = a \quad \forall\ a \in \tilde{R} \Rightarrow au+a+u = a \Rightarrow (a+1)u = 0 \Rightarrow u = 0 \in \tilde{R}$. Therefore the unity element exists and is equal to 0.

(d) Define mapping $\phi : R \longrightarrow \tilde{R}$ such that $\phi(x) = x-1$. Clearly the mapping is well-defined. We have

$$
\begin{aligned}
\phi(x+y) &= (x+y)-1\\
&= (x-1)+(y-1)+1\\
&= (x-1)\oplus(y-1)\\
&= \phi(x)\oplus\phi(y)
\end{aligned}
$$

Also

$$
\begin{aligned}
\phi(xy) &= xy-1\\
&= (x-1)(y-1)+(x-1)+(y-1)\\
&= (x-1)\cdot(y-1)\\
&= \phi(x)\cdot\phi(y)
\end{aligned}
$$

So the mapping ϕ is a ring homomorphism. Also $\phi(x) = \phi(y) \Rightarrow x-1 = y-1 \Rightarrow x = y$. So ϕ is one-to-one. Also if some $y \in \tilde{R}$, then $y+1 \in R$ is its inverse-image. So inverse-image of every element exists. So mapping is onto too. Thus ϕ is an isomorphism from R onto $\tilde{R}$. And hence $R \approx \tilde{R}$. ∎

*12. In Example 3.1.6 we discussed the ring of rational 2×2 matrices. Prove that this ring has no ideals other than (0) and the ring itself.
Solution: We denote the ring discussed in Example 3.1.6 as $M_2(\mathbb{R})$. Suppose U be some ideal of $M_2(\mathbb{R})$. So either $U = \left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}$ or $U \neq \left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}$. When $U \neq \left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}\right\}$, we have some $A = \begin{pmatrix}a&b\\c&d\end{pmatrix} \in U$ with $A \neq \begin{pmatrix}0&0\\0&0\end{pmatrix}$.

We took a little digression into defining another notation to represent any element of $M_2(\mathbb{R})$. We define $E_{11} = \begin{pmatrix}1&0\\0&0\end{pmatrix}, E_{12} = \begin{pmatrix}0&1\\0&0\end{pmatrix}, E_{21} = \begin{pmatrix}0&0\\1&0\end{pmatrix}, E_{22} =$

$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. So in this notation, we have $A = aE_{11} + bE_{12} + cE_{21} + dE_{22}$. Next we claim

$$E_{ij}E_{kl} = \begin{cases} E_{il} & \text{if } j = k \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{if } j \neq k \end{cases}$$

We left it to the reader to check this result.

Coming back to the problem, we have $A \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Therefore at least one of the a, b, c, d is non-zero. Suppose $a \neq 0$. So a^{-1} exists in $\mathbb{R}$. We have

$$\begin{aligned} & A = aE_{11} + bE_{12} + cE_{21} + dE_{22} \\ \Rightarrow\ & AE_{11} = (aE_{11} + bE_{12} + cE_{21} + dE_{22})E_{11} \\ \Rightarrow\ & AE_{11} = aE_{11} + cE_{21} \\ \Rightarrow\ & E_{11}AE_{11} = E_{11}(aE_{11} + cE_{21}) \\ \Rightarrow\ & E_{11}AE_{11} = aE_{11} \\ \Rightarrow\ & (a^{-1}E_{11})AE_{11} = E_{11} \end{aligned}$$

But $(a^{-1}E_{11})AE_{11} \in \langle A \rangle$, therefore

$$\begin{aligned} & E_{11} \in \langle A \rangle && (1) \\ \Rightarrow\ & E_{11}E_{12} \in \langle A \rangle \\ \Rightarrow\ & E_{12} \in \langle A \rangle \\ \Rightarrow\ & E_{21}E_{12} \in \langle A \rangle \\ \Rightarrow\ & E_{22} \in \langle A \rangle && (2) \\ \Rightarrow\ & E_{11} + E_{22} \in \langle A \rangle \text{ Using (1) and (2)} \\ \Rightarrow\ & I_2 \in \langle A \rangle \end{aligned}$$

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the multiplicative identity of $M_2(\mathbb{R})$. But $\langle A \rangle \subset U$ as $\langle A \rangle$ is the smallest ideal containing A and $A \in U$. Therefore $I_2 \in \langle A \rangle \subset U$. But $I_2 \in U$ implies $U = M_2(\mathbb{R})$. Also if instead of a some other element, say b or c or d is non-zero, we can analogously show $I_2 \in \langle A \rangle \subset U$, thereby implying $U = M_2(\mathbb{R})$. Thus we concluded, either $U = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ or $U = M_2(\mathbb{R})$. Hence $M_2(\mathbb{R})$ has no ideals other than $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ and $M_2(\mathbb{R})$ itself. ∎

*13. In Example 3.1.8 we discussed the real quaternions. Using this as a model we define the quaternions over the integers mod p, p an odd prime number, in exactly the same way; however, now considering all symbols of the form $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are integers mod p.

(a) Prove that this is a ring with p^4 elements whose only ideals are (0) and the ring itself.
**(b) Prove that this ring is *not* a division ring.
Solution:
(a) We denote the quaternions over integers mod p by Q_p. It is routine to check Q_p is a ring with $0(\equiv 0+0i+0j+0k)$ as additive identity and $1(\equiv 1+0i+0j+0k)$ as multiplicative identity. Also $o(Q_p)$ is equal to the number of ways of choosing four symbols from p symbols with repetition being allowed. Thus $o(Q_p) = p^4$. Next we aim to prove $\{0\}$ and Q_p are the only ideals of Q_p. Suppose U be some ideal of Q_p. Either $U = \{0\}$ or $U \neq \{0\}$. Suppose $U \neq \{0\}$, therefore some $u = a + bi + cj + dk \in U$ with $u \neq 0$. Since $u \neq 0$, therefore at least one of a, b, c, d is non-zero. Suppose $a \neq 0$, therefore a^{-1} exists as p being prime implies $\mathbb{Z}_p$ is a field. So we have

$$\begin{aligned} & a + bi + cj + dk \in U && (1)\\ \Rightarrow\ & i(a + bi + cj + dk)i \in U \\ \Rightarrow\ & -a - bi + cj + dk \in U && (2)\end{aligned}$$

Subtracting (2) from (1), we have

$$\begin{aligned} & 2(a + bi) \in U \\ \Rightarrow\ & a + bi \in U && (3)\\ \Rightarrow\ & j(a + bi)j \in U \\ \Rightarrow\ & -a + bi \in U && (4)\end{aligned}$$

Again subtracting (4) from (3), we have

$$\begin{aligned} & 2a \in U \\ \Rightarrow\ & a \in U \\ \Rightarrow\ & aa^{-1} \in U \\ \Rightarrow\ & 1 \in U\end{aligned}$$

But $1 \in U$ implies $U = Q_p$. In a similar way we can see if $b \neq 0$ or $c \neq 0$ or $d \neq 0$, we have $1 \in U$, thereby implying $U = Q_p$. So we conclude if U be some ideal of Q_p, then either $U = \{0\}$ or $U = Q_p$.

(b) Since $p \neq 2$, therefore Q_p is a non-commutative finite ring. But Wedderburn Theorem† asserts that a finite division ring must be commutative. So Q_p must not be a division ring. We can also prove the result using Lagrange Theorem that any positive integer can be expressed as sum of square of four integers. So we have $p = a^2 + b^2 + c^2 + d^2$ for some integers a, b, c, d. If $a = b = c = d = 0$, then $p = 0$, which is not the case. So all a, b, c, d cannot be equal to zero simultaneously. Also if $a = b = c = d = 0 \bmod p$, with

†see Section 7.2 of the book

$a = b = c = d \neq 0$, then $p^2 \mid (a^2 + b^2 + c^2 + d^2)$, or $p^2 \mid p$ which is not true. So at least there is some element x out of a, b, c, d such that $x \neq 0 \bmod p$. So if $u = a + bi + cj + dk$ and $v = a - bi - cj - dk$, then $u \neq 0 \bmod p$ and $v \neq 0 \bmod p$. But $uv = a^2 + b^2 + c^2 + d^2 = p = 0 \bmod p$. So we have $uv = 0$ with neither u nor v a zero element in Q_p. So Q_p is not an integral domain, consequently not a division ring. ∎

If R is any ring a subset L of R is called a *left-ideal* of R if

1. L is a subgroup under addition.
2. $r \in R$, $a \in L$ implies $ra \in L$.

(One can similarly define *right-ideal*.) An ideal is thus simultaneously a left- and right-ideal of R.

14. For $a \in R$ let $Ra = \{xa \mid x \in R\}$. Prove that Ra is a left-ideal of R.
Solution: Suppose $x, y \in Ra$, therefore $x = r_1 a$ and $y = r_2 a$ for some $r_1, r_2 \in R$. But then $x - y = r_1 a - r_2 a = (r_1 - r_1)a = r_3 a$ for some $r_3 \in R$. Thus $x - y \in Ra$. So Ra is a subgroup of R under addition. Next suppose some $x \in Ra$ and $r \in R$. So $x = r_4 a$ for some $r_4 \in R$. We have $rx = r(r_4 a) = (rr_4)a = r_5 a$ for some $r_5 \in R$. Thus $rx \in Ra \quad \forall\, x \in Ra$ and $r \in R$. So Ra is a left-ideal of R. ∎

15. Prove that the intersection of the two left-ideals of R is a left-ideal of R.
Solution: Suppose U_1, U_2 be two left-ideals of R. Define $U = U_1 \cap U_2$. We need to show U is also a left-ideal of R. Suppose some $x, y \in U$, therefore $x \in U_1$ and $x \in U_2$, $y \in U_1$ and $y \in U_2$. Since $y \in U_1$ so $-y \in U_1$ too as U_1 is a left-ideal of R. So $x \in U_1$ and $-y \in U_1$ implies $x - y \in U_1$. Similarly $x \in U_2$ and $-y \in U_2$, implying $x - y \in U_2$. Thus $x - y \in U_1$ and $x - y \in U_2$. So $x - y \in U_1 \cap U_2 = U$. Thus U forms a subgroup under addition. Next for $x \in U$ and $r \in R$, we have $rx \in U_1$ as U_1 is a left-ideal of R. Also $rx \in U_2$ as U_2 is a left-ideal of R. Thus $rx \in U_1$ and $rx \in U_2$, or $rx \in U_1 \cap U_2$. Thus $rx \in U \quad \forall\, x \in U$ and $r \in R$. So U is a left-ideal of R. ∎

16. What can you say about the intersection of a left-ideal and right-ideal of R?
Solution: Intersection of a left-ideal and right-ideal of R need not to a left-ideal or a right-ideal. We substantiate our statement with an example. Consider $M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$. Clearly $M_2(\mathbb{Z})$ is a ring. We define

$$U_1 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

and

$$U_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

We left it to the reader to check U_1 is a left-ideal of $M_2(\mathbb{Z})$ and U_2 is a right-ideal of $M_2(\mathbb{Z})$. Whereas $U_1 \cap U_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Z} \right\}$. Clearly $U_1 \cap U_2$ is not a left ideal as for $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in U_1 \cap U_2$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$, we have $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin U_1 \cap U_2$. Similarly $U_1 \cap U_2$ is not a right-ideal as for $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in U_1 \cap U_2$ and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$, we have $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \notin U_1 \cap U_2$. So $U_1 \cap U_2$ is neither a left-ideal nor a right-ideal. ∎

17. If R is a ring and $a \in R$ let $r(a) = \{x \in R \mid ax = 0\}$. Prove that $r(a)$ is a right-ideal of R.
Solution: Suppose $x, y \in r(a)$, therefore $ax = ay = 0$. But then $a(x - y) = ax - ay = 0 - 0 = 0$. So $x - y \in r(a)$. Thus $r(a)$ is a subgroup of R under addition. Next if $x \in r(a)$ and $r \in R$, we have $a(xr) = (ax)r = 0r = 0$. So $xr \in r(a) \quad \forall\, x \in r(a)$ & $r \in R$. Hence $r(a)$ is a right-ideal of R. ∎

18. If R is a ring and L is a left-ideal of R let $\lambda(L) = \{x \in R \mid xa = 0 \quad \forall\, a \in L\}$. Prove that $\lambda(L)$ is the two-sided ideal of R.
Solution: Suppose $x, y \in \lambda(L)$, therefore $xa = 0 \quad \forall a \in L$ and $ya = 0 \quad \forall a \in L$. But then $(x - y)a = 0 \quad \forall\, a \in L$. Thus $x - y \in \lambda(L)$ showing $\lambda(L)$ a subgroup of R under addition. Next suppose $x \in \lambda(L)$ and $r \in R$. We have for $a \in L$, $(xr)a = x(ra) = x(a_1)$ for some $a_1 \in L$ as L is the left-ideal of R. So $(xr)a = x(a_1) = 0$ as $x \in \lambda(L)$. Thus $xr \in \lambda(L) \quad \forall\, x \in \lambda(L)$ & $r \in R$. Again for all $a \in L$, $(rx)a = r(xa) = r0 = 0$. Thus $rx \in \lambda(L) \quad \forall x \in \lambda(L)$ & $r \in R$. Hence $\lambda(L)$ is an ideal of R. ∎

19. Let R be a ring in which $x^3 = x$ for every $x \in R$. Prove that R is a commutative ring.
Solution: First suppose $x^2 = 0$ for any $x \in R$. But $x^2 = 0 \Rightarrow x(x^2) = x0 \Rightarrow x^3 = 0 \Rightarrow x = 0$ as $x^3 = x$. Thus

$$x^2 = 0 \Rightarrow x = 0 \tag{1}$$

Next, we claim x^2 commute with all elements of R. We have

$$\begin{aligned} (x^2y - x^2yx^2)^2 &= (x^2y - x^2yx^2)(x^2y - x^2yx^2) \\ &= x^2yx^2y - x^2yx^2yx^2 - x^2yx^2x^2y + x^2yx^2x^2yx^2 \end{aligned}$$

$$= x^2yx^2y - x^2yx^2yx^2 - x^2yx^4y + x^2yx^4yx^2$$

But $x^4 = x^3x = xx = x^2$, so

$$\begin{aligned}(x^2y - x^2yx^2)^2 &= x^2yx^2y - x^2yx^2yx^2 - x^2yx^4y + x^2yx^4yx^2 \\ &= x^2yx^2y - x^2yx^2yx^2 - x^2yx^2y + x^2yx^2yx^2 \\ &= 0\end{aligned}$$

But then (1) implies $x^2y - x^2yx^2 = 0$ too, or

$$x^2y = x^2yx^2 \tag{2}$$

Again we can see $(yx^2 - x^2yx^2)^2 = 0$. So $yx^2 - x^2yx^2 = 0$, or

$$yx^2 = x^2yx^2 \tag{3}$$

From (2) and (3) we conclude $x^2y = yx^2 \quad \forall x, y \in R$. Finally, we have for all $x, y \in R$

$$\begin{aligned}xy = xy^3 &= (xy^2)y = y^2xy \\ &= y^2x^3y = y^2x(x^2y) = y^2xyx^2 \\ &= yyxyxx = y(yx)(yx)x = y(yx)^2x \\ &= yx(yx)^2 = (yx)^3 = yx\end{aligned}$$

So $xy = yx \quad \forall\, x, y \in R$, showing R to be a commutative ring. ∎

20. If R is a ring with unit element 1 and ϕ is a homomorphism of R *onto* R' prove that $\phi(1)$ is the unit element of R'.
Solution: Let some $\bar{y} \in R'$. But since ϕ is an onto mapping, so there exist $x \in R$ such that $\phi(x) = \bar{y}$. We have

$$\bar{y}\phi(1) = \phi(x)\phi(1) = \phi(x1) = \phi(x) = \bar{y}$$

Similarly,

$$\phi(1)\bar{y} = \bar{y}$$

Hence $\phi(1)$ is the identity element of R'. ∎

21. If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that $I(\phi) \neq R$, prove that $\phi(1)$ is the unit element of R'.
Solution: Let $\bar{0}$ represent the additive identity of R'. First, we claim $\phi(1) \neq \bar{0}$. Suppose $\phi(1) = \bar{0}$, then we have for all $x \in R$,

$$\phi(x) = \phi(x1) = \phi(x)\phi(1) = \phi(x)\bar{0} = \bar{0}$$

But that means $I(\phi) = R$ which is not the case. Hence $\phi(1) \neq \bar{0}$. Also we have

$$\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) \tag{1}$$

Finally, we claim $\phi(1)$ is the multiplicative identity. We establish our claim by contradiction. Suppose there exist some $\bar{y} \in R'$ such that $\bar{y}\phi(1) \neq \bar{y}$. So $\bar{y}\phi(1) - \bar{y} \neq \bar{0}$. Also $\phi(1) \neq \bar{0}$ and R' being an integral domain, so $(\bar{y}\phi(1) - \bar{y})\phi(1) \neq \bar{0}$. But

$$\begin{aligned}
&(\bar{y}\phi(1) - \bar{y})\phi(1) \neq \bar{0} \\
\Rightarrow\ &\bar{y}\phi(1)\phi(1) - \bar{y}\phi(1) \neq \bar{0} \\
\Rightarrow\ &\bar{y}\phi(1) - \bar{y}\phi(1) \neq \bar{0} \text{ Using (1)} \\
\Rightarrow\ &\bar{0} \neq \bar{0}, \text{ which is not true.}
\end{aligned}$$

So there exists no such $\bar{y} \in R'$ such that $\bar{y}\phi(1) \neq \bar{y}$. Thus $\bar{y}\phi(1) = \bar{y} \quad \forall\, \bar{y} \in R'$. Similarly $\phi(1)\bar{y} = \bar{y} \quad \forall\, \bar{y} \in R'$ Hence $\phi(1)$ is the unity element of R'. ∎

Problems (Page 139)

1. Let R be a ring with unit element, R not necessarily commutative, such that the only right-ideals of R are (0) and R. Prove that R is a division ring.
Solution: Clearly $R \neq \{0\}$ as $1 \in R$. Therefore we can assume some $a \in R$ with $a \neq 0$. Now consider $aR = \{ar \mid r \in R\}$. We can easily prove that aR is a right-ideal of R. Also it is given that only $\{0\}$ and R are the only right-ideals of R. So either $aR = \{0\}$ or $aR = R$. Clearly, $aR = \{0\}$ is not possible as $1 \in R$, so $a1 = a \in aR$. So we have only possibility $aR = R$. Now $1 \in R$, so for some $a' \in R$ we have $aa' = 1$. But that means, a' the inverse element of a exists in R. Since a is some arbitrarily chosen element with the only stipulation that $a \neq 0$, so all non-zero elements have inverse in R. Thus R is a division ring. ∎

2. Let R be a ring such that the only right ideals of R are (0) and R. Prove that either R is a division ring or that R is a ring with a prime number of elements in which $ab = 0$ for every $a, b \in R$.
Solution: We define $U = \{x \in R \mid xr = 0 \quad \forall\ r \in R\}$ and we claim U is a right-ideal of R. Clearly $0 \in U$ as $0r = r \quad \forall\ r \in R$. Suppose $u_1, u_2 \in U$, therefore $u_1 r = 0 \quad \forall\ r \in R$ and $u_2 r = 0 \quad \forall\ r \in R$. But $(u_1 - u_2)r = u_1 r - u_2 r = 0 - 0 = 0 \quad \forall\ r \in R$, therefore $u_1 - u_2 \in U$. So U forms a subgroup of R under addition. Also for $u \in U$ and $r \in R$, we have $ur = 0 \in U$. So $ur \in U \quad \forall\ u \in U\ \&\ r \in R$. Thus U is a right-ideal of R. But the only right-ideals of R are $\{0\}$ and R, therefore, either $U = \{0\}$ or $U = R$.

Case 1: When $U = R$, it means $ur = 0 \quad \forall\ u \in U$ and $r \in R$ i.e. $u.r = 0 \quad \forall\ u, r \in R$. Also multiplicative identity, 1 does not exist as if it had existed would mean $1 \in U \Rightarrow 1R = \{0\} \Rightarrow R = \{0\} \Rightarrow 1 \notin R$ as $1 \neq 0$. Also any subgroup of R under addition is a right-deal as 0 belongs to all subgroup of R under addition. Therefore $\{0\}$ and R are the only subgroup of R under addition. But that mean either $R = \{0\}$ or $o(R)$ is a prime. Thus in this case either $R = \{0\}$ or a ring with prime order, with no multiplicative identity and satisfying $r_1 r_2 = 0 \quad \forall\ r_1, r_2 \in R$. Note when $R = \{0\}$, then it is trivially a division ring.

Case 2: When $U = \{0\}$, it means $xr = 0 \quad \forall\ r \in R$ only for $x = 0$. In other words, for $a \neq 0$ we have $ar \neq 0$ at least for some $r \in R$. Now either $R = \{0\}$ or $R \neq \{0\}$. Suppose $R \neq \{0\}$, there exist some $a \in R$ with $a \neq 0$. But then $aR \neq \{0\}$. Also aR is a right-ideal; and $\{0\}$ and R are the only possible right-ideals, therefore, $aR = R$. We claim R to be a division ring. To establish our claim, we need to show existence of multiplicative right-identity 1 and right-inverse of any any non-zero element, say a. Suppose some $x, y \in R$ such that $xy = 0$ with $x \neq 0$ and $y \neq 0$. We have $xR = R$ and $yR = R$ as $x \neq 0$ and $y \neq 0$. But then $(xy)R = x(yR) = x(R) = R$. So $xy = 0 \Rightarrow 0R = R$ or $\{0\} = R$, which is not the case. Therefore in R, $x \neq 0$ and $y \neq 0 \Rightarrow xy \neq 0$. Reading the contrapositive of the statement, we have $xy = 0 \Rightarrow x = 0$ or $y = 0$, or R has no

zero-divisors. Now $aR = R$ implies there exist some element $u_0 \in R$ such that $au_0 = a$. Clearly $u_0 \neq 0$ otherwise that would mean $a = 0$. Also $(au_0)u_0 = au_0$, or $a(u_0u_0 - u_0) = 0$. But R has no zero-divisors and $a \neq 0$, so $u_0u_0 - u_0 = 0$. Therefore $u_0u_0 = u_0$. We claim u_0 to the required multiplicative right-identity. Suppose if not, then there must exist some $r \in R$ such that $ru_0 \neq r$. But then $(ru_0 - r)u_0 = ru_0u_0 - ru_0 = ru_0 - ru_0 = 0$, i.e. $(ru_0 - r)u_0 = 0$. Again R has no zero-divisors, so $ru_0 - r = 0$ as $u_0 \neq 0$. Thus $ru_0 = r$ which is a contradiction. Hence $ru_0 = r \quad \forall\, r \in R$, or u_0 is the multiplicative right-identity of R. Again $aR = R$ implies that there exist some a' such that $aa' = u_0$. So the right-inverse a' of an arbitrarily chosen element $a \neq 0$ exists in R. This establishes R to be a division ring. So we have either $R = \{0\}$ or is a division ring. But $\{0\}$ itself is a division ring. So R is a division ring.

Combining both *Cases*, we have either R is a division ring or R is a ring of prime order with $r_1r_2 = 0 \quad \forall\, r_1, r_2 \in R$. Hence the result. ∎

3. Let J be the ring of integers, p a prime number, and (p) the ideal of J consisting of all multiples of p. Prove
(a) $J/(p)$ is isomorphic to J_p, the ring of integers mod p.
(b) Using Theorem 3.5.1 and part (a) of this problem, that J_p is a field.
Solution:
(a) We define $\phi : J/\langle p\rangle \longrightarrow J_p$ such that $\phi(\langle p\rangle + x) = x \bmod p$. We claim mapping ϕ is well-defined. Suppose some $\langle p\rangle + x = \langle p\rangle + x'$. So we have $x = x' + mp$ for some integer m. Therefore $\phi(\langle p\rangle + x) = x \bmod p = (x' + mp) \bmod p = x' \bmod p = \phi(\langle p\rangle + x')$. Also $\phi(\langle p\rangle + x) \in J_p \quad \forall\, x \in J$. Thus ϕ is well-defined. We have

$$\begin{aligned}
\phi(\langle p\rangle + x) = \phi(\langle p\rangle + y) &\Rightarrow x \equiv y \bmod p \\
&\Rightarrow x - y \equiv 0 \bmod p \\
&\Rightarrow x - y = mp \text{ for some integer } m \\
&\Rightarrow x - y \in \langle p\rangle \\
&\Rightarrow \langle p\rangle + x = \langle p\rangle + y
\end{aligned}$$

So $\phi(\langle p\rangle + x) = \phi(\langle p\rangle + y)$ implies $\langle p\rangle + x = \langle p\rangle + y$. Thus mapping ϕ is one-to-one. Also if some $y \in J_p$, then we have $\phi(\langle p\rangle + y) = y$, i.e. every element of J_p has inverse-image in $J_p/\langle p\rangle$. So mapping ϕ is onto too. Finally, we establish ϕ is a homomorphism. We have

$$\begin{aligned}
\phi((\langle p\rangle + x) + (\langle p\rangle + y)) &= \phi(\langle p\rangle + (x + y)) \\
&= (x + y) \bmod p \\
&= (x \bmod p + y \bmod p) \bmod p \\
&= \phi(\langle p\rangle + x) + \phi(\langle p\rangle + y)
\end{aligned}$$

And

$$\begin{aligned}\phi((\langle p\rangle + x)(\langle p\rangle + y)) &= \phi(\langle p\rangle + (xy)) \\ &= (xy) \bmod p \\ &= ((x \bmod p)(y \bmod p)) \bmod p \\ &= \phi(\langle p\rangle + x)\phi(\langle p\rangle + y)\end{aligned}$$

So mapping ϕ is a homomorphism too. Concluding ϕ is an onto isomorphism from $J/\langle p\rangle$ to J_p. So $J/\langle p\rangle \approx J_p$.

(b) First we will show that $\langle p\rangle$ is a maximal ideal of J. Suppose, if possible there exists some ideal U of R such that $\langle p\rangle \subsetneq U \subsetneq J$. Since $U \neq \langle p\rangle$, therefore there exists some $x \in U$ such that $x \neq \langle p\rangle$. So $x \neq pk$ for some integer k. But that means $p \nmid x$. Also p being prime, therefore $gcd(p, x) = 1$. Thus $pi + xj = 1$ for some $i, j \in J$. But $p \in \langle p\rangle \subset U$, therefore $pi \in U$; also $x \in U$, therefore $xj \in U$. So $pi + xj \in U$, or $1 \in U$. But $1 \in U$ implies $U = J$. Thus there does not exist an ideal U such that $\langle p\rangle \subsetneq U \subsetneq J$. So $\langle p\rangle$ is a maximal ideal of J. Finally, using Theorem 3.5.1, we have $J/\langle p\rangle$ is a field. But $J/\langle p\rangle \approx J_p$, so J_p too is a field. ∎

**4. Let R be the ring of all real-valued continuous functions on the closed unit interval. If M is a maximal ideal of R, prove that there exists a real number γ, $0 \leq \gamma \leq 1$, such that $M = M_\gamma = \{f(x) \in R \mid f(\gamma) = 0\}$.
Solution:[Warning: solution is wrong explain why!] Let $\mathbb{R}$ denotes the field of real numbers. Suppose M be some maximal ideal of R. We define $A_\alpha = \{f(x) \mid_{x=\alpha} \mid f(x) \in M\}$ where $\alpha \in [0, 1]$. It is easy to see that A_α is an ideal of $\mathbb{R}$. But $\mathbb{R}$ being a field, so either $A_\alpha = \{0\}$ or $A_\alpha = \mathbb{R}$. Also we have either $A_\alpha = \{0\}$ for some $\alpha \in [0, 1]$ or $A_\alpha \neq \{0\}$ for all $\alpha \in [0, 1]$.

Case 1: Suppose $A_\alpha = \{0\}$ for some $\alpha = \gamma$(say) $\in [0, 1]$. Therefore we have $\{f(x) \mid_\gamma \mid f(x) \in M\} = \{0\}$. In other words, for all $f(x) \in M$, we have $f(\gamma) = 0$. We define $M_\gamma = \{f(x) \in R \mid f(\gamma) = 0\}$. Therefore $M \subset M_\gamma$. So we have $M \subset M_\gamma \subset R$. Also it is easy to check that M_γ is an ideal of R. But $M_\gamma \neq R$ as there are functions $h(x) \in R$ such that $h(\gamma) \neq 0$. So M being a maximal implies $M_\gamma = M$.

Case 2: In this case we have $A_\gamma \neq \{0\}$ for all $\alpha \in [0, 1]$. Therefore $A_\alpha = \mathbb{R}$ for all $\alpha \in [0, 1]$. Now since M is maximal ideal in R, so there exists a function $g(x) \in R$ such that $g(x) \notin M$. Also for $m(x) \in M$ and $r(x) \in R$, we have $m(x)r(x) \in M$. Therefore $g(x) \neq m(x)r(x)$ for any $m(x) \in M$ and any $r(x) \in R$. But that also means that there exists some $\beta \in [0, 1]$ such that $g(x) \mid_{x=\beta} \neq m(x)r(x) \mid_{x=\beta}$ for any $m(x) \in M$ and any $r(x) \in R$. Also $A_\beta = \mathbb{R}$, so $m(\beta)$ can assume any value in $\mathbb{R}$. Also $r(\beta)$ can assume any value in $\mathbb{R}$. Therefore $m(\beta)r(\beta)$ can assume any value in $\mathbb{R}$. So $g(\beta) \neq m(\beta)r(\beta)$ is not

possible as $g(\beta) \in \mathbb{R}$. So $A_\alpha = \mathbb{R}$ for all $\alpha \in [0,1]$ is not possible.

Thus we concluded if M is some maximal ideal of R, then M must equal to M_γ for some $\gamma \in [0,1]$, where $M_\gamma = \{f(x) \in R \mid f(\gamma) = 0\}$. ∎

Problems (Page 142)

1. Prove that if $[a,b]=[a',b']$ and $[c,d]=[c',d']$ then $[a,b][c,d]=[a',b'][c',d']$.
Solution: We have

$$[a,b]=[a',b'] \Leftrightarrow ab'=a'b \tag{1}$$

Similarly,

$$[c,d]=[c',d'] \Leftrightarrow cd'=c'd \tag{2}$$

We need to show

$$\begin{aligned} & [a,b][c,d]=[a',b'][c',d'] \\ \Leftrightarrow\ & [ac,bd]=[a'c',b'd'] \\ \Leftrightarrow\ & acb'd'=a'c'bd \end{aligned} \tag{3}$$

We have

$$\begin{aligned} acb'd' &= (ab')(cd') \\ &= (a'b)(c'd) \end{aligned}$$

Using (1) and (2)

$$= a'c'bd$$

Hence $[a,b][c,d]=[a',b'][c',d']$. ∎

2. Prove the distributive law in F.
Solution: We have

$$\begin{aligned} [a,b]([c,d]+[e,f]) &= [a,b][cf+ed,df] \\ &= [a(cf+ed),bdf] \\ &= [acf+aed,bdf] \\ &= [bacf+baed),b^2df] \\ &= [(ac)(bf)+(ae)(bd),(bd)(bf)] \\ &= [ac,bd]+[ae,bf] \\ &= [a,b][c,d]+[a,b][e,f] \end{aligned}$$

Similarly the other distributive law hold good. ∎

3. Prove that the mapping $\phi : D \longrightarrow F$ defined by $\phi(a)=[a,1]$ is an isomorphism of D into F.

Solution: We need to show ϕ is an one-to-one homomorphism. Clearly mapping ϕ is well-defined. Also we have

$$\begin{aligned}\phi(a+b) &= [a+b,1] \\ &= [a,1]+[b,1] \\ &= \phi(a)+\phi(b)\end{aligned}$$

Also

$$\begin{aligned}\phi(ab) &= [ab,1] \\ &= [a,1][b,1] \\ &= \phi(a)\phi(b)\end{aligned}$$

So mapping ϕ is a ring homomorphism. Also we have

$$\begin{aligned}\phi(a)=\phi(b) &\Rightarrow [a,1]=[b,1] \\ &\Rightarrow a1=b1 \\ &\Rightarrow a=b\end{aligned}$$

Thus mapping ϕ is one-to-one too. Hence ϕ is an one-to-one homomorphism. ∎

4. Prove that if K is any field which contains D then K contains a subfield isomorphic to F. (*In this sense F is the smallest field containing D.*)
Solution: We are given D is an integral domain; K some field containing D; and F field of quotients of D. We define $\phi : F \longrightarrow K$ such that $\phi([a,b]) = ab^{-1}$. We claim mapping ϕ so defined is a well-defined mapping. We have $[a,b] \in F \Rightarrow a,b \in D$ with $b \neq 0 \Rightarrow a,b \in K$ with $b \neq 0 \Rightarrow a,b^{-1} \in K \Rightarrow ab^{-1} \in K$. Also if $[a,b] = [a',b']$ with $b,b' \neq 0$, then we have $ab' = a'b \Rightarrow ab'(b^{-1}b'^{-1}) = a'b(b^{-1}b'^{-1}) \Rightarrow ab^{-1} = a'b'^{-1} \Rightarrow \phi([a,b]) = \phi([a',b'])$. Hence the mapping is well-defined.
Also we have

$$\begin{aligned}\phi([a,b]+[c,d]) &= \phi([ad+cb,bd]) \\ &= (ad+cb)(bd)^{-1} \\ &= (ad+cb)(b^{-1}d^{-1}) \\ &= adb^{-1}d^{-1}+cbb^{-1}d^{-1} \\ &= ab^{-1}+cd^{-1} \\ &= \phi([a,b])+\phi([c,d])\end{aligned}$$

and

$$\phi([a,b][c,d]) = \phi([ac,bd])$$

$$
\begin{aligned}
&= ac(bd)^{-1} \\
&= acb^{-1}d^{-1} \\
&= (ab^{-1})(cd^{-1}) \\
&= \phi([a,b])\phi([c,d])
\end{aligned}
$$

Thus ϕ is a ring homomorphism. Also we have

$$
\begin{aligned}
\phi([a,b]) = \phi([c,d]) &\Rightarrow ab^{-1} = cd^{-1} \\
&\Rightarrow ab^{-1}(bd) = cd^{-1}(bd) \\
&\Rightarrow ad = cb \\
&\Rightarrow [a,b] = [c,d]
\end{aligned}
$$

So mapping ϕ is one-to-one too. Thus ϕ is an one-to-one homomorphism. Also $\phi(F)$ is a subfield of K (Check). Thus $F \approx \phi(F)$. Hence the result. ∎

*5. Let R be a commutative ring with unit element. A non-empty subset S of R is called a multiplicative system if
1. $0 \notin S$
2. $s_1, s_2 \in S$ implies that $s_1, s_2 \in S$.
Let $\mathcal{M}$ be the set of all ordered pairs (r,s) where $r \in R$, $s \in S$. In $\mathcal{M}$ define $(r,s) \sim (r',s')$ if there exists an element $s'' \in S$ such that

$$s''(rs' - sr') = 0.$$

(a) Prove that this defines an equivalence relation on $\mathcal{M}$.
Let the equivalence class of (r,s) be denoted by $[r,s]$, and let R_S be the set of all the equivalence classes. In R_S define $[r_1,s_1] + [r_2,s_2] = [r_1s_2 + r_2s_1, s_1s_2]$ and $[r_1,s_1][r_2,s_2] = [r_1r_2, s_1s_2]$.
(b) Prove that the addition and multiplication described above are well-defined and that R_S forms a ring under these operations.
(c) Can R be embedded in R_S?
(d) Prove that the mapping $\phi : R \longrightarrow R_S$, defined by $\phi(a) = [as, s]$ is a homomorphism of R into R_S and find the kernel of ϕ.
(e) Prove that this kernel has no element of S in it.
(f) Prove that every element of the form $[s_1,s_2]$(where $s_1, s_2 \in S$) in R_S has an inverse in R_S.
Solution:
(a) A relation is an equivalence if it satisfies reflexivity, symmetry and transitivity properties.
Reflexivity: We have $s'(rs - rs) = 0$ for any $s' \in S$, which means $(r,s) \sim (r,s)$. Hence the relation is reflexive.
Symmetry: We are given $(r,s) \sim (r',s')$. So $s''(rs' - sr') = 0$ for some $s'' \in S$. But $s''(rs' - sr') = 0 \Rightarrow -s''(r's - s'r) = 0 \Rightarrow (r',s') \sim (r,s)$. Hence the relation is symmetric too.

Transitivity: We are given $(r,s) \sim (r',s')$ and $(r',s') \sim (r'',s'')$. But $(r,s) \sim (r',s')$ implies $s_1(rs' - r's) = 0$ for some $s_1 \in S$. So we have

$$s_1 r s' = s_1 r' s \tag{1}$$

Similarly, $(r',s') \sim (r'',s'')$ implies, for some $s_2 \in S$

$$s_2 r' s'' = s_2 r'' s' \tag{2}$$

We need to show

$$\begin{aligned} & (r,s) \sim (r'',s'') \\ \Leftrightarrow\ & s_3(rs'' - r''s) = 0 \end{aligned}$$

for some $s_3 \in S$. Let $s_3 = s_1 s_2 s'$, therefore

$$\begin{aligned} & (r,s) \sim (r'',s'') \\ \Leftarrow\ & s_1 s_2 s'(rs'' - r''s) = 0 \\ \Leftarrow\ & (s_1 r s') s_2 s'' - s_1 s_2 s' r'' s = 0 \end{aligned}$$

Using (1),

$$\begin{aligned} \Leftarrow\ & (s_1 r' s) s_2 s'' - s_1 s_2 s' r'' s = 0 \\ \Leftarrow\ & s_1 s (s_2 r' s'') - s_1 s_2 s' r'' s = 0 \end{aligned}$$

Using (2),

$$\begin{aligned} \Leftarrow\ & s_1 s (s_2 r'' s') - s_1 s_2 s' r'' s = 0 \\ \Leftarrow\ & 0 = 0 \end{aligned}$$

Thus the relation is transitive too. Hence the relation $\sim$ is an equivalence relation.

(b) We will first show addition $+ : R_S \times R_S \longrightarrow R_S$ is well-defined. Suppose $[r_1,s_1] = [r_1',s_1']$ and $[r_2,s_2] = [r_2',s_2']$. But $[r_1,s_1] = [r_1',s_1']$ implies

$$s_3 r_1 s_1' = s_3 r_1' s_1, \tag{3}$$

for some $s_3 \in S$. Also $[r_2,s_2] = [r_2',s_2']$ implies

$$s_4 r_2 s_2' = s_4 r_2' s_2, \tag{4}$$

for some $s_4 \in S$. Now in order to prove addition is well-defined, we need to show

$$[r_1,s_1] + [r_2,s_2] = [r_1',s_1'] + [r_2',s_2']$$

$$\Leftrightarrow [r_1s_2 + r_2s_1, s_1s_2] = [r_1's_2' + r_2's_1', s_1's_2']$$
$$\Leftrightarrow s_5((r_1s_2 + r_2s_1)s_1's_2' - (r_1's_2' + r_2's_1')s_1s_2) = 0$$

for some $s_5 \in S$. Let $s_5 = s_3s_4$, therefore

$$[r_1, s_1] + [r_2, s_2] = [r_1', s_1'] + [r_2', s_2']$$
$$\Leftarrow s_3s_4((r_1s_2 + r_2s_1)s_1's_2' - (r_1's_2' + r_2's_1')s_1s_2) = 0$$

But putting values form (3) and (4), we have left-hand side of the above equation equals to 0. Hence addition is well-defined.

Next we will show multiplication is well-defined. Again suppose $[r_1, s_1] = [r_1', s_1']$ and $[r_2, s_2] = [r_2', s_2']$. But these equalities imply (3) and (4) respectively. We need to show

$$[r_1, s_1][r_2, s_2] = [r_1', s_1'][r_2', s_2']$$
$$\Leftrightarrow [r_1r_2, s_1s_2] = [r_1'r_2', s_1's_2']$$
$$\Leftrightarrow s_5(r_1r_2s_1's_2' - r_1'r_2's_1s_2) = 0$$

for some $s_5 \in S$. Let $s_5 = s_3s_4$, therefore

$$[r_1, s_1][r_2, s_2] = [r_1', s_1'][r_2', s_2']$$
$$\Leftarrow s_3s_4(r_1r_2s_1's_2' - r_1'r_2's_1s_2) = 0$$

Putting values from (3) and (4), we have left-hand side of the above equation equals to 0. Hence multiplication is well-defined too.

Since S is assumed to be non-empty, so some $s_0 \in S$. Now rest is routine to check R_S is a commutative ring with unity. Note that $[0, s_0]$ is the additive identity and $[s_0, s_0]$ is the multiplicative identity.

(c) In general no. (See part (d))

(d) We have $\phi : R \longleftarrow R_S$ such that $\phi(a) = [as, s]$. Easy to check ϕ is well-defined. Also

$$\begin{aligned}\phi(a + b) &= [(a + b)s, s] \\ &= [as^2 + bs^2, ss] \\ &= [as, s] + [bs + s] \\ &= \phi(a) + \phi(b)\end{aligned}$$

and

$$\phi(ab) = [(ab)s, s]$$

$$= [(as)(bs), ss]$$
$$= [as, s][bs, s]$$
$$= \phi(a)\phi(b)$$

Hence ϕ is a ring homomorphism.
Let K_ϕ denotes the kernel of mapping ϕ. Now K_ϕ in general depends upon the choice of S. We illustrate it with example. Suppose some positive integer $n = pq$, where p and q are prime integers. Consider $R = \mathbb{Z}_n$ with addition modulo n and multiplication modulo n as its addition and multiplication. Let $U_n = \{1 \leq x < n \mid gcd(x, n) = 1\}$. Let $S = U_n$ and $S' = U_n \cup \{p\}$. One can check both S and S' are multiplicative system of R. But when we are working with the multiplicative system S, K_ϕ turns out to be $\{0\}$. Whereas when we have S' as our multiplicative system, with $\phi(a) = [ap, p]$, $K_\phi \neq \{0\}$ as $\phi(q) = [0, p]$. As for a given ring, there might be more than one possible multiplicative system, so K_ϕ, in general depends upon the multiplicative system that we have chosen.

(e) Let $\phi : R \longrightarrow R_S$ such that $\phi(a) = [as, s]$, where $s \in S$. Let some $x \in K_\phi$, therefore $\phi(x) = [0, s] \Rightarrow [xs, s] = [0, s] \Rightarrow s'xs^2 = 0$ for some $s' \in S$. Now if $x \in S$, then $s'xs^2 \neq 0 \quad \forall\, s' \in S$. Thus if $x \in K_\phi$, then $x \notin S$. Hence the result.

(f) We have $[s_2, s_1]$ as the inverse element of $[s_1, s_2]$ for $s_1, s_2 \in S$ as $[s_2, s_1][s_1, s_2] = [s, s]$ where $s \in S$ and $[s, s]$ is the multiplicative identity. Hence every element of form $[s_1, s_2]$ for $s_1, s_s \in S$ has inverse in R_S. ∎

6. Let D be an integral domain, $a, b \in D$. Suppose that $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n. Prove that $a = b$.
Solution: First note that D is given only an integral domain, therefore multiplicative identity and inverse of an element under multiplication may not exist. So for $x \in D$, x^n is defined only for positive integers n.

When $a = 0$, we have $b^n = a^n = 0^n = 0$ where n is given a positive integer. If $n = 1$, then $b^1 = 0 = a$, hence the result. But if $n > 1$, then also we claim $b^n = 0$ implies $b = 0$. Suppose we have $b^n = 0$ with $b \neq 0$. But then there must exist $1 < p \leq n$ such that $b^p = 0$ and $b^{p-1} \neq 0$. So we have $b^p = b^{p-1}b = 0$, also D being an integral domain implies $b = 0$ or $b^{p-1} = 0$. In both the cases we have contradiction. Therefore $b^n = 0 \Rightarrow b = 0$. So if $a = 0$, then $a = b$.

When $a \neq 0$, we will prove the result by making use of the field of quotients of D. Let F be the field of quotients of D. Define $\phi : D \longrightarrow F$ such that $\phi(x) = [xd, d]$, where $d \neq 0 \in D$. It is easy to check that ϕ so defined is an one-to-one ring homomorphism. Now in the field F, with $a \neq 0$ and $d \neq 0$, we have $[ad, d] \neq [0, d]$ as D has no zero-divisors. So $[ad, d]^k$ is well-defined for all

$k \in \mathbb{Z}$. So we have

$$\begin{aligned}
\phi(a) &= [ad, d] \\
&= [ad, d]^1 \\
&= [ad, d]^{mi+nj} \text{ as } gcd(m, n) = 1 \\
&= [(ad)^{mi+nj}, d^{mi+nj}] \\
&= [a^{mi+nj} d^{mi+nj}, d^{mi+nj}] \text{ as } D \text{ is commutative} \\
&= [a^{mi+nj} d, d] \\
&= [a^{mi} a^{nj} d, d] \\
&= [(a^m)^i (a^n)^j d, d] \\
&= [(b^m)^i (b^n)^j d, d] \\
&= [b^{mi+nj} d, d] \\
&= [bd, d] \\
&= \phi(b)
\end{aligned}$$

But mapping ϕ being one-to-one, so $\phi(a) = \phi(b)$ implies $a = b$. Hence the result. ∎

7. Let R be a ring, possibly noncommutative, in which $xy = 0$ implies $x = 0$ or $y = 0$. If $a, b \in R$ and $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n, prove that $a = b$.
Solution: First note that R may not have multiplicative identity or the inverse element of all elements. So for $x \in R$, x^l is only defined for positive integers l. Next we claim that in R, $x^l = 0$ for some positive integer l implies $x = 0$. Suppose $x \neq 0$. But $x^l = 0$, therefore there exists some positive integer $p > 1$ such that $x^p = 0$ and $x^{p-1} \neq 0$. But then we have $x^p = x^{p-1}x = 0$, R being having no zero-divisors, implying $x^{p-1} = 0$ or $x = 0$, both of which is a contradiction. Hence $x^l = 0 \Rightarrow x = 0$.

Next since m and n are relatively prime, so $mi + nj = 1$ for some $i, j \in \mathbb{Z}$. First suppose $i > 0$, therefore $nj = 1 - mi < 0$ as $m > 1$. Note if m or n is equal to 1 then we have nothing to prove, so we have assumed $m, n > 1$. Therefore for $i > 0$, we have $j < 0$. Let $j = -k$, therefore $k > 0$ and $mi - nk = 1$. So we have

$$\begin{aligned}
& a^{mi} = a^{1+nk} \\
\Rightarrow\ & (a^m)^i = a(a^n)^k \\
\Rightarrow\ & (b^m)^i = a(b^n)^k \\
\Rightarrow\ & b^{mi} b = a b^{nk} b \\
\Rightarrow\ & b^{mi+1} = a b^{nk+1} \\
\Rightarrow\ & b b^{mi} = a b^{mi}
\end{aligned}$$

$$\Rightarrow (b-a)b^{mi} = 0$$

So R being having no zero-divisors, we have $b - a = 0$ or $b^{mi} = 0$. When $b - a = 0$, we have $b = a$. While $b^{mi} = 0$ implies $b = 0$, which in turn mean $a^n = b^n = 0^n = 0$. So $a = 0$ too. Thus $a = b$ in both cases. Similarly when $i < 0$, we can show $j > 0$ and can proceed in a similar fashion to prove $a = b$. Finally if $i = 0$, then we have $nj = 1 \Rightarrow n = 1 \Rightarrow a^1 = b^1$. So $a = b$ in this case too. Hence $a = b$. ∎

Problems (Page 149)

1. In a commutative ring with unit element prove that the relation a is associate of b is an equivalence relation.
Solution: A relation is an equivalence relation if it satisfies reflexivity, symmetry, and transitivity properties.

> *Reflexivity*: Since $a = 1a$, and 1 is also a unit element, so a is associate of a itself. Thus associate relation is reflexive.
>
> *Symmetry*: Suppose a is associate of b. So $a = ub$ for some unit element u. u being unit element, therefore u^{-1} exists. So we have $a = ub \Rightarrow b = u^{-1}a$, showing b is associate of a. Thus the associate relation is symmetric too.
>
> *Transitivity*: Suppose a is associate of b, and b is associate of some c. So we have $a = u_1 b$ and $b = u_2 c$ for some units u_1 and u_2. Therefore $a = u_1 b = u_1 u_2 c$. But $u_1 u_2$ is again a unit as $(u_1 u_2)(u_1^{-1} u_2^{-1}) = 1$. So a is associate of c. Thus the associate relation is transitive too.

And hence the associate relation is an equivalence relation. ∎

2. In a Euclidean ring prove that any two greatest common divisors of a and b are associates.
Solution: Suppose d_1 and d_2 are greatest common divisors of a and b. That means $d_1 \mid a$ and $d_1 \mid b$. But d_2 being greatest common divisor of a and b, therefore if some $d_1 \mid a$ and $d_2 \mid b$, then d_2 must divide d_1. So $d_2 \mid d_1$. Symmetry of the argument implies $d_1 \mid d_2$. But then by Lemma 3.7.2, we have d_1 and d_2 are associates. Hence any two greatest common divisors are associates. ∎

3. Prove that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that $d(a) = d(1)$.
Solution: First, suppose a is a unit element. We will show $d(a) = d(1)$. Since in a Euclidean ring, $d(b) \leq d(ba)$ for all non-zero a and b, so assuming $b = 1$, we have $d(1) \leq d(a1)$, or $d(1) \leq d(a)$. Also a being unit element, so a^{-1} exists. Again $d(a) \leq d(ab)$, so putting $b = a^{-1}$, we have $d(a) \leq d(aa^{-1}) \Rightarrow d(a) \leq d(1)$. Hence $d(a) = d(1)$.

Conversely, suppose for some non-zero a, $d(a) = d(1)$. We need to show a is a unit element. In a Euclidean ring, we have $1 = qa + r$ for some q and r, with either $r = 0$ or $d(r) < d(a)$. When $r = 0$, we have $1 = qa$, which means a is a unit element. When $r \neq 0$, we have $d(r) < d(a)$. But $d(a) = d(1)$, so

$$d(r) < d(1) \tag{1}$$

Also $d(1) \leq d(1r)$, i.e.

$$d(1) \leq d(r) \tag{2}$$

But (1) and (2) implies $d(r) < d(r)$ which is absurd, hence $r = 0$ is the only possibility. So a is a unit element. Thus in a Euclidean ring, a is a unit element if and only if $d(a) = d(1)$. ∎

4. Prove that in a Euclidean ring (a, b) can be found as follows:

$$\begin{aligned} b &= q_0 a + r_1, \text{ where } d(r_1) < d(a) \\ a &= q_1 r_1 + r_2, \text{ where } d(r_2) < d(r_1) \\ r_1 &= q_2 r_2 + r_3, \text{ where } d(r_3) < d(r_2) \\ &\vdots \qquad\qquad\qquad\qquad \vdots \\ r_{n-1} &= q_n r_n \\ \text{and} \qquad r_n &= (a, b). \end{aligned}$$

Solution: We will first show that $gcd(a, b) = gcd(a, b - qa)$ for all $q \in R$, where R is assumed to be a Euclidean ring. Suppose $d_1 = gcd(a, b)$ and $d_2 = gcd(a, b - qa)$. So $d_1 \mid a$ and $d_2 \mid b$. Therefore $d_1 \mid a$ and $d_1 \mid (b - qa)$. But $gcd(a, b-qa) = d_2$, so $d_1 \mid d_2$. Again $d_2 \mid a$ and $d_2 \mid (b-qa)$. Therefore $d_2 \mid a$ and $d_2 \mid b$. But $gcd(a, b) = d_1$. Therefore $d_2 \mid d_1$. But $d_1 \mid d_2$ and $d_2 \mid d_1$ implies d_1 and d_2 are associates. So $gcd(a, b) = gcd(a, b - qa)$ upto associates.

Now since R is a Euclidean ring, therefore $b = q_0 a + r_1$, where either $r_1 = 0$ or $d(r_1) < d(a)$. If $r_1 = 0$, we are done as a is the required gcd. But if $r_1 \neq 0$, then we have $gcd(a, b) = gcd(a, b - q_0 a) = gcd(a, r_1) = gcd(r_1, a)$. Again we write $a = q_1 r_1 + r_2$ for some q_1, r_2 with either $r_2 = 0$ or $d(r_2) < d(r_1)$. Again if $r_2 = 0$, then clearly $gcd(a, b) = gcd(r_1, a) = r_1$. But if $r_2 \neq 0$, then we have $gcd(a, b) = gcd(r_1, a) = gcd(r_2, r_1)$. We can continue like this till we get some $r_{n+1} = 0$. Also when $r_{n+1} = 0$, we have $gcd(a, b) = gcd(r_1, a) = gcd(r_2, r_1) = \cdots = gcd(r_n, r_{n-1}) = r_n$ as $r_{n-1} = q_n r_n + 0$. All left is to show that r_{n+1} must be equal to 0 for some $n \in \mathbb{N}$. But suppose the process keep on going infinitely with all r_i not equal to 0. But then we get a strictly decreasing sequence $d(a), d(r_1), d(r_2), \cdots$ in $\mathbb{N}$ as $d(a) > d(r_1) > d(r_2) > \cdots$. Also $d(r_i) \geq 0 \quad \forall\, i$. So r_{n+1} must be equal to 0 for some $n \in \mathbb{N}$. Hence the result. ∎

5. Prove that if an ideal U of a ring R contains a unit of R, then $U = R$.
Solution: We will make use of the fact that if some $u \in U$ and $r \in R$, then $ur \in U$. Suppose U contains some unit element u. As u is a unit, therefore u^{-1} exists in R. Now $u \in U$ and $u_{-1} \in R$, therefore $uu^{-1} \in U$, or $1 \in U$. Again $1 \in U$ and let some $r \in R$, so we have $1r \in U$, or $r \in U$. That is for all $r \in R$, we have $r \in U$, which means $R \subset U$. But by definition, $U \subset R$. Therefore $U = R$. Hence the result. ∎

6. Prove that the units in a commutative ring with a unit element form an abelian group.
Solution: Let I be the set of all units elements. Ring being commutative implies I is commutative under multiplication. Suppose u_1 and u_2 are units. Therefore u_1^{-1}, u_2^{-1} exist. But then $(u_1u_2)(u_1^{-1}u_2^{-1}) = 1$. Therefore $u_1u_2 \in I$, or the closure property holds good. I being subset of the ring, therefore associativity under multiplication holds for all its elements. Also 1, multiplicative identity being a unit belongs to I too. Finally suppose some $u_1 \in I$, therefore there exists u_1^{-1} in the ring such that $u_1u_1^{-1} = 1$. But the equation also tells us that u_1^{-1} is a unit element, or $u_1^{-1} \in I$. Therefore existence of inverse of each element is also shown. So I is an abelian group under the multiplication. ∎

7. Given two elements a, b in the Euclidean ring R their *least common multiple* $c \in R$ is an element in R such that $a \mid c$ and $b \mid c$ and such that whenever $a \mid x$ and $b \mid x$ for $x \in R$ then $c \mid x$. Prove that any two elements in the Euclidean ring R have a least common multiple in R.
Solution: We assume both a and b as non-zero elements, otherwise $a \mid c$ or $b \mid c$ would not be defined. We define $\langle a\rangle$ as the smallest ideal of R containing a. One can easily see that whenever some ring R is commutative and has unity element, then we have $\langle a\rangle = aR = \{ar \mid r \in R\}$. So $\langle a\rangle = aR$. Similarly we have $\langle b\rangle = bR$. Let $U = \langle a\rangle \cap \langle b\rangle$. Clearly U is an ideal of R. Now we make use of the fact that R is a principal ideal ring. Note that a Euclidean ring is always a principal ideal ring. So $U = cR$ for some $c \in R$. We claim c is the required least common multiple of a and b. We have $U \subset \langle a\rangle$. Also $c = c1 \in cR$. So $c \in U \subset \langle a\rangle$. Therefore $c = ar_1$ for some $r_1 \in R$, or $a \mid c$. Similarly, $c \in U \subset \langle b\rangle$, implying $c = br_2$, or $b \mid c$. So $a \mid c$ and $b \mid c$. Next suppose $a \mid x$ and $b \mid x$ for some $x \in R$. Therefore $x = ar_3$ and $x = br_4$ for some $r_3, r_4 \in R$. But that would mean $x \in aR = \langle a\rangle$ and $x \in bR = \langle b\rangle$. So $x \in \langle a\rangle \cap \langle b\rangle = U$. Therefore $x = cr_5$ for some $r_5 \in R$. So $c \mid x$. Thus whenever $a \mid x$ and $b \mid x$ implies $c \mid x$. Thus c is the least common multiple of a and b. So we concluded that the least common multiple of two non-zero elements always exists in a Euclidean ring. ∎

8. In Problem 7, if the least common multiple of a and b is denoted by $[a, b]$, prove that $[a, b] = ab/(a, b)$.
Solution: Let c and d be the least common multiple and the greatest common divisor respectively of a and b in R. We assume R to be a Euclidean ring. Therefore $\langle c\rangle = \langle a\rangle \cap \langle b\rangle$ and $\langle d\rangle = \langle a, b\rangle = \langle a\rangle + \langle b\rangle$. Also in a commutative ring we have $\langle xy\rangle = \langle\langle x\rangle\langle y\rangle\rangle$. So we have

$$\begin{aligned}
\langle cd\rangle &= \langle\langle c\rangle\langle d\rangle\rangle \\
&= \langle(\langle a\rangle \cap \langle b\rangle)(\langle a\rangle + \langle b\rangle)\rangle \\
&= \langle(\langle a\rangle \cap \langle b\rangle)\langle a\rangle + (\langle a\rangle \cap \langle b\rangle)\langle b\rangle\rangle \\
&= \langle((\langle a\rangle\langle a\rangle) \cap (\langle b\rangle\langle a\rangle)) + ((\langle a\rangle\langle b\rangle) \cap (\langle b\rangle\langle b\rangle))\rangle
\end{aligned}$$

$$
\begin{aligned}
&= \langle (\langle a \rangle \cap (\langle a \rangle \langle b \rangle)) + ((\langle a \rangle \langle b \rangle) \cap \langle b \rangle) \rangle \\
&= \langle \langle a \rangle \langle b \rangle + \langle a \rangle \langle b \rangle \rangle \\
&= \langle \langle a \rangle \langle b \rangle \rangle \\
&= \langle ab \rangle
\end{aligned}
$$

But $\langle cd \rangle = \langle ab \rangle$ implies $cd = ab$(upto associates). Hence the result. ∎

Problems (Page 152)

1. Find all the units in $J[i]$.
Solution: Using Problem 3 (Page 149 of the book), we have u a unit element of $J[i]$ if and only if $d(u) = d(1)$. Let $u = a + bi$, therefore u is a unit element if and only if $d(u) = a^2 + b^2 = d(1) = 1^2 + 0^2 = 1$. But the integral solutions of $a^2 + b^2 = 1$ are $a = 0, b = \pm 1$ and $a = \pm 1, b = 0$. Thus $i, -i, 1, -1$ are the only unit elements of $J[i]$ ∎

2. If $a + bi$ is not a unit of $J[i]$ prove that $a^2 + b^2 > 1$.
Solution: We have $d(a + bi) \in \mathbb{W}$. If $d(a + bi) = a^2 + b^2 = 0$, then $a + bi = 0$. When $d(a + bi) = 1 = d(1)$, then $a + bi$ is a unit element. So if $a + bi$ is neither a unit element nor a zero element then $d(a + bi) > 1$. Hence the result. ∎

3. Find the greatest common divisor in $J[i]$ of
(a) $3 + 4i$ and $4 - 3i$ (b) $11 + 7i$ and $18 - i$.
Solution:
(a) Clearly $3 + 4i = i(4 - 3i)$. So $gcd(3 + 4i, 4 - 3i) = 4 - 3i$

(b) We resort to $\mathbb{Q}[i]$. We have

$$\begin{aligned}\frac{18 - i}{11 + 7i} &= \frac{(18 - i)(11 - 7i)}{(11 + 7i)(11 - 7i)} \\ &= \frac{191 - 137i}{170} \\ &= \left(1 + \frac{21}{170}\right) - \left(1 - \frac{33}{170}\right) i \\ &= (1 - i) + \frac{21 + 33i}{170} = q + r' \text{ (say)} \qquad (1)\end{aligned}$$

Note that we have reduced $r' = a + ib$ (say) such that $|a|, |b| \leq \frac{1}{2}$. So $d(r') \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 < 1$. Multiplying (1) by $11 + 7i$, we have $18 - i = (11 + 7i)q + (11 + 7i)r' = (11 + 7i)q + r$. So $d(r) = d((11 + 7i)r') = d(11 + 7i)d(r') < d(11 + 7i)$ as $d(r') < 1$. Thus we are following the steps of Euclidean algorithm for finding gcd as described in Problem 4 (Page 149 of the book). So we have $18 - i = (11 + 7i)(1 - i) + r$ where r can be found by equating both sides of this equation itself. Thus we have $18 - i = (11 + 7i)(1 - i) + 3i$ with $d(3i) < d(11 + 7i)$. Also

$$gcd(18 - i, 11 + 7i) = gcd(11 + 7i, 3i)$$

Again

$$\begin{aligned}\frac{11 + 7i}{3i} &= \frac{(11 + 7i)(-3i)}{(3i)(-3i)} \\ &= \frac{21 - 33i}{9}\end{aligned}$$

$$= (2-4i) + \frac{3+3i}{9}$$

So we have $11+7i = (3i)(2-4i) + (-1+i)$ and

$$gcd(11+7i, 3i) = gcd(3i, -1+i)$$

Again we have

$$\begin{aligned}\frac{3i}{-1+i} &= \frac{3i(-1-i)}{(-1+i)(-1-i)} \\ &= \frac{3-3i}{2} \\ &= (1-i) + \frac{1-i}{2}\end{aligned}$$

So we have $3i = (-1+i)(1-i) + i$ and

$$gcd(3i, -1+i) = gcd(-1+i, i)$$

But $gcd(-1+i, i) = 1$ as i is a unit element of $J[i]$. Hence

$$gcd(18-i, 11+7i) = 1 \quad \blacksquare$$

4. Prove that if p is a prime number of the form $4n+3$, then there no x such that $x^2 \equiv -1 \bmod p$.
Solution: We need to show there is no x such that $x^2 + 1 \equiv 0 \bmod p$, when p is of form $4n+3$. Consider polynomial $f(x) = x^2 + 1$ in $\mathbb{Z}_4[x]$. We have

$$\begin{aligned}f(x) \mid_{x=0} &= 1 \\ f(x) \mid_{x=1} &= 2 \\ f(x) \mid_{x=2} &= 1 \\ f(x) \mid_{x=3} &= 2\end{aligned}$$

Thus $f(x) \neq 3$ in $\mathbb{Z}_4[x]$. Now consider $f(x)$ as a polynomial in $\mathbb{Z}[x]$. So we have $f(x) \neq 4n+3$ for all $x \in \mathbb{Z}$ and for any $n \in \mathbb{Z}$. So if p is of form $4n+3$, $f(x) = x^2 + 1 \not\equiv 0 \bmod p$ for any $x \in \mathbb{Z}$. Hence the result.

ALITER: Suppose $x^2 \equiv -1 \bmod p$ has solution, where $p = 4n+3$ for some $n \in \mathbb{W}$. We have $\frac{p-1}{2} = 2n+1$. So we have

$$\begin{aligned}x^2 \equiv -1 \bmod p &\Rightarrow (x^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \bmod p \\ &\Rightarrow x^{p-1} = (-1)^{2n+1} \bmod p\end{aligned}$$

But we have $x^{p-1} = 1 \bmod p$, for p a prime number (Fermat Theorem), so

$$x^2 \equiv -1 \bmod p \Rightarrow 1 = -1 \bmod p$$

which is only possible when $p = 2$, which is not case. Hence $x^2 \equiv -1 \bmod p$ has no solution in x for p prime of form $4n + 3$. ∎

5. Prove that no prime of the form $4n + 3$ can be written as $a^2 + b^2$ where a and b are integers.
Solution: As in the previous problem we consider $a^2 + b^2$ with $a, b \in \mathbb{Z}_4$. By brute force, we can see $a^2 + b^2 \neq 3 \bmod 4$ for all $a, b \in \mathbb{Z}_4[x]$. Considering $a^2 + b^2$ in $\mathbb{Z}$, we have $a^2 + b^2 \neq 4n + 3$ for any $n \in \mathbb{Z}$. Thus if p is of form $4n + 3$, then it cannot be equal to $a^2 + b^2$ for any $a, b \in \mathbb{Z}$. Hence the result. ∎

6. Prove that there is an infinite number of primes of the form $4n + 3$.
Solution: We will adapt the proof given by Euclid. Suppose primes of form $4n+3$ are finite. Let $3 = p_1 < p_2 < \cdots < p_k$ for some $k \in \mathbb{N}$, are the all primes of form $4n+3$. Consider $a = 4(p_1 p_2 \cdots p_k) - 1$. Clearly, $a = 4((p_1 p_2 \cdots p_k) - 1) + 3$, i.e. is a number of form $4n + 3$. Also $a > p_k$, so a is a composite number as $p_1, p_2, \cdots, p_k$ are the only primes of form $4n + 3$. We have $p_i \nmid a \quad \forall\, i$ as if $p_i \mid a$ implies $p_i \mid 1$ which is not the case. Also $2 \nmid a$ as $2 \nmid 1$. Thus if a is a composite number then $a = q_1 q_2 \cdots q_l$ where $q_i \quad \forall\, i$ are primes of form $4n + 1$. But product of integers of form $4n + 1$ is again an integer of form $4n + 1$. Thus it leads to the conclusion that a is an integer of form $4n + 1$, which is not true as a is an integer of form $4n + 3$. Thus primes of form $4n + 3$ cannot be finite. ∎

*7. Prove there exists an infinite number of primes of the form $4n + 1$.
Solution: Suppose there are finite number of primes of form $4n + 1$. Let $p_1, p_2, \cdots, p_k$ be all the primes of form $4n + 1$ for some $k \in \mathbb{N}$. We define $a = (2p_1 p_2 \cdots p_k)^2 + 1$. Clearly a is of form $4n + 1$. But $a > p_i$ for all i, therefore a must be composite. Let some prime p divides a. Therefore $a = 0 \bmod p \Rightarrow (2p_1 p_2 \cdots p_k)^2 + 1 = 0 \bmod p \Rightarrow (2p_1 p_2 \cdots p_k)^2 = -1 \bmod p$. This means that the equation $x^2 = -1 \bmod p$ in x has solution which is $x = 2p_1 p_2 \cdots p_k$. But then by Problem 4, p must not be of form $4n + 3$. So p is of form $4n + 1$ or is equal to 2. When $p = 2$, we have $2 \mid a \Rightarrow 2 \mid (2p_1 p_2 \cdots p_k)^2 + 1$. But $2 \mid (2p_1 p_2 \cdots p_k)^2$, so $2 \mid a$ implies $2 \mid 1$ which is not true. So $p = 2$ is not feasible. When p is of form $4n + 1$, then $p = p_i$ for some i as these are the only primes of form $4n + 1$. But then again $p \mid a$ leads to conclusion that $p \mid 1$ which is not true. Thus the assumption that primes of form $4n + 1$ are finite leads to contradiction. Hence primes of form $4n + 1$ must be infinite in number. ∎

*8. Determine all the prime elements in $J[i]$.

Solution: We first claim if $z \in J[i]$ is a prime element(unique upto associates), then $z \mid p$ for some prime $p \in \mathbb{Z}$. To establish our claim first note that $z\bar{z} = d(z) \in \mathbb{N}$. But $\mathbb{Z}$ being a Unique Factorization Domain, so we have $z\bar{z} = d(z) = p_1 p_1 \cdots p_k$ for some prime elements $p_i \in \mathbb{Z}$. Also $z \mid z\bar{z}$, so $z \mid p_1 p_2 \cdots p_k$. Now z a prime element in $J[i]$ and p_i belonging in $J[i]$ too. So z must divides some p_i. Hence our claim. We restate our result again that if z is prime in $J[i]$, then it must divides some prime element of $\mathbb{Z}$. So to categorize all prime elements of $J[i]$, we first categorize prime elements in $\mathbb{Z}$ and then find all prime elements in $J[i]$ corresponding to each prime in $\mathbb{Z}$. We categorize prime elements of $\mathbb{Z}$ in three categories; prime elements of form $4n+1$, prime elements of form $4n+3$, and the prime element 2.

Case 1 p is a prime element of form $4n+1$: We have by Theorem 3.8.2, $p = a^2 + b^2 = (a+bi)(a-bi)$. So $d(p) = d((a+bi)(a-bi)) = d(a+bi)d(a-bi) = (a^2+b^2)(a^2+b^2)$. So $p^2 = (a^2+b^2)^2$, or $p = a^2 + b^2 = d(a+bi) = d(a-bi)$. But $d(a+ib) = p$, a prime element in $\mathbb{Z}$ implies $a+ib$ is a prime element in $J[i]$ as if $a+bi$ is not a prime element in $J[i]$ mean $a+bi = z_1 z_2$ with $d(z_1) \neq 1$ and $d(z_2) \neq 1$, which in turn implies $p = d(a+bi) = d(z_1 z_2) = d(z_1)d(z_2)$, showing p is not a prime element in $\mathbb{Z}$ which is not true. Similarly, $a-bi$ is a prime element in $J[i]$. Next, we claim $a+bi$ and $a-bi$ are not associates because if $a+bi$ and $a-bi$ are associates that would imply $a = \pm b \Rightarrow a^2 = b^2 \Rightarrow p = 2a^2 \Rightarrow 2 \mid p$ which is not the case. So $a+bi$ and $a-bi$ are not associates in $J[i]$. Finally, we claim that this decomposition of p into the sum of squares of integers is unique upto signs and the order in which a, b appear. Suppose decomposition is not unique, therefore $p = c^2 + d^2 = (c+di)(c-di)$. But then we know $J[i]$ is a Unique Factorization Domain, so $c+di = u(a+ib)$, or $c+di = u(a-bi)$, where u is the unit element of $J[i]$. Taking values of u equal to $1, -1, i, -i$ one-by-one, one can see either $a = \pm c$ or $a = \pm d$. So decomposition of p into a^2+b^2 is unique upto sign and the order. Thus we concluded, when p is a prime of form $4n+1$, there corresponds exactly two prime elements(unique upto associates) $(a+bi), (a-bi) \in J[i]$, such that $(a+bi) \mid p$ and $(a-bi) \mid p$.

Case 2 p is a prime of form $4n+3$: We claim p is prime in $J[i]$ too. Suppose p is composite in $J[i]$, therefore $p = z_1 z_2$ with $d(z_1) \neq 1$ and $d(z_2) \neq 1$. Let $z_1 = a+bi$. So $p = z_1 z_2 \Rightarrow d(p) = d(z_1 z_2) \Rightarrow p^2 = d(z_1)d(z_2) \Rightarrow p = d(z_1) = d(z_2) \Rightarrow p = a^2 + b^2$. But by Problem 5, p of form $4n+3$ cannot be written as sum of two squares, hence contradiction. So p is a prime element of $J[i]$. Thus we concluded, p is the only prime element in $J[i]$ such that $p \mid p$.

Case 3 when $p = 2$: This case is trivial to check $2 = (1+i)(1-i)$ with $1+i$ as prime element in $J[i]$. Note that $1-i$ is associate of $1+i$. Thus $1+i$ is the only prime in $J[i]$ dividing 2.

We summarize our finding that if z is a prime element in $J[i]$, then either $z = a+bi$ or $z = a-bi$ with $d(z) = p$ where p is a prime of form $4n+1$ in $\mathbb{Z}$; or $z = p$ where p is a prime of form $4n+3$ in $\mathbb{Z}$; or $z = 1+i$. ∎

*9. Determine all positive integers which can be written as a sum of two squares (of integers).

Solution: Clearly, $n = 1 = 1^2 + 0^2$ is expressible as sum of two squares. For $n \neq 1$, we claim that $n = p_1 p_2 \cdots p_l$ is expressible as sum of two squares if and only if every prime factor p_i of form $4k+3$ has even multiplicity. First suppose it is given that $n = p_1 p_2 \cdots p_l$ is expressible as sum of two squares, we need to show that every prime factor p_i of form $4k+3$ has even multiplicity. To prove it by induction, we need to modify our statement to be proved. We assert that for all $n \in \mathbb{N}$, $n \neq 1$, we have either n not expressible as sum of two squares or if it does then its every prime factor of form $4k+3$ has even multiplicity. Note that we have excluded $n = 1$. When $n = 2$, we have $2 = 1^2 + 1^2$ and $2 = 2$, having no prime factor of form $4k+3$. So the result is vacuously valid for $n = 2$. Suppose the statement is valid for $n = m - 1$. We need to show that it is equally valid for $n = m$. Now either m cannot be written as sum of two squares or it can be. If it cannot be, then we have nothing left to prove. So we assume $m = a^2 + b^2$. Let $m = p_1 p_2 \cdots p_l$. Again if m has no prime factor of form $4k+3$, we have nothing to prove. But suppose some prime factor p_{i_0} of m is of form $4k+3$, then we have $p_{i_0} \mid n \Rightarrow p_{i_0} \mid (a^2 + b^2)$. Now we will work in $J[i]$ to conclude that $p_{i_0} \mid (a^2 + b^2) \Rightarrow p_i \mid a$ and $p_i \mid b$. Since p_{i_0} is of form $4k+3$ so p_{i_0} is also a prime element in $J[i]$. But $p_{i_0} \mid a^2 + b^2 \Rightarrow p_{i_0} \mid (a+bi)(a-bi) \Rightarrow p_{i_0} \mid (a+bi)$ or $p_{i_0} \mid (a-bi)$. When $p_{i_0} \mid (a+bi)$, we have $(a+bi) = (c+di)p_{i_0}$ for some $c + di \in J[i]$. But that means $a = cp_{i_0}$ and $b = dp_{i_0}$, or $p_{i_0} \mid a$ and $p_{i_0} \mid b$. Similarly, when $p_{i_0} \mid (a-bi)$, we have $p_{i_0} \mid a$ and $p_{i_0} \mid b$. We return back to work in $\mathbb{Z}$. We have $p_{i_0} \mid a$ and $p_{i_0} \mid b$, therefore $a = p_{i_0} a'$ and $b = p_{i_0} b'$ for some $a', b' \in \mathbb{Z}$. So

$$n = p_{i_0}^2 (a'^2 + b'^2) \tag{1}$$

From (1) we can conclude $n \geq p_{i_0}^2$. So either $n = p_{i_0}^2$ or $n > p_{i_0}^2$. If $n = p^2$, our statement is validated for $n = m$. But if $n > p_{i_0}^2$, we define $n' = a'^2 + b'^2$. Using (1), we have $n' = \frac{n}{p_{i_0}^2}$. But $n > p_{i_0}^2$, so $n' > 1$. Also $p_{i_0}^2 > 1$, so $n' < n$. Invoking inductive hypothesis, we have n' either not expressible as a sum of two squares or if it does then its every prime factor of form $4k+3$ has even multiplicity. But then $n = p_{i_0}^2 n'$ also is either not expressible as a sum of two squares or if it does then its every prime factor of form $4k+3$ has even multiplicity. Thus our assertion is true for $n = m$ too. Thus our assertion is valid in general. From our assertion(or modified statement), we conclude that if n is equal to sum of two squares, then its every prime factor is of form $4k+3$ is of even multiplicity.

Conversely, suppose it is given that $n = p_1 p_2 \cdots p_l$ with every prime factor p_i of form $4k+3$ having even multiplicity, then we need to show n is expressible as sum of two squares. Consider any p_i, prime factor of n. Since p_i is prime, so either it is 2, or is of form $4k+1$, or is of form $4k+3$. When $p_i = 2$, then $p_i = 1^2 + 1^2$. When p_i is of form $4k+1$, then $p_i = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. When p_i is of form $4k+3$, then it is given to be of even multiplicity, therefore

p_i^{2j} for some $j \geq 1$ must be the factor of n. We can treat $p_i^{2j} = (p_i^j)^2 + 0^2$. Thus, we saw n is a product of sum of two squares. Also we observe that $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$, i.e. product of two numbers which are expressible as sum of two squares is again a number which can be expressed as sum of two squares. One can apply this observation over and over again to see product of sum of two squares is again a sum of two squares. Hence n is a product of two squares. Thus n with its every prime factor of form $4k + 1$ having even multiplicity implies n is expressible as sum of two squares.

Thus $n = p_1 p_2 \cdots p_l$ with $n \neq 1$ is expressible as sum of two squares if and only if every prime factor p_i of form $4k + 3$ has even multiplicity. With this result at our disposal, we can determine all integers which can be expressed as sum of two squares. ∎

Problems (Page 158)

1. Find the greatest common divisor of the following polynomials over F, the field of rational numbers:
(a) $x^3 - 6x^2 + x + 4$ and $x^5 - 6x + 1$.
(b) $x^2 + 1$ and $x^6 + x^3 + x + 1$.
Solution:
(a) Using long division method, we have

$$x^5 - 6x + 1 = (x^3 - 6x^2 + x + 4)(x^2 + 6x + 35) + 200x^2 - 65x - 139$$

So $gcd(x^5 - 6x + 1, x^3 - 6x^2 + x + 4) = gcd(x^3 - 6x^2 + x + 4, 200x^2 - 65x - 139)$.
Again we have

$$x^3 - 6x^2 + x + 4 = (200x^2 - 65x - 139)(\frac{x}{200} - \frac{227}{8000}) - \frac{239}{1600}x + \frac{447}{8000}$$

So $gcd(x^3 - 6x^2 + x + 4, 200x^2 - 65x - 139) = gcd\left(200x^2 - 65x - 139, -\frac{239}{1600}x + \frac{447}{8000}\right)$.
Again we have

$$200x^2 - 65x - 139 = \left(-\frac{239}{1600}x + \frac{447}{8000}\right)\left(-\frac{320000}{239}x - \frac{3752000}{57121}\right) - \frac{7730176}{57121}$$

So $gcd\left(200x^2 - 65x - 139, -\frac{239}{1600}x + \frac{447}{8000}\right) = gcd\left(-\frac{239}{1600}x + \frac{447}{8000}, -\frac{7730176}{57121}\right) =$ 1. Hence

$$gcd(x^5 - 6x + 1, x^3 - 6x^2 + x + 4) = 1$$

(b) Using long division method, we have

$$x^6 + x^3 + x + 1 = (x^2 + 1)(x^4 - x^2 + x + 1)$$

So we have $gcd(x^6 + x^3 + x + 1, x^2 + 1) = gcd(x^2 + 1, 0) = x^2 + 1$. So we have

$$gcd(x^6 + x^3 + x + 1, x^2 + 1) = x^2 + 1 \quad \blacksquare$$

2. Prove that
(a) $x^2 + x + 1$ is irreducible over F, the field of integers mod 2.
(b) $x^2 + 1$ is irreducible over the integers mod 7.
(c) $x^3 - 9$ is irreducible over the integers mod 31.
(d) $x^3 - 9$ is reducible over the integers mod 11.
Solution:
(a) We have

$$x^2 + x + 1 \mid_{x=0} = 1 \bmod 2$$
$$x^2 + x + 1 \mid_{x=1} = 1 \bmod 2$$

So $x^2 + x + 1 \neq 0 \quad \forall\, x \in \mathbb{Z}_2$, implying $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

(b) We have

$$\begin{aligned}
x^2+1\mid_{x=0} &= 1 \bmod 7\\
x^2+1\mid_{x=1} &= 2 \bmod 7\\
x^2+1\mid_{x=2} &= 5 \bmod 7\\
x^2+1\mid_{x=3} &= 3 \bmod 7\\
x^2+1\mid_{x=4} &= 3 \bmod 7\\
x^2+1\mid_{x=5} &= 5 \bmod 7\\
x^2+1\mid_{x=6} &= 2 \bmod 7
\end{aligned}$$

So $x^2+1 \neq 0 \quad \forall\, x \in \mathbb{Z}_7$. So x^2+1 is irreducible in $\mathbb{Z}_7[x]$

(c) We have

$$\begin{aligned}
x^3-9\mid_{x=0} &= 22 \bmod 31\\
x^3-9\mid_{x=1} &= 23 \bmod 31\\
x^3-9\mid_{x=2} &= 30 \bmod 31\\
x^3-9\mid_{x=3} &= 18 \bmod 31\\
x^3-9\mid_{x=4} &= 24 \bmod 31\\
x^3-9\mid_{x=5} &= 23 \bmod 31\\
x^3-9\mid_{x=6} &= 21 \bmod 31\\
x^3-9\mid_{x=7} &= 24 \bmod 31\\
x^3-9\mid_{x=8} &= 7 \bmod 31\\
x^3-9\mid_{x=9} &= 7 \bmod 31\\
x^3-9\mid_{x=10} &= 30 \bmod 31\\
x^3-9\mid_{x=11} &= 20 \bmod 31\\
x^3-9\mid_{x=12} &= 14 \bmod 31\\
x^3-9\mid_{x=13} &= 18 \bmod 31\\
x^3-9\mid_{x=14} &= 7 \bmod 31\\
x^3-9\mid_{x=15} &= 18 \bmod 31\\
x^3-9\mid_{x=16} &= 26 \bmod 31\\
x^3-9\mid_{x=17} &= 6 \bmod 31\\
x^3-9\mid_{x=18} &= 26 \bmod 31\\
x^3-9\mid_{x=19} &= 30 \bmod 31\\
x^3-9\mid_{x=20} &= 24 \bmod 31\\
x^3-9\mid_{x=21} &= 14 \bmod 31\\
x^3-9\mid_{x=22} &= 6 \bmod 31
\end{aligned}$$

$$x^3 - 9 \mid_{x=23} = 6 \bmod 31$$
$$x^3 - 9 \mid_{x=24} = 20 \bmod 31$$
$$x^3 - 9 \mid_{x=25} = 23 \bmod 31$$
$$x^3 - 9 \mid_{x=26} = 21 \bmod 31$$
$$x^3 - 9 \mid_{x=27} = 20 \bmod 31$$
$$x^3 - 9 \mid_{x=28} = 26 \bmod 31$$
$$x^3 - 9 \mid_{x=29} = 14 \bmod 31$$
$$x^3 - 9 \mid_{x=30} = 21 \bmod 31$$

So $x^3 - 9 \neq 0 \quad \forall\, x \in \mathbb{Z}_{31}$. So $x^3 - 9$ is irreducible in $\mathbb{Z}_{31}[x]$

(d) We have

$$x^3 - 9 \mid_{x=0} = 1 \bmod 11$$
$$x^3 - 9 \mid_{x=1} = 3 \bmod 11$$
$$x^3 - 9 \mid_{x=2} = 10 \bmod 11$$
$$x^3 - 9 \mid_{x=3} = 7 \bmod 11$$
$$x^3 - 9 \mid_{x=4} = 0 \bmod 11$$
$$x^3 - 9 \mid_{x=5} = 5 \bmod 11$$
$$x^3 - 9 \mid_{x=6} = 9 \bmod 11$$
$$x^3 - 9 \mid_{x=7} = 4 \bmod 11$$
$$x^3 - 9 \mid_{x=8} = 8 \bmod 11$$
$$x^3 - 9 \mid_{x=9} = 5 \bmod 11$$
$$x^3 - 9 \mid_{x=10} = 1 \bmod 11$$

So $x^3 - 9 = 0$ for $x = 4$. Therefore $x - 4$, or $x + 7$ is a factor. We can see by long division $x^3 - 9 = (x+7)(x^2 + 4x + 5)$. So $x^3 - 9$ is reducible in $\mathbb{Z}_{11}[x]$. ∎

3. Let F, K be two fields $F \subset K$ and suppose $f(x), g(x) \in F[x]$ are relatively prime in $F[x]$. Prove that they are relatively prime in $K[x]$.
Solution: First we can easily see that if 1 is the multiplicative identity of F, then it is also the multiplicative identity of K too. Now since $f(x), g(x)$ are relatively prime in $F[x]$, so $1 = \lambda(x)f(x) + \mu(x)g(x)$, for some $\lambda(x), \mu(x) \in F[x]$. But since $F \subset K$, therefore $1, \lambda(x), \mu(x), f(x), g(x)$ are also elements of $K[x]$. So the relation $1 = \lambda(x)f(x) + \mu(x)g(x)$ is equally valid in $K[x]$. But that would mean $f(x), g(x)$ as elements of $K[x]$ are relatively prime in $K[x]$. Hence the result. ∎

4. (a) Prove that x^2+1 is irreducible over the field F of integers mod 11 and prove directly that $F[x]/(x^2+1)$ is a field having 121 elements.
(b) Prove that x^2+x+4 is irreducible over F, the field of integers mod 11 and prove directly that $F[x]/(x^2+x+4)$ is a field having 121 elements.
*(c) Prove that the fields of part (a) and (b) are isomorphic.
Solution:
(a) We have

$$\begin{aligned}
x^2+1\mid_{x=0} &= 1 \bmod 11\\
x^2+1\mid_{x=1} &= 2 \bmod 11\\
x^2+1\mid_{x=2} &= 5 \bmod 11\\
x^2+1\mid_{x=3} &= 10 \bmod 11\\
x^2+1\mid_{x=4} &= 6 \bmod 11\\
x^2+1\mid_{x=5} &= 4 \bmod 11\\
x^2+1\mid_{x=6} &= 4 \bmod 11\\
x^2+1\mid_{x=7} &= 6 \bmod 11\\
x^2+1\mid_{x=8} &= 10 \bmod 11\\
x^2+1\mid_{x=9} &= 5 \bmod 11\\
x^2+1\mid_{x=10} &= 2 \bmod 11
\end{aligned}$$

So $x^2+1\neq 0 \quad \forall\, x\in F$. So x^2+1 is irreducible over $F[x]$.

Now consider $F[x]/\langle x^2+1\rangle$. Since $\langle x^2+1\rangle$ is an ideal of $F[x]$, so $F[x]/\langle x^2+1\rangle$ is a ring. Also $F[x]/\langle x^2+1\rangle = \{\langle x^2+1\rangle + ax+b \mid a,b\in F\}$. Since F has 11 elements, so $F[x]/\langle x^2+1\rangle$ has $11\times 11 = 121$ elements. F being commutative implies $F[x]/\langle x^2+1\rangle$ is also commutative. Next we will prove $F[x]/\langle x^2+1\rangle$ to be an integral domain, which would, in turn will prove $F[x]/\langle x^2+1\rangle$ to be a field as every finite integral domain is a field. Suppose $(\langle x^2+1\rangle + ax + b)(\langle x^2+1\rangle + cx+d) = \langle x^2+1\rangle$, with $(\langle x^2+1\rangle + ax+b) \neq \langle x^2+1\rangle$. But $(\langle x^2+1\rangle + ax+b)(\langle x^2+1\rangle + cx+d) = \langle x^2+1\rangle$ implies

$$\begin{aligned}
&\langle x^2+1\rangle + (ax+b)(cx+d) = \langle x^2+1\rangle\\
\Rightarrow\ &\langle x^2+1\rangle + acx^2 + (ad+bc)x + bd = \langle x^2+1\rangle\\
\Rightarrow\ &\langle x^2+1\rangle + ac(x^2+1) + (ad+bc)x + (bd-ac) = \langle x^2+1\rangle\\
\Rightarrow\ &\langle x^2+1\rangle + (ad+bc)x + (bd-ac) = \langle x^2+1\rangle\\
\Rightarrow\ &(ad+bc)x + (bd-ac) \in \langle x^2+1\rangle\\
\Rightarrow\ &ad+bc = bd-ac = 0 \bmod 11 \qquad (1)
\end{aligned}$$

$(\langle x^2+1\rangle + ax+b) \neq \langle x^2+1\rangle$ implies $a=b\neq 0 \bmod 11$ simultaneously. Suppose $a=0 \bmod 11$, therefore $b\neq 0 \bmod 11$. In this case, (1) reduces to

$$\begin{aligned}
bc &= 0 \bmod 11\\
bd &= 0 \bmod 11
\end{aligned} \qquad (2)$$

But since $b \neq 0 \mod 11$ and F being a field, so (2) implies $c = d = 0 \mod 11$. Similarly, if $b = 0 \mod 11$, then also $c = d = 0 \mod 11$. Next if both $a, b \neq 0 \mod 11$, then (1) reduces to

$$\begin{aligned} (a^2 + b^2)c &= 0 \mod 11 \\ (a^2 + b^2)d &= 0 \mod 11 \end{aligned} \tag{3}$$

Let $11 = p$. Suppose, if possible $a^2 + b^2 = 0 \mod p$. So $a^2 + b^2 = kp$ for some positive integer k. Note that p is a prime of form $4n + 3$. So using Problem 9 (page 152 of the book) we have p^i with i a positive odd integer as a factor of k. Thus at least $p \,|\, k$. So at least $p^2 \,|\, a^2 + b^2$. Working in $J[i]$, we have $a^2 + b^2 = (a + bi)(a - bi)$. So $p^2 \,|\, (a + bi)(a - bi)$, which gives three possibilities, 1) $p \,|\, (a + bi)$; 2) $p^2 \,|\, (a + bi)$; 3) $p^2 \,|\, (a - bi)$. All three possibilities, imply $p \,|\, a$ and $p \,|\, b$ (Why). So $a = b = 0 \mod 11$. Thus $a^2 + b^2 = 0 \mod 11$ implies $a = b = 0 \mod 11$. So when $a, b \in F - \{0\}$, we have $a^2 + b^2 \neq 0 \mod 11$. So $c = d = 0 \mod 11$. Thus we see $(\langle x^2 + 1\rangle + ax + b)(\langle x^2 + 1\rangle + cx + d) = \langle x^2 + 1\rangle$, with $(\langle x^2 + 1\rangle + ax + b) \neq \langle x^2 + 1\rangle$ implies $\langle x^2 + 1\rangle + cx + d = \langle x^2 + 1\rangle$. Hence $F[x]/\langle x^2 + 1\rangle$ is an integral domain. Ans so, being finite, it is a field.

(b) We have

$$\begin{aligned} x^2 + x + 4 \,|_{x=0} &= 4 \mod 11 \\ x^2 + x + 4 \,|_{x=1} &= 6 \mod 11 \\ x^2 + x + 4 \,|_{x=2} &= 10 \mod 11 \\ x^2 + x + 4 \,|_{x=3} &= 5 \mod 11 \\ x^2 + x + 4 \,|_{x=4} &= 2 \mod 11 \\ x^2 + x + 4 \,|_{x=5} &= 1 \mod 11 \\ x^2 + x + 4 \,|_{x=6} &= 2 \mod 11 \\ x^2 + x + 4 \,|_{x=7} &= 5 \mod 11 \\ x^2 + x + 4 \,|_{x=8} &= 10 \mod 11 \\ x^2 + x + 4 \,|_{x=9} &= 6 \mod 11 \\ x^2 + x + 4 \,|_{x=10} &= 4 \mod 11 \end{aligned}$$

So $x^2 + x + 4 \neq 0 \quad \forall\, x \in F$. So $x^2 + x + 4$ is irreducible over $F[x]$.

Again as we see in part (a), $F[x]/\langle x^2 + x + 4\rangle$ is a commutative ring with 121 elements. To show $F[x]/\langle x^2 + x + 4\rangle$ a field we will first prove it to be an integral domain. Suppose $(\langle x^2 + x + 4\rangle + ax + b)(\langle x^2 + x + 4\rangle + cx + d) = \langle x^2 + x + 4\rangle$ with $\langle x^2 + x + 4\rangle + ax + b \neq \langle x^2 + x + 4\rangle$. So we have

$$\begin{aligned} &\langle x^2 + x + 4\rangle + (ax + b)(cx + d) = \langle x^2 + x + 4\rangle \\ \Rightarrow\ &\langle x^2 + x + 4\rangle + acx^2 + (ad + bc)x + bd = \langle x^2 + x + 4\rangle \end{aligned}$$

$$\Rightarrow \langle x^2+x+4\rangle + ac(x^2+x+4) + (ad+bc-ac)x + (bd-4ac) = \langle x^2+x+4\rangle$$
$$\Rightarrow (ad+bc-ac)x + (bd-4ac) \in \langle x^2+x+4\rangle$$
$$\Rightarrow ad+bc-ac = bd-4ac = 0 \bmod 11 \tag{1}$$

If $a = 0 \bmod 11$, then $b \neq 0 \bmod 11$ as $\langle x^2+x+4\rangle + ax + b \neq \langle x^2+x+4\rangle$. But then (1) reduces to

$$\begin{aligned} bc &= 0 \bmod 11 \\ bd &= 0 \bmod 11 \end{aligned} \tag{2}$$

Since $b \neq 0 \bmod 11$, therefore $c = d = 0 \bmod 11$. Similarly if $b = 0 \bmod 11$, we have $a \neq 0 \bmod 11$, and (1) reduces to

$$\begin{aligned} a(d-c) &= 0 \bmod 11 \\ -4ac &= 0 \bmod 11 \end{aligned} \tag{3}$$

But $a \neq 0 \bmod 11$, so $c = 0 \bmod 11$, which in turn forces $d = 0 \bmod 11$. Thus $c = d = 0$ in this case too. Finally suppose both $a, b \neq 0 \bmod 11$, then (1) reduces to

$$\begin{aligned} (4a^2+b^2-ba)c &= 0 \bmod 11 \\ (4a^2+b^2-ba)d &= 0 \bmod 11 \end{aligned} \tag{4}$$

Now $4a^2+b^2-ab = 4a^2+b^2+10ab = 25a^2+b^2+10ab-21a^2 = (5a+b)^2+a^2$ (We are working in modulo 11). As in previous part if $4a^2+b^2-ab = (5a+b)^2+a^2 = 0 \bmod 11$, then $11 \mid a$ and $11 \mid (5a+b)$. Thus $4a^2+b^2-ab = 0 \bmod 11$ implies $a = b = 0 \bmod 11$. In other words if $a, b \neq 0 \bmod 11$, then $4a^2+b^2-ab \neq 0 \bmod 11$. But then F being a field makes (4) implying $c = d = 0 \bmod 11$. Thus $(\langle x^2+x+4\rangle + ax + b)(\langle x^2+x+4\rangle + cx + d) = \langle x^2+x+4\rangle$ with $\langle x^2+x+4\rangle + ax + b \neq \langle x^2+x+4\rangle$ implies $\langle x^2+x+4\rangle + cx + d = \langle x^2+x+4\rangle$. So $F[x]/\langle x^2+x+4\rangle$ is an integral domain, and hence is a field.

(c) Define $\phi : F[x]/\langle x^2+1\rangle \longrightarrow F[x]/\langle x^2+x+4\rangle$ such that $\phi(\langle x^2+1\rangle + ax+b) = \langle x^2+x+4\rangle + ax + (b+6a)$. We claim ϕ is an one-to-one and onto ring homomorphism. Firstly, one can easily see that mapping is well-defined. Next we prove mapping is a ring homomorphism. We have

$$\begin{aligned} &\phi((\langle x^2+1\rangle + ax + b) + (\langle x^2+1\rangle + a'x + b')) \\ &= \phi((\langle x^2+1\rangle + (a+a')x + (b+b')) \\ &= \langle x^2+x+4\rangle + (a+a')x + (b+b') + 6(a+a') \\ &= \langle x^2+x+4\rangle + (ax+b+6a) + (a'x+b'+6a') \\ &= (\langle x^2+x+4\rangle + (ax+b+6a)) + (\langle x^2+x+4\rangle + (a'x+b'+6a')) \\ &= \phi(\langle x^2+1\rangle + ax + b) + \phi(\langle x^2+1\rangle + a'x + b') \end{aligned}$$

Also we have

$$\begin{aligned} &\phi((\langle x^2+1\rangle + ax + b)(\langle x^2+1\rangle + a'x + b')) \\ &= \phi(\langle x^2+1\rangle + aa'x^2 + (ab'+ba')x + bb') \end{aligned}$$

$$
\begin{aligned}
&= \phi(\langle x^2+1\rangle + aa'(x^2+1) + (ab'+ba')x + (bb'-aa')) \\
&= \phi(\langle x^2+1\rangle + (ab'+ba')x + (bb'-aa')) \\
&= \langle x^2+x+4\rangle + (ab'+ba')x + (bb'-aa') + 6(ab'+ba') \\
&= \langle x^2+x+4\rangle + (ab'+ba')x + (bb'+6ab'+6ba'-aa') \qquad (1)
\end{aligned}
$$

Also

$$
\begin{aligned}
&\phi(\langle x^2+1\rangle + ax + b)\phi(\langle x^2+1\rangle + a'x + b') \\
&= (\langle x^2+x+4\rangle + ax + (b+6a))(\langle x^2+x+4\rangle + a'x + (b'+6a')) \\
&= \langle x^2+x+4\rangle + aa'x^2 + (a(b'+6a') + (b+6a)a')x + \\
&\quad (b+6a)(b'+6a') \\
&= \langle x^2+x+4\rangle + aa'(x^2+x+4) + (a(b'+6a') + (b+6a)a' - aa')x + \\
&\quad (b+6a)(b'+6a') - 4aa' \\
&= \langle x^2+x+4\rangle + (ab'+6aa'+ba'+6aa'-aa')x + \\
&\quad (bb'+6ab'+6ba'+36aa'-4aa') \\
&= \langle x^2+x+4\rangle + (ab'+ba')x + (bb'+6ab'+6ba'-aa') \qquad (2)
\end{aligned}
$$

So from (1) and (2) we have $\phi((\langle x^2+1\rangle + ax + b)(\langle x^2+1\rangle + a'x + b')) = \phi(\langle x^2+1\rangle + ax + b)\phi(\langle x^2+1\rangle + a'x + b')$ Hence ϕ is a ring homomorphism. Next we prove mapping ϕ is one-to-one mapping. We have

$$
\begin{aligned}
&\phi(\langle x^2+1\rangle + ax + b) = \phi(\langle x^2+1\rangle + a'x + b') \\
&\Rightarrow \langle x^2+x+4\rangle + ax + b + 6a = \langle x^2+x+4\rangle + a'x + b' + 6a' \\
&\Rightarrow (a-a')x + (b+6a-b'-6a') \in \langle x^2+x+4\rangle \\
&\Rightarrow (a-a')x + (b+6a-b'-6a') = 0 \bmod 11 \\
&\Rightarrow (a-a') = (b+6a-b'-6a') = 0 \bmod 11 \\
&\Rightarrow a = a' \bmod 11 \text{ and } b = b' \bmod 11 \\
&\Rightarrow \langle x^2+1\rangle + ax + b = \langle x^2+1\rangle + a'x + b'
\end{aligned}
$$

Hence ϕ is an one-to-one mapping. Also if some $\tilde{y} = \langle x^2+x+4\rangle + ax + b \in F[x]/\langle x^2+x+4\rangle$, then $\tilde{x} = \langle x^2+1\rangle + ax + (b+5a) \in F[x]/\langle x^2+1\rangle$ is the inverse-image of $\tilde{y}$. Thus inverse-image of every $\tilde{y} \in F[x]/\langle x^2+x+4\rangle$ exists. So ϕ is onto too. Thus we have mapping ϕ an one-to-one and onto ring homomorphism. So

$$
\frac{F[x]}{\langle x^2+1\rangle} \approx \frac{F[x]}{\langle x^2+x+4\rangle} \qquad \blacksquare
$$

5. Let F be the field of real numbers. Prove that $F[x]/(x^2+1)$ is a field isomorphic to the field of complex numbers.

Solution: We have x^2+1 a irreducible element of $F[x]$, where F is the field of real numbers. Therefore $\langle x^2+1\rangle$ is a maximal ideal of $F[x]$. So $F[x]/\langle x^2+1\rangle$

is field. Moreover $F[x]/\langle x^2+1\rangle = \{\langle x^2+1\rangle + ax + b \mid a, b \in F\}$. To exhibit an one-to-one and onto homomorphism, we define mapping $\phi : F[x]/\langle x^2+1\rangle \longrightarrow \mathbb{C}$ such that $\phi(\langle x^2+1\rangle + ax + b) = b + ia$, where $\mathbb{C}$ is the field of complex numbers. Clearly mapping ϕ is well-defined. Also mapping is one-to-one and onto too. Next

$$\begin{aligned}
&\phi((\langle x^2+1\rangle + ax + b) + (\langle x^2+1\rangle + a'x + b')) \\
&\qquad = \phi(\langle x^2+1\rangle + (a+a')x + (b+b')) \\
&\qquad = b + b' + i(a+a') \\
&\qquad = (b+ia) + (b'+ia') \\
&\qquad = \phi(\langle x^2+1\rangle + ax + b) + \phi(\langle x^2+1\rangle + a'x + b')
\end{aligned}$$

and

$$\begin{aligned}
&\phi((\langle x^2+1\rangle + ax + b)(\langle x^2+1\rangle + a'x + b')) \\
&\qquad = \phi(\langle +x^2+1\rangle + (ax+b)(a'x+b')) \\
&\qquad = \phi(\langle x^2+1\rangle + aa'x^2 + (ab'+ba')x + bb') \\
&\qquad = \phi(\langle x^2+1\rangle + aa'(x^2+1) + (ab'+ba')x + bb' - aa') \\
&\qquad = \phi(\langle x^2+1\rangle + (ab'+ba')x + (bb'-aa')) \\
&\qquad = (bb'-aa') + i(ab'+ba') \\
&\qquad = (a+ib)(a'+ib') \\
&\qquad = \phi(\langle x^2+1\rangle + ax + b)\phi(\langle x^2+1\rangle + a'x + b')
\end{aligned}$$

Thus mapping ϕ is a ring homomorphism too. Hence $F[x]/\langle x^2+1\rangle \approx \mathbb{C}$. ∎

*6. Define the *derivative* $f'(x)$ of the polynomial

$$\begin{aligned}
f(x) &= a_0 + a_1x + \cdots + a_nx^n \\
\text{as } f'(x) &= a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}.
\end{aligned}$$

Prove that if $f(x) \in F[x]$, where F is the field of rational numbers, then $f(x)$ is divisible by the square of a polynomial if and only if $f(x)$ and $f'(x)$ have a greatest common divisor $d(x)$ of positive degree.
Solution: We first assert two results which we are going to use in the proof.

1. If $f(x) = g(x)h(x)$, then $f'(x) = g'(x)h(x) + g(x)h'(x)$;
2. If $f(x) = (g(x))^n$ for some $n \in \mathbb{N}$, then $f'(x) = n(g(x))^{n-1}g'(x)$.

We left the proof of above results as an exercise for the reader.

Now first suppose, $f(x)$ is divisible by the square of a polynomial, say $h(x)$ with $deg(h(x)) \geq 1$. Therefore, $f(x) = (h(x))^2g(x)$. So $f'(x) = (2h(x)h'(x))g(x) +$

$(h(x))^2 g'(x) = h(x)(2h'(x)g(x) + h(x)g'(x))$. But that means $h(x) \mid f(x)$ and $h(x) \mid f'(x)$. So $h(x) \mid gcd(f(x), f'(x))$, or $gcd(f(x), f'(x)) = h(x)q(x)$ for some $q(x) \in F[x]$. Also $deg(h(x)q(x)) = deg(h(x)) + deg(q(x)) \geq 1$ as $deg(h(x)) \geq 1$. Thus greatest common divisor of $f(x)$ and $f'(x)$ is of positive degree.

Conversely, suppose some $gcd(f(x), f'(x)) = h(x)$ with $deg(h(x)) \geq 1$. So $f(x) = h(x)g(x)$ for some $g(x) \in F[x]$. Also $f'(x) = h'(x)g(x)+h(x)g'(x)$, therefore $h(x) \mid h'(x)g(x)+h(x)g'(x) \Rightarrow h(x) \mid h'(x)g(x)$. But $deg(h'(x)) < deg(h(x))$, so some irreducible factor $p(x)$ of $h(x)$ does not divide $h'(x)$, because if every irreducible factor of $h(x)$ divides $h'(x)$ would imply $deg(h'(x)) \geq deg(h(x))$ which is not the case. So some $p(x) \mid h(x)$ and $p(x) \nmid h'(x)$. But $h(x) \mid h'(x)g(x)$, therefore $p(x) \mid h'(x)g(x)$. So $p(x) \mid g(x)$ as $p(x) \nmid h'(x)$. But $p(x) \mid h(x)$ and $p(x) \mid g(x)$ implies $(p(x))^2 \mid h(x)g(x)$. Thus $(p(x))^2 \mid f(x)$. Also $p(x)$ being irreducible implies $deg(p(x)) \geq 1$. Thus we concluded, some $f(x) \in F[x]$ is divisible by the square of a polynomial with positive degree if and only if greatest common divisor of $f(x)$ and $f'(x)$ is of positive degree. ∎

7. If $f(x)$ is in $F[x]$, where F is the field of integers mod p, p a prime, and $f(x)$ irreducible over F of degree n prove that $F[x]/(f(x))$ is a field with p^n elements.
Solution: Since $f(x)$ is irreducible, therefore by Lemma 3.9.6 $\langle f(x) \rangle$ is a maximal ideal of $F[x]$. Then using Theorem 3.5.1, we have $F[x]/\langle f(x) \rangle$ is a field. Also every element of $F[x]/\langle f(x) \rangle$ can be uniquely represented as $\langle f(x) \rangle + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in F$, so the field $F[x]/\langle f(x) \rangle$ has p^n elements. Hence the result. ∎

Problems (Page 161)

1. Let D be a Euclidean ring, F its field of quotients. Prove the Gauss Lemma for polynomials with coefficients in D factored as products of polynomials with coefficients in F.
Solution: Suppose some $f(x) \in D[x]$. Therefore $f(x) \in F[x]$ too. Also suppose $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$. But then using Problem 11 (Page 166 of the book), we have $g(x) = \frac{g'(x)}{\lambda}$ for some $g'(x) \in D[x]$ and $\lambda \in D$. Also if content of $g'(x)$ is d_1, then $g'(x) = d_1 g''x$, where $g''(x) \in D[x]$ is a primitive. So $g(x) = \frac{d_1}{\lambda} g''(x)$. Similarly, $h(x) = \frac{d_2}{\mu} h''(x)$ where $h''(x)$ is primitive in $D[x]$ and $d_2, \mu \in D$. So we have

$$f(x) = \frac{d_1 d_2}{\lambda \mu} g''(x) h''(x)$$

Also content of $g''(x), h''(x)$ equal to 1 implies content of $g''(x)h''(x)$ is also 1. Now $f(x), g''(x)h''(x) \in D[x]$ with content 1, therefore $\frac{d_1 d_2}{\lambda \mu} = 1$. So we have $f(x) = g''(x)h''(x)$ showing $f(x)$ is reducible in $D[x]$ too. Thus if $f(x) \in D[x]$ is reducible in $F[x]$, then $f(x)$ is also reducible in $D[x]$. Hence the result. ∎

2. If p is a prime number, prove that the polynomial $x^n - p$ is irreducible over the rationals.
Solution: Let $f(x) = x^n - p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. So $a_n = 1$, $a_0 = -p$ and rest $a_i = 0$. We apply Eisenstein criterion. We have $f(x) \in \mathbb{Z}[x]$, and $p \mid a_0, p \mid a_1, \cdots, p \mid a_{n-1}$, and $p \nmid a_n$. Also $p^2 \nmid a_0$. Therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$. Hence the result. ∎

3. Prove that the polynomial $1 + x + \cdots + x^{p-1}$, where p is a prime number, is irreducible over the field of rational numbers. (*Hint:* Consider the polynomial $1 + (x+1) + (x+1)^2 + \cdots + (x+1)^{p-1}$, and use the Eisenstein criterion.)
Solution: Let $f(x) = 1 + x + \cdots + x^{p-1}$. Now $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. We have $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$, therefore $f(x) = \frac{x^p - 1}{x - 1}$ (undefined notation?). So we have

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{1}{x}({}^nC_1 x + {}^nC_2 x^2 + \cdots + {}^nC_p x^p) \\ &= {}^nC_1 + {}^nC_2 x + \cdots + {}^nC_{p-1} x^{p-2} + {}^nC_p x^{p-1} \end{aligned}$$

Now we have ${}^nC_r r! = p(p-1)\cdots(p-r+1)$ for $r > 0$. Also $p \nmid r!$ for $r < p$ as p is prime. So if $1 \le r \le p-1$, we have with $p \nmid r!$ and $p \mid p(p-1)\cdots(p-r+1)$, implying $p \mid {}^nC_r$. Thus p divides all coefficient of $f(x+1)$ except for the coefficient of x^{p-1} which is 1. Also $p^2 \nmid p$, the constant coefficient of $f(x+1)$. So by Eisenstein criterion $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. And hence $f(x)$ is irreducible

in $\mathbb{Q}$. ∎

4. If m and n are relatively prime integers and if

$$\left(x - \frac{m}{n}\right) \mid (a_0 + a_1 x + \cdots + a_r x^r),$$

where the a's are integers, prove that $m \mid a_0$ and $n \mid a_r$.
Solution: Let

$$a_0 + a_1 x + \cdots + a_r x^r = (x - m/n)(b_0 + b_1 x + \cdots + b_{r-1} x^{r-1}) \qquad (1)$$

Comparing coefficients of $x^0, x^1, x^2, \cdots$ and expressing in terms of a_i, we have

$$\begin{aligned}
b_0 &= -\frac{n}{m} a_0 \\
b_1 &= -\frac{n}{m}\left(a_1 + \frac{n}{m} a_0\right) \\
b_2 &= -\frac{n}{m}\left(a_2 + \frac{n}{m}\left(a_1 + \frac{n}{m} a_0\right)\right) \\
&\vdots \\
b_{r-1} &= -\frac{n}{m}\left(a_{r-1} + \frac{n}{m}\left(a_{r-2} + \cdots\right)\right)
\end{aligned}$$

But we have $b_{r-1} = a_r$. Therefore

$$a_r = -\frac{n}{m}\left(a_{r-1} + \frac{n}{m}\left(a_{r-2} + \cdots\right)\right)$$

Also $gcd(m, n) = 1$, so $n \mid a_r$. Again comparing coefficients of $x^r, x^{r-1}, \cdots$ in (1) and expressing in terms of a_i, we have

$$\begin{aligned}
b_{r-1} &= a_r \\
b_{r-2} &= a_{r-1} + \frac{m}{n} a_r \\
b_{r-3} &= a_{r-2} + \frac{m}{n}\left(a_{r-1} + \frac{m}{n} a_r\right) \\
&\vdots \\
b_0 &= a_1 + \frac{m}{n}\left(a_2 + \frac{m}{n}(\cdots)\right)
\end{aligned}$$

But we have $b_0 = -\frac{n}{m} a_0$. Therefore

$$-\frac{n}{m} a_0 = a_1 + \frac{m}{n}\left(a_2 + \frac{m}{n}(\cdots)\right)$$

or

$$a_0 = -\frac{m}{n}\left(a_1 + \frac{m}{n}\left(a_2 + \frac{m}{n}(\cdots)\right)\right)$$

Since $gcd(m, n) = 1$, therefore $m \mid a_0$. Hence the result. ∎

5. If a is rational and $x - a$ divides an integer monic polynomial, prove that a must be an integer.

Solution: Suppose a is a rational number, therefore we can assume $a = \frac{p}{q}$ with $gcd(p, q) = 1$. Let $f(x) \in \mathbb{Z}[x]$ be some monic polynomial. Let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ for some $m \in \mathbb{N}$. We are give $(x - p/q) \mid f(x)$. So $f(x) = (x - p/q)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. Since $g(x) \in \mathbb{Q}[x]$, therefore $g(x) = \frac{d}{\lambda}g'(x)$, where $g'(x)$ is primitive in $\mathbb{Z}[x]$ and $d, \lambda \in \mathbb{Z}$. So we have

$$\begin{aligned} f(x) &= \frac{d}{\lambda}\left(x - \frac{p}{q}\right)g'(x) \\ &= \frac{d}{\lambda q}(qx - p)g'(x) \end{aligned} \tag{1}$$

Now since $gcd(p, q) = 1$, therefore $qx - p$ is a primitive in $\mathbb{Z}[x]$. Also $g'(x)$ is primitive in $\mathbb{Z}[x]$, so $(qx - p)g'(x)$ is primitive in $\mathbb{Z}[x]$. Also $f(x)$ being monic, therefore is primitive in $\mathbb{Z}[x]$. So from equation (1) we have $\frac{d}{\lambda q} = 1$. So we have

$$f(x) = (qx - p)g'(x) \tag{2}$$

Since $g'(x) \in \mathbb{Z}[x]$, therefore let $g'(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1}$ with all $b_i \in \mathbb{Z}$. Comparing coefficient of x^m in equation (2), we have $1 = qb_{m-1}$. But that means q is a unit in $\mathbb{Z}$, or $q = \pm 1$, showing p/q is an integer. Hence $a = p/q$ is an integer. ∎

Problems (Page 166)

1. Prove that $R[x]$ is a commutative ring with unit element whenever R is.
Solution: We are given R is a commutative ring with unity element. Suppose some $f(x) = a_m x^m + \cdots + a_0$ and $g(x) = b_n x^n + \cdots + b_0$ are elements in $R[x]$. Let $f(x)g(x) = c_{m+n}x^{m+n} + \cdots + c_0$ and $g(x)f(x) = d_{m+n}x^{m+n} + \cdots + d_0$. So we have for $0 \leqslant i \leqslant m+n$

$$\begin{aligned} c_i &= \sum_{j=0}^{i} a_j b_{i-j} \\ &= \sum_{j=0}^{i} b_{i-j} a_j \text{ as } R \text{ is commutative} \\ &= \sum_{k=i}^{0} b_k a_{i-k} \\ &= \sum_{k=0}^{i} b_k a_{i-k} \\ &= d_i \end{aligned}$$

So $f(x)g(x) = g(x)f(x)$, implying $R[x]$ is commutative too. Also if 1 is the multiplicative identity of R, we have $f(x)1 = 1f(x) = f(x)$. Thus multiplicative identity of R is also the multiplicative identity of $R[x]$. And hence $R[x]$ too is a commutative ring and has unity element. ∎

2. Prove that $R[x_1, \ldots, x_n] = R[x_{i_1}, \ldots, x_{i_n}]$, where $(i_1, \ldots, i_n)$ is a permutation of $(1, 2, \ldots, n)$.
Solution: Let some $f(x_1, \cdots, x_n) \in R[x_1, \ldots, x_n]$. Therefore

$$f(x_1, \cdots, x_n) = \sum a_{j_1, j_2, \cdots, j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}, \text{ where } a_{j_1, j_2, \cdots, j_n} \in R$$

Also $x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} = x_{i_1}^{j_{i_1}} x_{i_2}^{j_{i_2}} \cdots x_{i_n}^{j_{i_n}}$, so we have

$$\begin{aligned} f(x_1, \cdots, x_n) &= \sum a_{j_1, j_2, \cdots, j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \\ &= \sum a_{j_1, j_2, \cdots, j_n} x_{i_1}^{j_{i_1}} x_{i_2}^{j_{i_2}} \cdots x_{i_n}^{j_{i_n}} \in R[x_{i_1}, \ldots, x_{i_n}] \end{aligned}$$

So $R[x_1, \ldots, x_n] \subset R[x_{i_1}, \ldots, x_{i_n}]$. Similarly, we can show $R[x_{i_1}, \ldots, x_{i_n}] \subset R[x_1, \ldots, x_n]$. Hence $R[x_1, \ldots, x_n] = R[x_{i_1}, \ldots, x_{i_n}]$ ∎

3. If R is an integral domain, prove that for $f(x)$, $g(x)$ in $R[x]$, $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$.
Solution: Let $f(x) = a_0 + a_1 x + \cdots$, with $deg(f(x)) = m$ for some $m \in \mathbb{N}$.

So we have $a_m \neq 0$ and $a_i = 0 \quad \forall\ i > m$. Also let $g(x) = b_0 + b_1x + \cdots$, with $deg(g(x)) = n$ for some $n \in \mathbb{N}$. So $b_n \neq 0$ and $b_i = 0 \quad \forall\ i > n$. Let $h(x) = f(x)g(x) = c_0 + c_1x + \cdots$. We have

$$\begin{aligned} c_{m+n} &= \sum_{i=0}^{m+n} a_i b_{m+n-i} \\ &= (a_0b_{m+n} + \cdots + a_{m-1}b_{n+1}) + a_mb_n + (a_{m+1}b_{n-1} + \cdots + a_{m+n}b_0) \\ &= 0 + a_mb_n + 0 \\ &\neq 0 \text{ as } R \text{ is an integral domain and } a_m \neq 0 \text{ and } b_n \neq 0 \end{aligned}$$

Also for some integer $k \geqslant 1$ we have

$$\begin{aligned} c_{m+n+k} = & \sum_{i=0}^{m+n+k} a_i b_{m+n-i} \\ &= (a_0b_{m+n} + \cdots + a_{m-1}b_{n+k+1} + a_mb_{n+k}) + \\ &\quad (a_{m+1}b_{n+k-1} + \cdots + a_{m+n+k}b_0) \\ &= 0 + 0 = 0 \end{aligned}$$

So $deg(h(x)) = m + n$, or $deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$. Hence the result. ∎

4. If R is an integral domain with unit element, prove that any unit in $R[x]$ must already be a unit in R.
Solution: Suppose $f(x)$ be some unit in $R[x]$, therefore there exists some $g(x) \in R[x]$ such that $f(x)g(x) = 1$, where 1 is the multiplicative identity of R. Now we have $deg(1) = deg(f(x)g(x)) = deg(f(x)) + deg(g(x))$. But $deg(1) = 0$, therefore $deg(f(x)) + deg(g(x)) = 0$. Also $deg(f(x)), deg(g(x)) \geq 0$, therefore we have only possibility that $deg(f(x)) = deg(g(x)) = 0$. But that means $f(x) = a_0$ and $g(x) = b_0$ for some $a_0, b_0 \in R$. So $f(x)g(x) = 1 \Rightarrow a_0b_0 = 1$. But that means a_0 is a unit in R. Thus any unit of $R[x]$ is a unit of R too. Hence the result. ∎

5. Let R be a commutative ring with no nonzero *nilpotent* elements (that is, a^n implies $a = 0$). If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ in $R[x]$ is a zero-divisor, prove that there is an element $b \neq 0$ in R such that $ba_0 = ba_1 = \cdots = ba_m = 0$.
Solution: Since $f(x)$ is the zero-divisor in $R[x]$, therefore there exist $g(x) \in R[x]$ with $g(x) \neq 0$ such that $f(x)g(x) = 0$. Let $deg(g(x)) = n$. Thus $g(x) = b_0 + b_1x + \cdots + b_nx^n$ with $b_n \neq 0$. Also for $i \in \mathbb{N}$, $a^i = 0 \Rightarrow a = 0$, therefore $b_n^i \neq 0$ for all $i \in \mathbb{N}$ as $b_n \neq 0$. Let $f(x)g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$. But $f(x)g(x) = 0$, therefore $c_i = 0 \quad \forall\ i$. So $c_{m+n} = a_mb_n = 0$. We claim $a_{m-j}b_n^{j+1} = 0$ for all $0 \leq j \leq m$ and we establish our claim by induction over j. As $a_mb_n = 0$, so the result is true for the base case, $j = 0$. Suppose

$a_{m-j}b_n^{j+1} = 0$ for all $0 \leq j \leq k-1$. We need to show, result is valid for $j = k$ too. We have

$$\begin{aligned} & c_{m+n-k} = a_{m-k}b_n + a_{m-k+1}b_{n-1} + \cdots + a_m b_{n-k} = 0 \\ \Rightarrow\ & a_{m-k}b_n b_n^k + a_{m-k+1}b_{n-1}b_n^k + \cdots + a_m b_{n-k}b_n^k = 0b_n^k \\ \Rightarrow\ & a_{m-k}b_n^{k+1} + 0 + \cdots + 0 = 0 \\ \Rightarrow\ & a_{m-k}b_n^{k+1} = 0 \end{aligned} \tag{1}$$

So the result holds good for $j = k$ too. Thus we have $a_m b_n = a_{m-1}b_n^2 = \cdots = a_{m-j}b_n^{j+1} = \cdots = a_0 b_n^{m+1} = 0$. But that also means $a_m b_n^{m+1} = a_{m-1}b_n^{m+1} = \cdots = a_0 b_n^{m+1} = 0$, or $a_m b = a_{m-1}b = \cdots = a_0 b = 0$, where $b = b_n^{m+1}$. Hence the result. ∎

6. Do Problem 5 dropping the assumption that R has no nonzero nilpotent elements.

Solution: We choose some $g(x) \in R[x]$ from the set $\{g_i(x) \mid f(x)g_i(x) = 0\}$ such that $deg(g(x)) \leq deg(g_i(x)) \quad \forall i$. Note that the existence of such $g(x)$ is guaranteed as $S = \{deg(g_i(x)) \mid g_i(x)f(x) = 0\}$ is a non-empty set and is bounded from below. Now let $deg(g(x)) = n$ for some $n \in \mathbb{N}$ and therefore, let $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ with $b_n \neq 0$. Also $f(x)g(x) = 0$. Comparing coefficient of x^{m+n} in $f(x)g(x)$, we have $a_m b_n = 0$. So $a_m(f(x)g(x)) = a_m 0 \Rightarrow (a_m g(x))f(x) = 0$. Let $g'(x) = a_m g(x)$. So $g'(x)$ is a polynomial of degree less than n with $g'(x)f(x) = 0$, which is not possible as $g(x)$ is the polynomial with degree less than or equal to the degree of all polynomials with $g_i(x)f(x) = 0$. So

$$a_m g(x) = 0 \tag{1}$$

We claim $a_{m-j}g(x) = 0$ for $0 \leq j \leq m$. We establish our claim by induction over j. Base case with $j = 0$ has already been shown holding true. Suppose $a_{m-j}g(x) = 0$ for $0 \leq j \leq k-1$, i.e. result holds good upto $j = k-1$. We need to show result holds good for $j = k$ too, i.e. $a_{m-k}g(x) = 0$. We have

$$\begin{aligned} & f(x)g(x) - \sum_{j=0}^{k-1} a_{m-j}x^{m-j}g(x) = 0 \\ \Rightarrow\ & (f(x) - \sum_{j=0}^{k-1} a_{m-j}x^{m-j})g(x) = 0 \\ \Rightarrow\ & (a_0 + a_1 x + \cdots + a_{n-k}x^{n-k})g(x) = 0 \\ \Rightarrow\ & a_{m-k}b_n = 0 \end{aligned} \tag{2}$$

Now we have $f(x)g(x) = 0 \Rightarrow a_{m-k}(g(x)f(x)) = a_{m-k}0 \Rightarrow (a_{m-k}g(x))f(x) = 0$. Again let $a_{m-k}g(x) = g'(x)$, therefore $g'(x)f(x) = 0$. But (2) implies $deg(g'(x)) < deg(g(x))$, which is not possible, forcing $g'(x) = 0$. So $a_{m-k}g(x) = 0$, showing result is valid for $j = k$ too. Hence result is valid for all possible

j. Thus, we have $a_i g(x) = 0 \quad \forall\ i$. In particular, $a_i b_n = 0$ for all i. So if $b = b_n \neq 0$, we have $a_0 b = a_1 b = \cdots = a_m b = 0$. Hence the result. ∎

*7. If R is a commutative ring with unit element, prove that $a_0 + a_1 x + \cdots + a_n x^n$ in $R[x]$ has an inverse in $R[x]$ (i.e., is unit in $R[x]$) if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent elements in R.
Solution: We first prove two results required to prove the main result. First we claim that in a ring $\tilde{R}$, if $\tilde{x}, \tilde{y}$ are nilpotent, then so is $\tilde{x} + \tilde{y}$. Since $\tilde{x}$ and $\tilde{y}$ are nilpotent, so $\tilde{x}^l = 0$ and $\tilde{y}^m = 0$ for some $l, m \in \mathbb{N}$. But then $(\tilde{x} + \tilde{y})^{l+m} = 0$, showing $\tilde{x} + \tilde{y}$ is also a nilpotent. Hence the result. Secondly, in a ring $\tilde{R}$, if $\tilde{u}$ is unit and $\tilde{x}$ is nilpotent, then $\tilde{u} + \tilde{x}$ is again a unit. If $\tilde{x}$ is nilpotent, then $\tilde{x}^k = 0$ for some $k \in \mathbb{N}$. We have $(\tilde{u} + \tilde{x})(\tilde{u}^{-1} - \tilde{u}^{-2}\tilde{x} + \cdots + (-1)^{k-1}\tilde{u}^{-k}\tilde{x}^{k-1}) = 1 + (-1)^{k-1}\tilde{u}^{-k}\tilde{x}^k = 1$, showing $\tilde{u} + \tilde{x}$ is a unit element in $\tilde{R}$. Hence the result.

Now suppose a_0 is a unit element and $a_1, a_2, \cdots, a_n$ are nilpotent. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. But a_i are nilpotent implies $a_i x^i$ are nilpotent polynomials in $R[x]$. Also sum of two nilpotent elements is again a nilpotent, therefore $a_1 x + a_2 x^2 + \cdots + a_n x^n$ is a nilpotent polynomial in $R[x]$. Let $f(x) = a_0 + g(x)$, where $g(x) = a_1 x + \cdots + a_n x^n$ is a nilpotent polynomial in $R[x]$. But sum of a unit element and a nilpotent is again a unit, therefore $f(x)$ is a unit in $R[x]$. So $f(x)$ has inverse in $R[x]$

Conversely, suppose $f(x) = a_0 + a_1 x + \cdots + a_n x^n \neq 0$ in $R[x]$ has inverse, therefore there exists $g(x) = b_0 + b_1 x + \cdots + b_m x^m \neq 0$ in $R[x]$ such that $f(x)g(x) = 1$. Comparing constant terms of $f(x)g(x) = 1$, we have $a_0 b_0 = 1$. Thus a_0 is a unit element in R. Next we aim to show a_n is nilpotent. Comparing coefficient of x^{n+m} in the equation $f(x)g(x) = 1$, we have $a_n b_m = 0$. We claim $a_n^{j+1} b_{m-j} = 0$ for all $0 \leq j \leq m$; and we establish our claim by induction over j. For the base case $j = 0$, we need to show $a_n b_m = 0$, which we have already shown. Let $a_m^{j+1} b_{n-j} = 0$ for all $0 \leq j \leq i - 1$. We aim to show that the result is valid for $j = i$ too. Comparing coefficient of x^{n+m-i} in the equation $f(x)g(x) = 1$, we have

$$a_n b_{m-i} + a_{n-1} b_{m-i+1} + \cdots + a_{n-i} b_m = 0$$

Multiplying by a_n^i, and using induction hypothesis, we have $a_n^{i+1} b_{m-i} = 0$. Thus result is valid for $j = i$ too. So $a_n^{j+1} b_{m-j} = 0$ for all $0 \leq j \leq m$. For $j = m$, we have $a_n^{m+1} b_0 = 0 \Rightarrow a_n^{m+1} = 0$ as b_0 a unit element in R. So a_n is a nilpotent in R. Next we claim a_{n-k} is nilpotent for all $0 \leq k \leq n - 1$. We prove our claim by induction over k. When $k = 0$, we have already seen a_n is a nilpotent as $a_n^{m+1} = 0$. Suppose the result hold good for all $0 \leq k \leq i - 1$, we will show the result holds good for $k = i$ too. We have $f(x)$ unit element, and $a_{n-i+1} x^{n-i+1}, a_{n-i+2} x^{n-i+2}, \cdots, a_n x^n$ as idempotent, so $f(x) - a_{n-i+1} x^{n-i+1} - a_{n-i+2} x^{n-i+2} - \cdots - a_n x^n$ is a unit element in $R[x]$, or $a_0 + a_1 x + \cdots + a_{m-i} a^{m-i}$ is a unit element. So proceeding as we did for

base case, we get $(a_{n-i})^{j+1}b_{m-j} = 0$ for all $0 \leq j \leq m$. So for $j = m$, we have $a_{n-i}^{m+1} = 0$ as b_0 is a unit element. Thus we see result is valid for $k = i$ too. Thus a_{n-k} is nilpotent for all $0 \leq k \leq n-1$. In other words, $a_1, a_2, \cdots, a_n$ are nilpotent elements. Thus $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is a unit in $R[x]$ if and only if a_0 is a unit and rest a_i are nilpotent elements in R. ∎

8. Prove that when F is a field, $F[x_1, x_2]$ is not a principal ideal ring.
Solution: We break the problem in two parts. First we will show for F being a field implies $F[x_1]$ is not a field. Second, if $F[x_1, x_2]$ is a principal ideal ring over $F[x_1]$, then $F[x_1]$ must be a field.

Suppose $F[x_1]$ is a field, with given that F is a field. Therefore if $f(x_1) \neq 0 \in F[x_1]$, then $f(x_1)$ must be a unit element. But $f(x_1) = 1x_1 \in F[x_1]$ with $f(x_1)g(x_1) \neq 1 \quad \forall\ g(x_1) \in F[x_1]$ as $deg(f(x_1)g(x_1)) \geq 1$ while $deg(1) = 0$. This means that $f(x_1) = x_1$ has no inverse which is not possible as $F[x_1]$ is assumed to be a field. Hence $F[x_1]$ is not a field.

Next suppose $F[x_1, x_2]$ is a principal ideal ring over $F[x_1]$. We define $\psi : F[x_1, x_2] \longrightarrow F[x_1]$ such that $\psi(f_0(x_1) + f_1(x_1)x_2 + f_2(x_1)x_2^2 + \cdots) = f_0(x_1)$. We left it to the reader to check ϕ so defined is well-defined and is an onto ring-homomorphism. Thus $F[x_1, x_2]/K_\psi \approx F[x_1]$, where K_ψ is the kernel of mapping ψ. Note that K_ψ is an ideal in $F[x_1, x_2]$. Also

$$\begin{aligned}
K_\psi &= \{f(x_1, x_1) \mid \psi(f(x_1, x_2)) = 0\} \\
&= \{0 + g_1(x_1)x_2 + g_2(x_1)x_2^2 + \cdots \mid g_i(x_1) \in F[x_1] \quad \forall i\} \\
&= \{x_2(g_1(x_1) + g_2(x_1)x_2 + \cdots) \mid g_i(x_1) \in F[x_1] \quad \forall i\} \\
&= \{x_2 g(x_1, x_2) \mid g(x_1, x_2) \in F[x_1, x_2]\} \\
&= \langle x_2 \rangle
\end{aligned}$$

Now suppose, if possible there exist an ideal $M \in F[x_1, x_2]$ such that $K_\psi \subsetneq M \subsetneq F[x_1, x_2]$. But since $F[x_1, x_2]$ is assumed to be a principal ideal ring, therefore $M = h(x_1, x_1)F[x_1, x_2] = \langle h(x_1, x_1) \rangle$ as $F[x_1, x_2]$ is a commutative ring with unity. Also since $\langle x_2 \rangle \subsetneq \langle h(x_1, x_2) \rangle$, therefore $x_2 \in \langle h(x_1, x_2) \rangle \Rightarrow x_2 = h(x_1, x_2)q(x_1, x_2)$ for some $q(x_1, x_2) \in F[x_1, x_2]$. Therefore

$$\begin{aligned}
deg(x_2) &= deg(h(x_1, x_2)q(x_1, x_2)) \\
1 &= deg(h(x_1, x_2)) + deg(q(x_1, x_2))
\end{aligned}$$

So either $deg(h(x_1, x_2)) = 1$ and $deg(q(x_1, x_2)) = 0$, or $deg(h(x_1, x_2)) = 0$ and $deg(q(x_1, x_2)) = 1$. When $deg(h(x_1, x_2)) = 1$ and $deg(q(x_1, x_2)) = 0$, $x_2 = h(x_1, x_2)q(x_1, x_2)$ forces $h(x_1, x_2) = ux_2$ and $q(x_1, x_2) = u^{-1}$, where u is a unit element in $R[x_1]$. But then $M = \langle h(x_1, x_2) \rangle = \langle ux_2 \rangle = \langle x_2 \rangle = U$ which is not the case. In the second case, with $deg(h(x_1, x_2)) = 0$ and $deg(q(x_1, x_2)) = 1$, we have only possible solution as $h(x_1, x_2) = u$ and $q(x_1, x_2) = u^{-1}x_2$. But

then $M = \langle h(x_1, x_2)\rangle = \langle u\rangle = \langle 1\rangle = F[x_1, x_2]$ which contradicts our assumption. Thus U is a maximal ideal of $F[x_1, x_2]$. So $F[x_1, x_2]/U$ is a field. But $F[x_1, x_2]/U \approx F[x_1]$. So $F[x_1]$ is also a field.

Combing the two results, we have $F[x_1, x_2]$ is not a principal ideal ring for F being a field. ∎

9. Prove, completely, Lemma 3.11.2 and its corollary.
Solution: First we show the existence of greatest common divisor in a unique factorization domain. Let R be some unique factorization domain and some $a, b \in R$. We avoid $a = b = 0$ as greatest common divisor is not defined for it. When either of them is 0 while other not, then trivially their greatest common divisor is the non-zero element itself. So we now assume both a and b are non-zero. If any of them is unit, then their greatest common divisor is equal to 1 trivially. So we also assume non of them is not unit too. But then R being a unique factorization domain, so $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, where $\alpha_i \geq 0$ and $\beta_i \geq 0$, and p_i are irreducible factors. Note that such representation with common irreducible factors is possible as we have in this notation $p_i^0 = 1$. We define $\gamma_i = \text{Min}(\alpha_i, \beta_i) \quad \forall\ i$. Let $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$. Clearly d is uniquely(upto associates) determined for the given a, b. We claim $d = gcd(a, b)$. Clearly $d \mid a$ and $d \mid b$. Now suppose some $c \mid a$ and $c \mid b$. But $c \mid a$ implies $c = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$ with $\delta_i \leq \alpha_i$. But $c \mid b$ also, so $\delta_i \leq \beta_i$. But that means $\delta_i \leq \text{Min}(\alpha_i, \beta_i)$. So $c \mid d$. Also unique decomposition of a and b into irreducible p_i guarantees their greatest common divisor is uniquely determined upto the associates. Hence d is the required greatest common divisor.

Next suppose $gcd(a, b) = 1$ and $a \mid bc$. We need to show $a \mid c$. If a is a unit, then $a \mid c$ trivially. So we assume a is not a unit. Clearly $a \nmid b$ as if $a \mid b$, then adding $a \mid a$, we have $a \mid gcd(a, b) = 1$ which is not possible as a is not a unit. But if $a \nmid b$, then $a \mid bc$ implies $a \mid c$ as if $a \nmid c$ too, then $a \nmid bc$ too, which is not the case. Hence $a \mid c$.

Finally, if a is irreducible and $a \mid bc$, then need to show $a \mid b$ or $a \mid c$. In other words, we need to show that in a unique factorization domain, every irreducible element is a prime too. If either of b or c is a unit, then we have trivially a dividing the non-unit element. So we assume a and b are non-unit elements. We have $a \mid bc$ implies $bc = ad$ for some $d \in R$ with d not a unit element otherwise it would mean a is a reducible element which is not true. Also R being a unique factorization domain, so $b = p_1 p_2 \cdots p_n$, $c = q_1 q_2 \cdots q_m$ and $d = r_1 r_2 \cdots r_k$ for some irreducible p_i, q_i, r_i. So we have

$$ar_1 r_2 \cdots r_k = p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m = x(\text{say})$$

x being an element in R must have a unique representation, therefore $a = up_i$ for some unit u and some $1 \leq i \leq n$, or $a = u' q_j$ for some unit u' and $1 \leq j \leq m$.

When $a = up_i$, we have $p_i = u^{-1}a \Rightarrow a \mid p_i \Rightarrow a \mid b$ as $p_i \mid b$ for all i. So in this case, $a \mid b$. When $a = u'q_j$, we have $q_j = u'_{-1}a \Rightarrow a \mid q_j \Rightarrow a \mid c$ as $q_j \mid c$ for all j. So in this case $a \mid c$. Thus we concluded $a \mid bc$ implies $a \mid b$ or $a \mid c$. ∎

10. (a) If R is a unique factorization domain, prove that every $f(x) \in R[x]$ an be written as $f(x) = af_1(x)$, where $a \in R$ and where$f_1(x)$ is primitive.

(b) Prove that the decomposition in part(a) is unique (up to associates).

Solution:

(a) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ for some $n \in \mathbb{W}$. Let a be the content of $f(x)$. Therefore $a = gcd(a_0, a_1, \cdots, a_n)$. Note that existence of a, unique upto associates is guaranteed as R is a unique factorization domain. Thus we have $a \mid a_i$ for all i. So $a_i = aa'_i$ for some $a'_i \in R$. And so $f(x) = aa'_0 + aa'_1x + \cdots + aa_nx^n = a(a'_0 + a'_1x + \cdots + a'_nx^n) = f_1(x)$(say). Now suppose p be the content of $f_1(x)$, therefore $p \mid a'_i$ for all i. So $a'_i = pa''_i$ for some $a''_i \in R$. This leads to $a_i = apa''_i$. So $ap \mid a_i \quad \forall\ i$. But $gcd(a_0, a_1, \cdots, a_n) = a$, therefore $ap \mid a \Rightarrow p \mid 1 \Rightarrow p$ is a unit, which shows $f_1(x)$ is primitive. Thus every $f(x) \in R[x]$ can be written as $f(x) = af_1(x)$ where a is the content of $f(x)$ and $f_1(x)$ is primitive.

(b) Suppose decomposition is not unique(upto associates). Let $f(x) = a_1f_1(x) = a_2f_2(x)$. But then a_1, a_1, both are the greatest common divisors of non-zero coefficients of $f(x)$, so are associate of each other. Again note that the greatest common divisor of elements exists uniquely(upto associates) in a unique factorization domain. Thus $a_1 = ua_2$ for some unit $u \in R$. Using this, $a_1f_1(x) = a_2f_2(x)$ implies $uf_1(x) = f_2(x)$. So a_1 is associate of a_2 and $f_1(x)$ is associate of $f_2(x)$. ∎

11. If R is an integral domain, and if F is its field of quotients, prove that any element $f(x)$ in $F[x]$ can be written as $f(x) = (f(x_0)/a)$, where $f(x_0) \in R[x]$ and $a \in R$.

Solution: Let

$$f(x) = \sum_{i \in \lambda} \frac{a_i}{b_i} x^i$$

where $a_i, b_i \in R$ and λ is some finite index set such that $\frac{a_i}{b_i} \neq 0 \quad \forall\ i \in \lambda$. Define $a = lcm(\{b_i \mid i \in \lambda\})$. Therefore $b_i \mid a \quad \forall\ i \in \lambda \Rightarrow a = b_ib'_i$ for all $i \in \lambda$ and corresponding $b'_i \in R$. So

$$\begin{aligned} f(x) &= \sum_{i \in \lambda} \frac{a_i}{b_i} x^i \\ &= \frac{a}{a} \left(\sum_{i \in \lambda} \frac{a_i}{b_i} x^i \right) \\ &= \frac{1}{a} \left(\sum_{i \in \lambda} a \frac{a_i}{b_i} x^i \right) \end{aligned}$$

$$= \frac{1}{a}\left(\sum_{i\in\lambda} b_i b_i' x^i\right)$$
$$= \frac{1}{a} f_0(x), \text{ where } f_0(x) = \sum_{i\in\lambda} b_i b_i' x^i \in R[x]$$

Hence the result. ∎

12. Prove the converse part of Lemma 3.11.4.
Solution: We are given $f(x) \in R[x]$, and $f(x)$ as an element of $F[x]$ is irreducible in $F[x]$. Suppose $f(x)$ is reducible in $R[x]$, therefore $f(x) = g(x)h(x)$ with neither $g(x)$ nor $h(x)$ is a unit or zero element in $R[x]$. But $R[x] \subset F[x]$, so $g(x), h(x) \in F[x]$ too. Also if $g(x), h(x)$ are not unit elements in $R[x]$, then they are also not unit elements in $F[x]$. But then the relation $f(x) = g(x)h(x)$ implies $f(x)$ is reducible in $F[x]$ which is not true. Hence $f(x)$ is irreducible in $R[x]$ too. ∎

13. Prove corollary 2 to Theorem 3.11.1.
Solution: If F is a field then $F[x_1]$ is a Euclidean domain (Theorem 3.9.1). But a Euclidean domain is also a unique factorization domain (Theorem 3.7.2). So $F[x_1]$ is a unique factorization domain. But $F[x_1]$ being a unique factorization domain implies $F[x_1, x_2]$ is also a unique factorization domain. Again $F[x_1, x_2]$ being a unique factorization domain implies $F[x_1, x_2, x_3]$ is a unique factorization domain. Continuing this way, we get $F[x_1, x_2, \ldots, x_n]$ is a unique factorization domain. ∎

14. Prove that a principal ideal ring is a unique factorization domain.
Solution: First we will prove two lemmas required to prove the main result.

Lemma 1: *In a principal ideal ring, an element is prime if and only if it is irreducible.* Let R be some principal ideal ring. First suppose a is prime. So a is neither a unit or zero element. Suppose $a = bc$, therefore $a \mid (bc)$. But a being prime implies $a \mid b$ or $a \mid c$. When $a \mid b$, it implies $b = ad$ for some $d \in R$. Therefore $a = bc = (ad)c = a(dc) \Rightarrow a(1 - dc) = 0 \Rightarrow 1 - dc = 0 \Rightarrow dc = 1$. So $a \mid b$ implies c is a unit. Similarly $a \mid c$ implies b is a unit. So if $a = bc$ implies either b or c is unit. Thus we concluded a is an irreducible element. Conversely suppose a is an irreducible in R. Suppose $a \mid (bc)$. We define $U = \{ax + by \mid x, y \in R\}$. Easy to check that U is an ideal of R. But R being a principal ideal ring, so $U = dR$ for some $d \in R$. But $a \in U$, so $a = dr$ for some $r \in R$. Now a being an irreducible element so $a = dr$ implies either d is a unit or r is a unit. When d is a unit, we have $U = dR = R$. So $1 \in U$. Therefore we have $1 = ar_1 + br_2$ for some $r_1, r_2 \in R$. But that means $c = c(ar_1) + c(br_2) \Rightarrow c = a(cr_1) + (bc)r_2 \Rightarrow c = a(cr_1 + r_2) \Rightarrow a \mid c$. So at least

$a \mid c$ (a may divides b too). On the other hand when r is a unit, $U = dR = aR$. But since $b \in U$, therefore $b = ar_3$ for some $r_3 \in R$. So at least $a \mid b$ in this case. Thus $a \mid bc$ implies $a \mid b$ or $a \mid c$. So if a is an irreducible then it is a prime too. Hence the lemma.

We call a sequence of ideals $U_1, U_2, \cdots$ as *strictly increasing sequence* if $U_n \subsetneq U_{n+1} \quad \forall n \in \mathbb{N}$. We claim in a principal ideal ring, any strictly increasing sequence of ideals $U_1, U_2, \cdots$ must be finite in length. Let $U = \bigcup_i U_i$. We first claim U is an ideal. Let some $x, y \in U$, therefore $x \in U_m$ and $y \in U_n$ for some ideals U_m, U_n in the strictly increasing sequence of ideals. So either $U_m \subsetneq U_n$ or $U_n \subsetneq U_m$. In first case, when $U_m \subsetneq U_n$, we have $x - y \in U_n \subset U$. Also in second case when $U_n \subsetneq U_m$, we have $x - y \in U_m \subset U$. So $x - y \in U \quad \forall\, x, y \in U$. Next, let some $x \in U$, therefore $x \in U_m$ for some ideal in the strictly increasing sequence. But $xr \in U_m \subset U \quad \forall\, r \in R$. Thus we have shown U is an ideal of R. But R being a principal ideal ring, therefore $U = aR$ for some $a \in R$. But $1 \in R$, therefore $a1 \in U$. So $a \in U_k$ for some ideal U_k in the strictly increasing sequence of ideals. But then $U = aR \subset U_k$, implying that U_k is the last member of the strictly increasing sequence of ideals. Hence in a principal ideal ring, any strictly increasing sequence of ideals, $U_1, U_2, \cdots$ must be finite in length.

Lemma 2: *In a principal ideal ring, any strictly increasing sequence of ideals, $U_1, U_2, \cdots$ must be finite in length.*

Now with the above lemmas at our disposal, we aim to prove that every principal ideal ring is a unique factorization domain. Suppose R be some principal ideal ring. Let some $a \in R$ with not a unit or zero-element. First we will show a is a product of irreducible elements. To prove so, we first show a has at least one irreducible factor. Now if a itself is an irreducible element, then we are done. But if not, then $a = b_1 a_1$, where neither b_1 or a_1 is a unit or zero-element. Now again if a_1 is an irreducible element then we are done, but if a_1 is not an irreducible element, then $a_1 = b_2 a_2$, where neither b_2 or a_2 is a unit or zero-element. Continuing this way we get a sequence $a_1, a_2, \cdots$ with each element neither a unit nor a zero-element. From this sequence we induce a sequence of ideals, $a_1R, a_2R, \cdots$. We claim this sequence of ideals is strictly increasing, i.e. $a_1R \subsetneq a_2R \subsetneq \cdots$. Clearly $a_nR \subset a_{n+1}R$ as $a_n = b_{n+1}a_{n+1}$. But $a_nR = a_{n+1}R$ implies $a_{n+1} = a_n r$ for some $r \in R$. But that means $a_{n+1} = b_{n+1}a_{n+1}r \Rightarrow a_{n+1}(1 - b_{n+1}r) = 0 \Rightarrow b_{n+1}r = 1$ as R is an integral domain. So b_{n+1} is a unit, a contradiction, implying $a_nR \subsetneq a_{n+1}R$. So we have a strictly increasing sequence of ideals, $a_1R, a_2R, \cdots$. But Lemma 2 implies this sequence of ideals must terminate for some a_k. But that means a_k cannot be factorized into product into $b_{k+1}a_{k+1}$ with both b_{k+1} and a_{k+1} not equal to 0 or unit. But that means a_k is an irreducible element. So we have shown that a must have an irreducible factor. We now show a is a product of irreducibles. We have $a = p_1 c_1$ where p_1 is an irreducible element as we have just shown a must have at least one irreducible factor. Clearly $c_1 \neq 0$, otherwise $a = 0$, which

is not the case. Also if c_1 is a unit, then we are done, but if not, then $c_1 = p_2c_2$, where p_2 is an irreducible element as c_1 too must have at least one irreducible factor. Continuing this way, we get a sequence $c_1, c_2, \cdots$. From this sequence we induce a sequence of ideals as $c_1R, c_2R, \cdots$. We claim this sequence of ideals is strictly increasing, i.e. $c_nR \subsetneq c_{n+1}R$. To establish our claim, we first note that $(p_{n+1}c_{n+1})R \subset c_{n+1}R$. Also if $(p_{n+1}c_{n+1})R = c_{n+1}R \Rightarrow c_{n+1} = p_{n+1}c_{n+1}r$ for some $r \in R$, or $c_{n+1}(1 - p_{n+1}r) = 0$. R being an integral domain implies $1 = p_{n+1}r$. But that means p_{n+1} is a unit, which is not the case. So $c_nR \subsetneq c_{n+1}R$. Thus the sequence of ideals $c_1R, c_2R, \cdots$ is strictly increasing. But Lemma 2 implies it must terminate for some c_j. But that means c_j cannot be factorized into the product $p_{j+1}c_{j+1}$ as otherwise we would have $c_jR \subsetneq c_{j+1}R$. But that also means c_j is an irreducible element. Thus we have $a = p_1p_2 \cdots p_jc_j$, with all factors as irreducibles.

What left to be shown is the uniqueness of this factorization upto the associates and the order in which the irreducible factors appear. Suppose $a = p_1p_2 \cdots p_m = q_1q_2 \cdots q_n$. We use induction over m, i.e number of irreducible factors, to show the uniqueness. When $m = 1$, we have $a = p_1$, i.e. a is an irreducible. Therefore, $a = q_1q_2 \cdots q_n$ implies $n = 1$ and $a = q_1$. Therefore for $m = 1$, we have $n = 1$ and $p_1 = q_1$. Suppose the uniqueness(upto the associates and the order) holds good for $m = i - 1$. We need to show result is valid for $m = i$ too. We have $a = p_1p_2 \cdots p_i = q_1q_2 \cdots q_n$. But since $p_1 \mid a$, therefore $p_1 \mid (q_1q_2 \cdots q_n)$. But since p_1 is irreducible, so by Lemma 1, p_1 is prime too. Therefore p_1 divides some q_i, say q_1. But q_1 itself is irreducible, therefore $q_1 = p_1u$ for some unit u. Now we have $up_1p_2 \cdots p_i = uq_1q_2 \cdots q_n = q_1(uq_2 \cdots q_n$. R being an integral domain, so

$$p_2p_3 \cdots p_i = uq_2q_3 \cdots q_n$$

But the induction hypothesis implies factors on both sides are same upto the associates and the order in which they appear as number of irreducible factors are $i - 1$. Also $up_1 = q_1$. So a is unique upto the associates and the order in which its factors appear for $m = i$ too. Hence a is uniquely decomposable into irreducible factors in general. Thus we concluded R is a unique factorization domain. ∎

15. If J is the ring of integers, prove that $J[x_1, \ldots, x_n]$ is a unique factorization domain.
Solution: J, ring of integers, is a unique factorization domain, so using Corollary 2 of theorem 3.11.1, we have $J[x_1, x_2, \ldots, x_n]$ is also a unique factorization domain. ∎