Definition of a ring (1-1)

A **ring** $(R,+,\times)$ is a set R together with two binary operations $+$ (called **addition**) and $\times$ (called **multiplication** and usually omitted in products) satisfying the following axioms:

(i) $(R,+)$ is an abelian group;
(ii) $(ab)c = a(bc)$ for all $a,b,c \in R$;
(iii) $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ for all $a,b,c \in R$.

If, in addition, $ab = ba$ for all $a,b \in R$ then R is a **commutative ring**. The (i) means:

(a) $(a+b)+c = a+(b+c)$ for all $a,b,c \in R$;
(b) there is element $0 \in R$ such that $0+a = a = a+0$ for all $a \in R$;
(c) for any $a \in R$ there is another element $-a \in R$ is that $a+(-a) = 0 = (-a)+a$;
(d) $a+b = b+a$ for all $a,b \in R$.

As seen in Group Theory, the axiom (b) implies that the **zero element** $0 \in R$ is unique. Further, the axiom (c) implies that for any given $a \in R$ its **negative** $-a$ is also unique.

The axiom (ii) says that × is **associative**; the axioms (iii) are the **distributive laws**.

One can just say that R **is a ring** when the definitions of + and × are clear.

If there exists an element $1 \in R$ such that $1 \neq 0$ and $1a = a = a1$ for all $a \in R$, then R is a **ring with identity**. Prove that the **identity element** $1 \in R$, if it exists, is unique.

Examples

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all commutative rings with identity under the usual $+$ and $\times$

(2) $\mathbb{N}$ and $\mathbb{N}^0 = \mathbb{N} \cup \{0\}$ with the usual operations $+$ and $\times$ are **not** rings as they are not groups under $+$

(3) $2\mathbb{Z} = \{2z \,|\, z \in \mathbb{Z}\}$ with the usual operations $+$ and $\times$ again, is a commutative ring without 1

(4) For a ring R and any $n \in \mathbb{N}$ denote by $M_n(R)$ the set of all $n \times n$ matrices with entries from R. Then

$$M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R}), M_n(\mathbb{C})$$

are rings with identity I_n under the usual $+$ and $\times$ for matrices. These four rings are **not** commutative for $n > 1$. Please prove that for **any** ring R the $M_n(R)$ is a ring.

(5) $(\mathbb{Z}_n, \oplus\,, \otimes)$ is a commutative ring with identity [1]. This ring will be denoted by $\mathbb{Z}\,/n\,\mathbb{Z}$.

(6) Let X be a non-empty set and let $R = 2^X$ be its power set. That is, R is the collection of all subsets of X. Define binary operations, for all $A, B \in R$,

$$A + B = A \triangle B,$$
$$A \times B = A \cap B.$$

Then $(R, +\,, \times)$ is a ring with the zero element $\varnothing$ and the identity element X.

Proofs

(5) We have seen that $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ is an abelian group and $\otimes$ is associative, commutative and has identity $[1]$.

Let $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$. Then

$$[a]([b] \oplus [c]) = [a][b+c] = [a(b+c)] = [ab+ac] = [ab] \oplus [ac] = [a][b] \oplus [a][c],$$

and similarly

$$([a] \oplus [b])[c] = [a][c] \oplus [b][c].$$

(6) First of all, let us check (i) that $(R, \triangle)$ is an abelian group. For any subsets $A, B, C \subset X$

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

Indeed, both the left-hand side and the right-hand side are the collection of elements of X which belong precisely to one or to all three of A, B and C. Then, for any $A \subseteq X$ we have $A \triangle \varnothing = A$, so $\varnothing$ is the neutral element for the operation $\triangle$. Furthermore, $A \triangle A = \varnothing$, so every A is its own inverse for the operation $\triangle$. So $(R, \triangle)$ is a group.

Finally, the definition of $\triangle$ implies

$$A \triangle B = B \triangle A,$$

so the operation $\triangle$ is commutative and $(R, \triangle)$ is an abelian group.

We are now going to verify axioms (ii) and (iii) of the definition of ring.

For (ii) just observe that for any subsets $A, B, C \subseteq X$

$$(A \cap B) \cap C = A \cap (B \cap C)\,.$$

Indeed, both sides of the equality above represent the collection of elements of X which belong to all three A, B and C.

To prove (iii) it is enough to check that for any subsets $A, B, C \subseteq X$ the equality

$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)\,,$$

because the operation $\cap$ is commutative. It holds true because both sides are the collection of elements of X that belong to A and to precisely one of two subsets B and C.

Also $X \neq \varnothing$ and $A \cap X = A$ for any $A \subseteq X$. So X is the identity element of our ring. $\square$

Jacobson Theorem (without proof)

Let R be a ring such that for any $a \in R$ there is an integer $n > 1$ (possibly depending on a) such that $a^n = a$. Then R is commutative.

Elementary properties of rings (1-2)

Any ring R is an abelian group under $+$ by definition. In particular there is a unique element $0 \in R$ such that $0+a = a = a+0$ for all $a \in R$. Under $\times$ the R can be non-commutative.

Further, for any $a \in R$ the $-a$ is the unique element such that $a + (-a) = 0 = (-a) + a$.

Lemma

(i) $a\,0 = 0 = 0\,a$ for all $a \in R\,$;
(ii) $a(-b) = -(ab) = (-a)b$ for all $a, b \in R\,$;
(iii) $(-a)(-b) = ab$ for all $a, b \in R\,$.

Proof

(i) We have $a\,0 = a(0+0) = a\,0 + a\,0$ by the distributive law for R. By adding $-a\,0$ to the left and right sides we get $0 = a\,0$. Similarly, we get $0 = 0\,a$.

(ii) $a(-b) + ab = a((-b)+b) = a\,0 = 0$ so $-(ab) = a(-b)$. Similarly, $(-a)b = -(ab)$.

(iii) $(-a)(-b) = -((-a)b)) = -(-(ab)) = ab$ by using (ii). □

In particular, if R has an identity 1 then for all $b \in R$

$$(-1)b = -(1\,b) = -b \qquad \text{and} \qquad (-1)(-1) = 1 \times 1 = 1\,.$$

Let R be any ring and let $S \subseteq R$ be a subset. Then S is called a **subring** of R if:

(a) $0 \in S$
(b) $a, b \in S \;\Rightarrow\; -a, a+b, ab \in S$.

If $S \subseteq R$ is a ring under the same operations + and × as R, then S is a subring of R.

Proposition

If S is a subring of R , then S is itself a ring under the same operations + and × as R .

Proof

From (a) we have $0 \in S$. From (b) if $a, b \in S$ then $-a, a+b \in S$. So $(S, +)$ is a subgroup of $(R, +)$. Hence S is an abelian group itself.

Also from (b), the subset $S \subseteq R$ is closed under ×. Let $a, b, c \in S$. Then $a, b, c \in R$ so

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

by the definition of the ring used for R . Hence S is also a ring. □

Examples

(1) $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ without an identity.

(2) $M_n(\mathbb{Z})$ is a subring of $M_n(\mathbb{Q})$ which is a subring of $M_n(\mathbb{R})$; they are subrings with 1.

(3) Let $d \in \mathbb{Z}$ with $d \neq 1$ be **square free**, that is d is not divisible by p^2 for all primes p:

$$d \in \{\ldots, -6, -5, -3, -2, -1, 2, 3, 5, 6, \ldots\}$$

Let

$$\mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

with the usual + and × operations. Then $\mathbb{Z}[\sqrt{d}\,]$ is a subring of $\mathbb{C}$ with the identity

$$1 = 1 + 0\sqrt{d}\,.$$

Moreover, if $d > 0$ then $\mathbb{Z}[\sqrt{d}\,]$ is also a subring of $\mathbb{R}$. For example, if $d = 2$ then

$$\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}\,.$$

If $d = -1$ then

$$\mathbb{Z}[\sqrt{-1}\,] = \mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$. The elements of the ring $\mathbb{Z}[i]$ are called the **Gaussian integers**.

(4) Let R be any ring. Let X be any non-empty set. Consider

$$F_R^X = \{f \,|\, f : X \to R\}\,.$$

Define the binary operations $+$ and $\times$ on F_R^X for all $x \in X$ by

$$(f+g)(x) = f(x) + g(x), \ (f \times g)(x) = (fg)(x) = f(x)g(x)$$

pointwise addition and multiplication - **not** composition of functions. Then F_R^X is a ring.

Proof

(i) Please check that the set F_R^X with the operation $+$ is an abelian group. The zero element of F_R^X is the function $X \mapsto R$ given by $x \mapsto 0$ for any $x \in X$. The negative $-f$ is given by

$$(-f)(x) = -f(x)\,.$$

(ii) Let $f, g, h \in F_R^X$. Then for all $x \in X$

$$\big(f(gh)\big)(x) = f(x)(gh)(x) = f(x)\big(g(x)h(x)\big) =$$
$$\big(f(x)g(x)\big)h(x) = (fg)(x)h(x) = \big((fg)h\big)(x)$$

so that $f(gh) = (fg)h$ and the operation $\times$ is associative.

(iii) For all $x \in X$ we have

$$\begin{aligned} \big(f(g+h)\big)(x) &= f(x)\big((g+h)(x)\big) = f(x)\big(g(x)+h(x)\big) \\ &= f(x)g(x) + f(x)h(x) = (fg)(x) + (fh)(x) = (fg+fh)(x) \end{aligned}$$

so that $f(g+h) = fg + fh$. Similarly, we have $(f+g)h = fh + gh$. □

The ring F_R^X is commutative, if and only if R is commutative. The ring F_R^X has an identity, if and only if R has an identity 1. The identity of F_R^X is then the function $X \to R : x \mapsto 1$.

Homomorphisms and isomorphisms (1-3)

Let R, S be rings. A function $\alpha : R \to S$ is a **ring homomorphism** if for all $a, b \in R$:

(i) $\alpha(a+b) = \alpha(a) + \alpha(b)$,
(ii) $\alpha(ab) = \alpha(a)\alpha(b)$.

If R, S are rings with identity 1 and $\alpha(1) = 1$, then α is a **unital ring homomorphism.**

In particular, by (i) our α is a homomorphism of groups with respect to the addition $+$ on R, S. By a fact proved in Group Theory, then $\alpha(0) = 0$ and $\alpha(-a) = -\alpha(a)$ for all $a \in R$.

A **ring isomorphism** is a bijective ring homomorphism. We say that R is **isomorphic** to S if there exists an isomorphism $\alpha : R \to S$ and write $R \cong S$. Now let R, S, T be rings.

Lemma

(a) $\iota : R \to R$ defined by $\iota(a) = a$ is a ring isomorphism, so $R \cong R$;

(b) if $\alpha : R \to S$ is a ring isomorphism, then $\alpha^{-1} : S \to R$ is also a ring isomorphism; so if $R \cong S$, then $S \cong R$;

(c) if $\alpha : R \to S, \beta : S \to T$ are ring homomorphisms (isomorphisms), then $\beta\alpha : R \to T$ is a ring homomorphism (isomorphism); so if $R \cong S \cong T$, then $R \cong T$;

(d) if $R \cong S$ then R is commutative if and only if S is commutative.

Proof

(a,d) Please practice with proving these two statements.

(b) Let $x, y \in S$. We already know from Group Theory that

$$\alpha^{-1}(x+y) = \alpha^{-1}(x) + \alpha^{-1}(y),$$
$$\alpha^{-1}(-x) = -\alpha^{-1}(x).$$

Put $a = \alpha^{-1}(x)$ and $b = \alpha^{-1}(y)$. Then $\alpha(a) = x$ and $\alpha(b) = y$. As α is a homomorphism,

$$\alpha(ab) = \alpha(a)\alpha(b) = xy\,,$$
$$\alpha^{-1}(x)\alpha^{-1}(y) = ab = \alpha^{-1}(xy)\,.$$

Thus α^{-1} preserves the multiplication and hence it is a homomorphism. It is also bijective.

(c) We know $\beta\alpha$ preserves the $+$ operation. For all elements $a, b \in R$ we also have

$$(\beta\alpha)(ab) = \beta(\alpha(ab)) = \beta(\alpha(a)\alpha(b)) = \beta(\alpha(a))\beta(\alpha(b)) = (\beta\alpha)(a)(\beta\alpha)(b)$$

because α and β are homomorphisms. If α and β are isomorphisms, then their composition $\beta\alpha$ is also a bijection, hence an isomorphism. □

Examples

(1) Let
$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})\,.$$

Then S is a subring of $M_2(\mathbb{R})$. Indeed, the zero matrix is in S and $-X, X+Y \in S$ for any $X, Y \in S$. Please check that then also $XY \in S$. Now define a function $\alpha : \mathbb{C} \to S$ by
$$\alpha(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Then α is a bijection. Moreover,
$$\begin{aligned} \alpha\big((a+ib)+(c+id)\big) &= \alpha\big((a+c)+i(b+d)\big) = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \alpha(a+ib) + \alpha(c+id) \end{aligned}$$

and
$$\begin{aligned} \alpha\big((a+ib)(c+id)\big) &= \alpha\big(ac-bd+i(ad+bc)\big) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \alpha(a+ib)\,\alpha(c+id)\,. \end{aligned}$$

Thus α is a ring homomorphism, hence a ring isomorphism and we have $\mathbb{C} \cong S$.

(2) Let $m, n \in \mathbb{N}$ such that m divides n. That is $n = m\,l$ for some $l \in \mathbb{N}$. Define

$$\alpha : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

by

$$\alpha([z]_n) = [z]_m$$

For any $z \in \mathbb{Z}$. For any $w \in \mathbb{Z}$ we have

$$\begin{aligned} [z]_n = [w]_n \text{ in } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow n \text{ divides } z - w \\ &\Rightarrow m \text{ divides } z - w \\ &\Leftrightarrow [z]_m = [w]_m \text{ in } \mathbb{Z}/m\mathbb{Z} \end{aligned}$$

so that α is well defined. We have the equalities

$$\begin{aligned} \alpha([z]_n \oplus [w]_n) &= \alpha([z+w]_n) \\ &= [z+w]_m \\ &= [z]_m \oplus [w]_m \\ &= \alpha([z]_n) \oplus \alpha([w]_n) \end{aligned}$$

and similarly, $\alpha([z]_n[w]_n) = \alpha([z]_n)\,\alpha([w]_n)$. Thus α is a ring homomorphism. Note that $|\mathbb{Z}/n\mathbb{Z}| = n$ and similarly, $|\mathbb{Z}/m\mathbb{Z}| = m$. Hence α is a ring isomorphism only if $m = n$. In the latter case our α is just the identity function ι, hence an isomorphism by definition.

Units and fields (1-4)

Let R be a ring with an identity 1. If $a \in R$ and there exists $b \in R$ such that $ab = 1 = ba$, then we say that a is a **unit** of R. Clearly then b is also a unit. We denote

$$U(R) = \{a \in R \,|\, a \text{ is a unit}\}.$$

Remarks

(a) We have $1 \times 1 = 1 = 1 \times 1$ so $1 \in U(R)$. However, the identity $1 \in R$ is **unique** while there may be other units $a \in U(R)$. Units should **not** be confused with the identity 1 .

(b) Note that $0 \notin U(R)$, because $0 \times b = 0 \neq 1$ for any $b \in R$.

(c) If $a \in U(R)$ then the element b such that $ab = 1 = ba$ is unique. In fact, even a stronger fact holds true: if for an $a \in R$ there exist $b, c \in R$ such that $ab = ca = 1$, then necessarily $b = c$, hence $a \in U(R)$. Indeed, in this case we have

$$b = 1b = (ca)b = c(ab) = c1 = c\,.$$

We say b is the **inverse** of a and write $b = a^{-1}$. Hence the units are just all the invertible elements of the ring R with the identity 1. Clearly, for any $a \in R$ we have $(a^{-1})^{-1} = a$.

Proposition

Let $(R, +\,, \times)$ be a ring with an identity 1. Then $(U(R), \times)$ is a group.

Proof

We know that 1 is a unit of R, that is we have $1 \in U(R)$. Moreover $1 \times a = a = a \times 1$ for all $a \in U(R)$. We also know that $\times$ is associative.

If $u, v \in U(R)$ then u^{-1}, v^{-1} exist in R such that

$$uu^{-1} = 1 = u^{-1}u \qquad \text{and} \qquad vv^{-1} = 1 = v^{-1}v\,.$$

Notice that u is the inverse of u^{-1}, so that $u^{-1} \in U(R)$. Further,

$$(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = u1u^{-1} = uu^{-1} = 1\,,$$

and similarly,

$$(v^{-1}u^{-1})(uv) = 1\,.$$

Hence $uv \in U(R)$ by definition. Thus $U(R)$ is a group under the ring multiplication. □

Examples

(1) $U(M_n(\mathbb{R})) = GL_n(\mathbb{R})$ is the **general linear group** over $\mathbb{R}$;

(2) $U(\mathbb{Z}) = \{1, -1\}$;

(3) $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$, $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$, $U(\mathbb{C}) = \mathbb{C} \setminus \{0\}$;

(4) $U(\mathbb{Z}/n\,\mathbb{Z}) = \{\,[a] : a \in \mathbb{Z} \text{ and } (a, n) = 1\,\}$;

(5) For p a prime, $U(\mathbb{Z}/p\,\mathbb{Z}) = (\mathbb{Z}/p\,\mathbb{Z}) \setminus \{[0]\}$.

Proofs

(4) If $[a] \in U(\mathbb{Z}/n\mathbb{Z})$ then $[a][b] = [1]$ for some $b \in \mathbb{Z}$, so that $[ab] = [1]$ and $n \,|\, (ab - 1)$. Hence $ab - 1 = nq$ for some $q \in \mathbb{Z}$ and $ab - nq = 1$. Hence $(a, n) \,|\, 1$ so that $(a, n) = 1$.

Conversely, if $(a, n) = 1$ then $1 = as + nt$ for some $s, t \in \mathbb{Z}$ and so

$$[1] = [as + nt] = [as] = [a][s]$$

and so $[a] \in U(\mathbb{Z}\,/n\,\mathbb{Z})$.

(5) If $[a] \neq [0]$ then p does not divide a . So $(a, p) = 1$ and $[a]$ is a unit by the previous. $\square$

Definition

A **field** is a commutative ring F with an identity 1 such that $U(F) = F \setminus \{0\}$.

Examples

The already familiar $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}/p\mathbb{Z}$ for p a prime, all are fields. There are many others!

Zero divisors and integral domains (1-5)

Let R be a ring and $R \neq \{0\}$. An element $a \in R$ is a **zero divisor** if for some $b \in R \setminus \{0\}$

$$ab = 0 \quad \text{or} \quad ba = 0.$$

Note that if $a \neq 0$ then b is a zero divisor too. The set of zero divisors is denoted by $ZD(R)$.

If a is not a zero divisor we say a is a **non zero divisor**. This means for all $b \in R \setminus \{0\}$ we have $ab \neq 0$ and $ba \neq 0$. The set of non zero divisors is denoted by $NZD(R)$.

An **integral domain (ID)** is a commutative ring R with an identity element 1 such that R has no non-trivial zero divisors, that is $ZD(R) = \{0\}$ or equivalently, $NZD(R) = R \setminus \{0\}$.

Remark

For any ring R the condition $ZD(R) = \{0\}$ is equivalent to either of:

(i) for all $a, b \in R \setminus \{0\}$ we have $ab \neq 0$

(ii) for all $a, b \in R$ the equality $ab = 0$ implies that $a = 0$ or $b = 0$.

Lemma

(a) If R is a ring with an identity 1, then $U(R) \subseteq NZD(R)$.

(b) Any field is an integral domain.

Proof

(a) Let $a \in U(R)$. If $ab = 0$ then

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

and similarly, if $ba = 0$ then $b = 0$. Hence $a \in NZD(R)$.

(b) Let F be a field. Then F is a commutative ring with an identity. Further, if $a \in F \setminus \{0\}$, then $a \in U(F)$ and so $a \in NZD(F)$ by (a). Hence F is an integral domain by definition.

Examples

(1) In $\mathbb{Z}$ we have $U(\mathbb{Z}) = \{1, -1\}$ but $NZD(\mathbb{Z}) = \mathbb{Z} \setminus \{0\}$. Hence $U(\mathbb{Z}) \subset NZD(\mathbb{Z})$ but $U(\mathbb{Z}) \neq NZD(\mathbb{Z})$. Thus $\mathbb{Z}$ is an integral domain but not a field, because $U(\mathbb{Z}) \neq \mathbb{Z} \setminus \{0\}$.

(2) In $M_2(\mathbb{R})$ the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a zero divisor, because $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(3) In $\mathbb{Z}/n\mathbb{Z}$ we have $ZD(\mathbb{Z}/n\mathbb{Z}) = \{0\} \cup \{\, [a] : a \in \mathbb{Z} \text{ where } a \neq 0 \text{ and } (a, n) > 1 \,\}$. Indeed, if $d = (a, n) > 1$ then

$$\left[\frac{n}{d}\right] \neq [0],$$

$$[a]\left[\frac{n}{d}\right] = \left[a\,\frac{n}{d}\right] = \left[\frac{a}{d}\,n\right] = \left[\frac{a}{d}\right][n] = [0].$$

Conversely, if $(a, n) = 1$ so that $[a]$ is unit and hence not a zero divisor by the Lemma □

Cancellation Property

Let R be a ring and let $a \in R$ be a non zero divizor. Then for all $b, c \in R$ we have

$$ab = ac \quad \Rightarrow \quad b = c\,,$$

$$ba = ca \quad \Rightarrow \quad b = c\,.$$

Proof

If $ab = ac$ then $a(b-c) = 0$. Since a is a non zero divisor, we have $b - c = 0$ and so $b = c$. Similarly, if $ba = ca$ then $b = c$. □

For an any ring R with an identity 1 we have $U(R) \subseteq NZD(R)$ by Part (a) of our Lemma

Proposition

Let R be a finite ring with an identity 1. Then $U(R) = NZD(R)$.

Proof

Due to our Lemma $U(R) \subseteq NZD(R)$. Let us prove the opposite inclusion, if R is finite. Let $R \setminus \{0\} = \{\, a_1, a_2, \ldots, a_n \,\}$. Fix $a_i \in NZD(R)$. Then $a_i\, a_j \neq 0$ for $j = 1, \ldots, n$. So

$$\{a_i\, a_j : j = 1, \ldots, n\} \subseteq R \setminus \{0\}.$$

If $a_i\, a_j = a_i\, a_k$, then $a_j = a_k$ by the first part of the above Cancellation Property. Thus

$$|\,\{a_i\, a_j : j = 1, \ldots, n\}\,| = n\,.$$

Therefore

$$\{a_i\, a_j : j = 1, \ldots, n\} = R \setminus \{0\}.$$

But $1 \in R \setminus \{0\}$, so that $1 = a_i\, a_\ell$ for some a_ℓ . Similarly, $1 = a_k\, a_i$ for some a_k . Now

$$a_\ell = 1a_\ell = (a_k a_i)a_\ell = a_k(a_i a_\ell) = a_k 1 = a_k\,.$$

Hence $a_i \in U(D)$. □

Corollary

Let R be a finite integral domain. Then R is a field.

Proof

The ring R is commutative since it is an integral domain. Also $1 \in R$ and $ZD(R) = \{0\}$. By the above Proposition $U(R) = NZD(R) = R \setminus \{0\}$. So R is a field by definition. □

The hypothesis that R is **finite** is necessary in the Proposition and the above Corollary. For example, $\mathbb{Z}$ is an infinite ring with 1 where $ZD(\mathbb{Z}) = \{0\}$ but $U(\mathbb{Z}) = \{1, -1\} \neq \mathbb{Z} \setminus \{0\}$. Also $\mathbb{Z}$ is an integral domain, not a field. However, the commutativity hypothesis was **not** made in the Proposition. It can also be removed from the Corollary, due to the next result.

Wedderburn Theorem (without proof)

Let R be a finite ring with an identity 1 such that $ZD(R) = \{0\}$. Then R is a field.

Ideals of a ring (2-1)

Let R be any ring and $I \subseteq R$ be a subset. Then I is an **ideal** of R if

(i) $0 \in I$;
(ii) $a \in I \Rightarrow -a \in I$;
(iii) $a, b \in I \Rightarrow a + b \in I$;
(iv) $a \in I, r \in R \Rightarrow ar, ra \in I$.

Note that an ideal is a subring as we can take $a, r \in I$ in (iv). But the converse is not true.

Examples

(1) Let $n \in \mathbb{N}$. Then $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. Indeed:

(i) $0 = n0 \in n\mathbb{Z}$;
(ii) if $nz \in n\mathbb{Z}$ then $-(nz) = n(-z) \in n\mathbb{Z}$;
(iii) for any $nz, nw \in n\mathbb{Z}$ we have $nz + nw = n(z + w) \in n\mathbb{Z}$;
(iv) for any $nz \in n\mathbb{Z}$ and $r \in \mathbb{Z}$ we have $(nz)r = r(nz) = n(zr) \in n\mathbb{Z}$.

(2) $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. Indeed, we have $2 \in \mathbb{Z}$ and $\dfrac{1}{3} \in \mathbb{Q}$ but $2 \times \dfrac{1}{3} = \dfrac{2}{3} \notin \mathbb{Z}$.

(3) The sets $\{0\}$ and R are **always** ideals of R.

Theorem

(a) Suppose that the ring R has element 1. If $I \subseteq R$ is an ideal with $1 \in I$, then $I = R$.

(b) Suppose that the ring R has element 1. If for any element $a \in R \setminus \{0\}$ there exists an element $b \in R$ such that $ab = 1$ or $ba = 1$, then the ideals $\{0\} \subseteq R$ and R itself are the **only** ideals of R.

(c) If R is a field, then $\{0\} \subseteq R$ and R are the only ideals of R.

Proof

(a) Suppose that $1 \in I$ and let $I \subseteq R$ be an ideal. By definition of an ideal, for any element $r \in R$ and any $a \in I$ we have $ra \in I$. In particular, this property holds true for $a = 1$. But then $ra = r$, so in fact $r \in I$ for any $r \in R$. Hence $I = R$.

(b) Suppose that the ideal $I \subseteq R$ is strictly bigger than $\{0\}$. Then there exists $a \in R \setminus \{0\}$ such that $a \in I$. By the hypothesis, there exists $b \in R$ such that either $ba = 1$ or $ab = 1$. But then the definition of the ideal implies that $1 \in I$, and by (a) we infer $I = R$.

(c) This is a particular case of (b). □

Definition

Let $\alpha : R \to S$ be a ring homomorphism. The **kernel** and the **image** of α are

$$\operatorname{Im} \alpha = \{\, \alpha(r) \in S : r \in R \,\} \text{ and } \operatorname{Ker} \alpha = \{\, r \in R : \alpha(r) = 0 \,\}.$$

Lemma

Let $\alpha : R \to S$ be a ring homomorphism. Then:

(a) $\operatorname{Im}\alpha$ is a subring of S ;
(b) $\operatorname{Ker}\alpha$ is an ideal of R .

Proof

(a) We know α is a group homomorphism with respect to the + operation. It was proved in Group Theory that $\alpha(0) = 0$. Hence $0 \in \operatorname{Im}\alpha$. If $a, b \in \operatorname{Im}\alpha$ then $a = \alpha(x), b = \alpha(y)$ for some $x, y \in R$. Then by Group Theory $-a = -\alpha(x) = \alpha(-x) \in \operatorname{Im}\alpha$. Also

$$a + b = \alpha(x) + \alpha(y) = \alpha(x + y) \quad \text{and} \quad ab = \alpha(x)\,\alpha(y) = \alpha(xy)\,.$$

Hence $-a, a + b, ab \in \operatorname{Im}\alpha$. Therefore $\operatorname{Im}\alpha$ is a subring of S.

(b) By Group Theory $\alpha(0) = 0$. Hence $0 \in \operatorname{Ker}\alpha$. Let $u, v \in \operatorname{Ker}\alpha$ but $w \in R$. Then

$$\alpha(-u) = -\alpha(u) = -0 = 0 \quad \text{so that } -u \in \operatorname{Ker}\alpha\,.$$

Also

$$\alpha(u + v) = \alpha(u) + \alpha(v) = 0 + 0 = 0\,,$$

$$\alpha(uw) = \alpha(u)\alpha(w) = 0\alpha(w) = 0 \qquad \text{and} \qquad \alpha(wu) = \alpha(w)\alpha(u) = \alpha(w)0 = 0\,.$$

Hence $-u, u + v, uw, wu \in \operatorname{Ker}\alpha$. Therefore $\operatorname{Ker}\alpha$ is an ideal of the ring R . □

Proposition

Let $\alpha : R \to S$ be a ring homomorphism. Then α is one-to-one if and only if $\operatorname{Ker}\alpha = \{0\}$.

Proof

Suppose α is one-to-one. We know that $0 \in \operatorname{Ker}\alpha$. If $r \in \operatorname{Ker}\alpha$, then $\alpha(r) = 0 = \alpha(0)$ and so $r = 0$. Hence $\operatorname{Ker}\alpha = \{0\}$.

Conversely, suppose that $\operatorname{Ker}\alpha = \{0\}$. Then for any $u, v \in R$

$$\begin{aligned} \alpha(u) = \alpha(v) \;\Leftrightarrow\; \alpha(u) - \alpha(v) = 0 \;&\Leftrightarrow\; \alpha(u - v) = 0 \\ \Leftrightarrow\; u - v \in \operatorname{Ker}\alpha \;&\Leftrightarrow\; u - v = 0 \;\Leftrightarrow\; u = v \quad \square \end{aligned}$$

Corollary

Let R be a field, S be any ring and $\alpha : R \to S$ be any ring homomorphism. Then either $\operatorname{Im}\alpha = \{0\}$ or α is one-to-one. More generally, the same property of α holds if we replace the hypothesis that R is a field by a weaker property, that R has 1 and for any $a \in R \setminus \{0\}$ there exists $b \in R$ such that $ab = 1$ or $ba = 1$.

Proof

By the part (b) of the Lemma $\operatorname{Ker}\alpha$ is an ideal. By the part (b) of the Theorem any ideal of R can be only either $\{0\}$ or the whole R . If $\operatorname{Ker}\alpha = \{0\}$, then α is one-to-one by the above Proposition. If $\operatorname{Ker}\alpha = R$, then α maps all elements of R to 0 , so $\operatorname{Im}\alpha = \{0\}$. $\square$

Examples of ideals (2-2)

(1) We know that for any ring R the identity map $\iota : R \to R$ is an isomorphism. Please check that the zero function $\omega : R \to R : a \mapsto 0$ is a ring homomorphism. Accordingly,

$$\begin{aligned}\operatorname{Ker}\iota &= \{\, a \in R : \iota(a) = 0 \,\} = \{\, a \in R : a = 0 \,\} = \{0\}\,, \\ \operatorname{Ker}\omega &= \{\, a \in R : \omega(a) = 0 \,\} = R\end{aligned}$$

both are ideals of R. We have already seen this independently of homomorphism properties.

(2) Let

$$T_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}.$$

Please check that $T_2(\mathbb{R})$ is a subring of $M_2(\mathbb{R})$. Now define a function $\alpha : T_2(\mathbb{R}) \to \mathbb{R}$ by

$$\alpha \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a.$$

Then α is a ring homomorphism. Indeed,

$$\alpha\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \right) = \alpha \begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix} = a + a' = \alpha \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \alpha \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix},$$

$$\alpha\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \right) = \alpha \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix} = aa' = \alpha \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \alpha \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}.$$

Here

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \operatorname{Ker}\alpha \quad \Leftrightarrow \quad \alpha\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = 0 \quad \Leftrightarrow \quad a = 0$$

so that

$$\operatorname{Ker}\alpha = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} : b, c \in \mathbb{R} \right\}$$

is an ideal of $T_2(\mathbb{R})$. This can also be checked directly, not using the ideal property of $\operatorname{Ker}\alpha$.

(3) Let I, J be ideals of any ring R . Please check that $I \cap J$ is also an ideal of R . Define

$$I + J = \{a + b : a \in I, b \in J\}.$$

Lemma

(a) The sum $I + J$ is an ideal of R .

(b) The union $I \cup J \subseteq I + J$.

(c) The sum $I + J$ is the **smallest** ideal of R containing $I \cup J$.

Proof

(a) We have $0 = 0 + 0 \in I + J$ as $0 \in I$ and $0 \in J$. Let $x, y \in I + J$ and $z \in R$. Then $x = a+b$ and $y = c+d$ where $a, c \in I$ and $b, d \in J$. Using the fact that I and J are ideals,

$$-x = -(a + b) = (-a) + (-b) \in I + J\,,$$

$$x + y = (a + b) + (c + d) = (a + c) + (b + d) \in I + J\,,$$

$$xz = (a+b)z = az + bz \in I + J$$

and similarly

$$zx = z(a+b) = za + zb \in I + J\,.$$

Hence $I + J$ is an ideal of R.

(b) Let $a \in I$. Then $a = a + 0 \in I + J$, so that $I \subseteq I + J$. Similarly, $J \subseteq I + J$. Hence

$$I \cup J \subseteq I + J\,.$$

(c) We need to prove that if $K \subseteq R$ is any ideal of R containing the set $I \cup J$, then K also contains the ideal $I + J$. Let K be such an ideal. Then for any $a \in I$ and $b \in J$ we have $a, b \in K$. Hence $a + b \in K$ since K is closed under the $+$ operation. Thus $I + J \subseteq K$. $\Box$

For instance, we know that $I = 4\,\mathbb{Z}$ and $J = 10\,\mathbb{Z}$ are ideals of $R = \mathbb{Z}$. We claim that

$$4\,\mathbb{Z} + 10\,\mathbb{Z} = 2\,\mathbb{Z}\,.$$

If $x \in 4\,\mathbb{Z} + 10\,\mathbb{Z}$ then $x = 4u + 10v = 2(2u + 5v) \in 2\,\mathbb{Z}$. Conversely, if $y = 2z \in 2\,\mathbb{Z}$ then

$$y = (4(-2) + 10)z = 4(-2z) + 10z \in 4\,\mathbb{Z} + 10\,\mathbb{Z}\,.$$

Hence $4\,\mathbb{Z} + 10\mathbb{Z} = 2\,\mathbb{Z}$. More generally, for any $m, n \in \mathbb{N}$ by a simliar argument we obtain

$$m\,\mathbb{Z} + n\,\mathbb{Z} = (m, n)\,\mathbb{Z}\,.$$

Factor rings (2-3)

Let $(G, +)$ be an abelian group and $H \subseteq G$ be a subgroup. For any $a \in G$ the subset

$$a + H = \{a + x : x \in H\} \subseteq G$$

is the **coset** relative to H with a **representative** a. Now let $b \in G$ be another element. The Lemma below was proved in Group Theory, summarising the basic facts about cosets.

Lemma

(i) $a + H = b + H \iff a - b \in H$;
(ii) $a + H = b + H \iff (a + H) \cap (b + H) \neq \varnothing$;
(iii) $a + H = H \iff a \in H$.

The collection of all different cosets of G relative to H is denoted by G/H and is called the **factor**, or the **quotient** of G by H.

Now let R be any ring and $I \subseteq R$ be any ideal. Then $(R, +)$ is an abelian group and I is a subgroup. Consider the factor set R/I. Define the binary operations $+$ and $\times$ on R/I by

$$(a + I) + (b + I) = (a + b) + I \quad \text{and} \quad (a + I) \times (b + I) = ab + I\,.$$

Proposition

The operations $+$, $\times$ are well defined and make the set R/I a ring, called the **factor ring** or the **quotient ring** of R by the ideal I.

Proof

Suppose $a + I = a' + I$ and $b + I = b' + I$. Then $a - a', b - b' \in I$ by the Lemma. Hence

$$(a - a') + (b - b') \in I \quad \text{and} \quad ab - a'b' = (a - a')b + a'(b - b') \in I\,.$$

Thus

$$(a + b) - (a' + b') \in I \quad \text{and} \quad ab - a'b' \in I\,.$$

Therefore

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I\\ &= (a' + b') + I\\ &= (a' + I) + (b' + I)\end{aligned}$$

and similarly,

$$(a + I) \times (b + I) = (a' + I) \times (b' + I)\,.$$

So the operations + and × on the set R/I are well defined.

Further, for any three cosets $a + I, b + I, c + I \in R/I$

$$\begin{aligned}\big((a + I) \times (b + I)\big) \times (c + I) &= (ab + I) \times (c + I)\\ &= (ab)c + I\\ &= a(bc) + I\\ &= (a + I) \times (bc + I)\\ &= (a + I) \times \big((b + I) \times (c + I)\big)\end{aligned}$$

so that the operation × is associative. Similarly,

$$\begin{aligned}(a+I)\times\big((b+I)+(c+I)\big) &= (a+I)\times((b+c)+I)\\ &= a(b+c)+I\\ &= (ab+ac)+I\\ &= (ab+I)+(ac+I)\\ &= (a+I)\times(b+I)+(a+I)\times(c+I)\,.\end{aligned}$$

Also

$$((b+I)+(c+I))\times(a+I)=(b+I)\times(a+I)+(c+I)\times(a+I)$$

by a similar argument. So the operation × is distributive.

By Group Theory we know that $(R/I,+)$ is a group with identity $I=0+I$ and

$$-(a+I)=(-a)+I\,.$$

This group is abelian as

$$(a+I)+(b+I)=(a+b)+I=(b+a)+I=(b+I)+(a+I)\quad\Box$$

Example

Let $R=\mathbb{Z}$ and $I=n\,\mathbb{Z}$ where $n\in\mathbb{N}$. Then I is an ideal of R. For any $a,b\in\mathbb{Z}$ we have

$$a+I=b+I\;\Leftrightarrow\;a-b\in n\mathbb{Z}\;\Leftrightarrow\;n\,|\,(a-b)\;\Leftrightarrow\;a\equiv b \bmod n\,.$$

Hence in the quotient ring $\mathbb{Z}/I$ we have $a+I=[a]$. Moreover the + and × operations on $\mathbb{Z}/I$ are the usual **modulo** n rules $\oplus$ and $\otimes$. So the factor ring $\mathbb{Z}/I$ coincides with $\mathbb{Z}/n\,\mathbb{Z}$.

Fundamental Theorem of Homomorphisms for Rings (FTHR)

Let R, S be rings and $\alpha : R \to S$ a homomorphism. Then $\operatorname{Ker} \alpha$ is an ideal of R, the $\operatorname{Im} \alpha$ is a subring of S and

$$R/\operatorname{Ker} \alpha \cong \operatorname{Im} \alpha \, .$$

Proof

We already proved that $\operatorname{Ker} \alpha$ is an ideal of R and $\operatorname{Im} \alpha$ is a subring of S. Hence we only need to prove the isomorphism property. Let $I = \operatorname{Ker} \alpha$.

Define

$$\overline{\alpha} : R/I \to \operatorname{Im} \alpha$$

by

$$\overline{\alpha}\,(a+I) = \alpha(a).$$

For any $a, b \in R$

$$\begin{aligned} a+I = b+I \quad &\Leftrightarrow \quad a-b \in I \\ &\Leftrightarrow \quad \alpha(a-b) = 0 \\ &\Leftrightarrow \quad \alpha(a) = \alpha(b) \\ &\Leftrightarrow \quad \overline{\alpha}\,(a+I) = \overline{\alpha}\,(b+I) \, . \end{aligned}$$

This shows that the mapping $\overline{\alpha}$ is well defined and one-to-one.

Moreover, our $\overline{\alpha}$ is onto. Indeed, take any $u \in \operatorname{Im} \alpha$. Then $u = \alpha(a)$ for some $a \in R$ and

$$\overline{\alpha}\,(a+I) = \alpha(a) = u \, .$$

Now let $a+I, b+I \in R/I$. Then

$$\begin{array}{rcl}
\overline{\alpha}\left((a+I)+(b+I)\right) & = & \overline{\alpha}\left((a+b)+I\right) \\
& = & \alpha(a+b) \\
& = & \alpha(a)+\alpha(b) \\
& = & \overline{\alpha}\,(a+I)+\overline{\alpha}\,(b+I)
\end{array}$$

and

$$\begin{array}{rcl}
\overline{\alpha}\left((a+I)\times(b+I)\right) & = & \overline{\alpha}\,(ab+I) \\
& = & \alpha(ab) \\
& = & \alpha(a)\alpha(b) \\
& = & \overline{\alpha}\,(a+I)\times\overline{\alpha}\,(b+I)
\end{array}$$

so that $\overline{\alpha}$ is a ring homomorphism, hence an isomorphism. □

Examples of factor rings (2-4)

(1) Let I be an ideal of a ring R. Define the **canonical homomorphism**

$$\pi : R \to R/I$$

by

$$\pi(a) = a + I.$$

Lemma

The mapping π is an onto homomorphism with $\operatorname{Ker}\pi = I$.

Proof

For any $a, b \in R$ we have

$$\pi(a+b) = (a+b) + I = (a+I) + (b+I) = \pi(a) + \pi(b)$$

and

$$\pi(ab) = ab + I = (a+I) \times (b+I) = \pi(a) \times \pi(b).$$

Further, for any $a + I \in R/I$ we have $a + I = \pi(a)$ so that the homomorphism π is onto. Because the zero element of R/I is the coset $0 + I = I$, we have

$$a \in \operatorname{Ker}\pi \;\Leftrightarrow\; \pi(a) = I \;\Leftrightarrow\; a + I = I \;\Leftrightarrow\; a \in I.$$

So $\operatorname{Ker}\pi = I$. □

(2) Let R be any ring. Let X be any non-empty set. Denote $F = F_R^X = \{f \mid f : X \to R\}$. We have already proved that F is a ring with addition $+$ and multiplication $\times$ of functions defined pointwise. That is, for all $x \in X$

$$(f + g)(x) = f(x) + g(x) \text{ and } (f \times g)(x) = f(x)g(x)\,.$$

The zero of this ring is the function $x \mapsto 0$ for all $x \in X$. For any $f \in F$ the negative $-f$ is the function given by $(-f)(x) = -f(x)$ for all $x \in X$. Now fix $a \in X$ and put

$$I = \{f \in F \mid f(a) = 0\}\,.$$

(i) The subset $I \subset F$ is an ideal. Indeed, the zero function $x \mapsto 0$ belongs to I. Further, for any functions $f, g \in I$ and $h \in F$ we have

$$\begin{gathered}(-f)(a) = -f(a) = -0 = 0\,,\\ (f + g)(a) = f(a) + g(a) = 0 + 0 = 0,\\ (f \times h)(a) = f(a) \times h(a) = 0 \times h(a) = 0\end{gathered}$$

so that $-f, f + g, f \times h \in I$. By a similar argument, $h \times f \in I$.

(ii) The ring $F/I \cong R$. An isomorphism $\alpha : F/I \to R$ can be defined by $\alpha(f + I) = f(a)$. Indeed, two functions $f, g \in F$ define the same coset if and only if $f + I = g + I$. This means that $f - g \in I$, which is equivalent to $f(a) = g(a)$. Hence the mapping α is well defined and one-to-one. For any $r \in R$ the constant function $x \mapsto r$ is mapped to r by α. Hence α is onto R. Please check that α is a ring homomorphism, hence an isomorphism.

(3) Let R, S be rings. Consider the **direct product ring** $R \times S$. This is the cartesian product of the sets R and S with the addition and multiplication defined by

$$(r, s) + (r', s') = (r + r', s + s') \quad \text{and} \quad (r, s)\,(r', s') = (r\,r', s\,s')$$

for $r, r' \in R$ and $s, s' \in S$. In particular, the zero element of the ring $R \times S$ is $(0, 0)$ and

$$-\,(r, s) = (-r, -s)\,.$$

Please check that $R \times S$ satisfies all the axioms of a ring. Let us now show that

$$I = \{(0, s) \mid s \in S\}$$

is an ideal of $R \times S$ and $(R \times S)/I \cong R$. Indeed, define a mapping

$$\alpha : R \times S \to R$$

by

$$\alpha(r, s) = r\,.$$

Then

$$\alpha((r, s) + (r', s')) = \alpha(r + r', s + s') = r + r' = \alpha(r, s) + \alpha(r', s')$$

and

$$\alpha((r, s)\,(r', s')) = \alpha(r, s)\,\alpha(r', s')$$

by a similar argument. Hence α is a homomorphism. We have also have $\operatorname{Ker}\alpha = I$, because

$$(r, s) \in \operatorname{Ker}\alpha \;\Leftrightarrow\; \alpha(r, s) = 0 \;\Leftrightarrow\; r = 0 \;\Leftrightarrow\; (r, s) \in I\,.$$

For any $r \in R$ we have $r = \alpha(r, 0)$. Hence α is onto and $\operatorname{Im}\alpha = R$. By the Fundamental Theorem of Homomorphisms for Rings $I = \operatorname{Ker}\alpha$ is an ideal of $R \times S$ and $(R \times S)/I \cong R$.

(4) Let

$$T_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}.$$

We have proved that that $T_2(\mathbb{R})$ is a subring of $M_2(\mathbb{R})$, hence a ring itself. Let us show that

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} : b, c \in \mathbb{R} \right\}$$

is an ideal of $T_2(\mathbb{R})$ and $T_2(\mathbb{R})/I \cong \mathbb{R}$. Indeed, we proved that $\alpha : T_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$\alpha \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a$$

is a homomorphism onto with $\operatorname{Ker} \alpha = I$. By the Fundamental Theorem of Homomorphisms for Rings I is an ideal of $T_2(\mathbb{R})$ and $T_2(\mathbb{R})/I \cong \mathbb{R}$.

Binomial Theorem (2-5)

Let R be an arbitrary ring. For any $a \in R$ and $z \in \mathbb{Z}$ define the element $za \in R$ as follows: $0a = 0$ and for every $z \in \mathbb{N}$

$$za = \underbrace{a + \ldots + a}_{z \text{ times}}$$

while

$$(-z)a = z(-a) = \underbrace{(-a) + \ldots + (-a)}_{z \text{ times}} = -(za)\,.$$

If $\alpha : R \to S$ is any ring homomorphism, then it is a homomorphism of additive groups in particular. That is,

$$\alpha(a+b) = \alpha(a) + \alpha(b) \quad \text{for all} \quad a, b \in R\,.$$

By Group Theory

$$\alpha(za) = z\alpha(a) \quad \text{for all} \quad a \in R\,, z \in \mathbb{Z}\,.$$

Proposition

For all $z, w \in \mathbb{Z}$ and $a, b \in R$ we have the equalities

$$\begin{array}{rcl} (z+w)a & = & za + wa \\ (zw)a & = & z(wa) \\ z(a+b) & = & za + zb \\ (za)(wb) & = & (zw)(ab) \end{array}$$

Proof

The first two equalities have been seen in Group Theory. For the third, if $z = 0$ then

$$0(a+b) = 0 = 0 + 0 = 0a + 0b\,.$$

If $z \in \mathbb{N}$, then by our definition

$$z(a+b) = \underbrace{(a+b) + \ldots + (a+b)}_{z \text{ times}} = \underbrace{a + \ldots + a}_{z \text{ times}} + \underbrace{b + \ldots + b}_{z \text{ times}} = za + zb\,.$$

Then by the above and by the fact $-(u+v) = (-u) + (-v)$ in an abelian group, we have

$$(-z)(a+b) = -(z(a+b)) = -(za+zb) = (-(za)) + (-(zb)) = (-z)a + (-z)b.$$

The proof of the fourth equality in our Proposition is an exercise. □

For any $n \in \mathbb{N}$

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!} \quad \text{where} \quad k = 0, 1, \ldots, n\,.$$

Theorem

Let R be any commutative ring. Let $a, b \in R$ and $n \in \mathbb{N}$. Put $a^n\, b^0 = a^n$ and $a^0\, b^n = b^n$. Then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}\, a^{n-k}\, b^k\,.$$

Proof

We will use the induction on n. For $n = 1$,

$$(a+b)^1 = a + b = a^1\,b^0 + a^0\,b^1 = \binom{1}{0}\,a^1\,b^0 + \binom{1}{1}\,a^0\,b^1$$

as required. Now suppose the result is true for some $n \in \mathbb{N}$. Then

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

$$\sum_{k=0}^{n}\binom{n}{k}\,a^{n+1-k}\,b^k + \sum_{i=0}^{n}\binom{n}{k}\,a^{n-k}\,b^{k+1}$$

where we use the equality $ba = ab$. The coefficients of $a^{n+1}\,b^0$ and $a^0\,b^{n+1}$ are respectively

$$\binom{n}{0} = 1 = \binom{n+1}{0} \quad \text{and} \quad \binom{n}{n} = 1 = \binom{n+1}{n+1}.$$

For any $k = 1, \ldots, n$ the coefficient of $a^{n+1-k}\,b^k$ is

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Hence as required,

$$(a+b)^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}\,a^{n+1-k}\,b^k. \qquad \square$$

Rings of polynomials (3-1)

Let R be a commutative ring with an identity 1. Let x be a symbol, not an element of R. A **polynomial** in x over R is a formal expression

$$f = a_0 + a_1\, x + \ldots + a_n\, x^n$$

where $n \in \mathbb{N}^0 = \mathbb{N} \cup \{0\}$ and $a_0, \ldots, a_n \in R$. We say a_i is the **coefficient** of x^i.

Conventions

(a) We assume that $x^0 = 1$ and $x^1 = x$.

(b) We can miss out terms with 0 coefficient. For instance, in the case $R = \mathbb{Z}$ we can write $1 + 0x + 2x^2$ simply as $1 + 2x^2$.

(c) We will abbreviate $1\, x^i$ by x^i.

(d) A polynomial of the form a where $a \in R$ will be called a **constant** polynomial.

(e) An equality

$$a_0 + a_1\, x + \ldots + a_n\, x^n = b_0 + b_1\, x + \ldots + b_m\, x^m$$

means

$$\begin{aligned} a_0 = b_0,\ a_1 = b_1,\ \ldots\ , a_n = b_n,\ b_{n+1} = \ldots = b_m = 0 \quad &\text{if} \quad m \geqslant n\,, \\ a_0 = b_0,\ a_1 = b_1,\ \ldots\ , a_m = b_m,\ a_{m+1} = \ldots = a_n = 0 \quad &\text{if} \quad m \leqslant n\,. \end{aligned}$$

For example, in the case $R = \mathbb{Z}$ we have

$$1 + 0x + 2x^2 = 1 + 0x + 2x^2 + 0x^3.$$

(f) The addition and multiplication of polynomials are defined as follows. The addition:

$$(a_0 + a_1\,x + \ldots + a_n\,x^n) + (b_0 + b_1\,x + \ldots + b_m\,x^m) = c_0 + c_1\,x + \ldots + c_\ell\,x^\ell$$

where $\ell = \max\{m, n\}$ and

$$c_i = \begin{cases} a_i + b_i & \text{if} \quad i \leqslant \min\{m, n\} \\ a_i & \text{if} \quad m < i \leqslant n \\ b_i & \text{if} \quad n < i \leqslant m \end{cases}$$

Note that $c_0 = a_0 + b_0$. The multiplication:

$$(a_0 + a_1\,x + \ldots + a_n\,x^n) \times (b_0 + b_1\,x + \ldots + b_m\,x^m) = d_0 + d_1x + \ldots + d_{n+m}\,x^{n+m}$$

where for $0 \leqslant k \leqslant m + n$

$$d_k = \sum_{i+j=k} a_i\,b_j\,.$$

Note that

$$(a_0 + a_1\,x + \ldots + a_n\,x^n) \times (b_0 + b_1\,x + \ldots + b_m\,x^m) =$$

$$a_0\,b_0 + (a_0\,b_1 + a_1\,b_0)\,x + \ldots + (a_n\,b_{m-1} + a_{n-1}\,b_m)\,x^{n+m-1} + a_n\,b_m\,x^{n+m}\,.$$

Notation

The set of all polynomials in x over R is denoted by $R[x]$.

Proposition

Let R be a commutative ring with an identity 1 . Then $(R[x], + \,, \times)$ is also a commutative ring with an identity. The zero and identity of $R[x]$ are the constant polynomials 0 and 1 .

Proof

This is a direct verification of the ring axioms for $R[x]$. It can done as a revision exercise. $\square$

Let f be any **non-zero** polynomial. Then for some $n \geqslant 0$ we can write

$$f = a_0 + \ldots + a_n \, x^n$$

where $a_n \neq 0$. The n is called the **degree** of f and denoted by $\deg f$. The a_n is called the **leading coefficient** of f . Notice that the zero polynomial 0 is **not** assigned any degree.

Note that $\alpha : R \to R[x]$ given by $\alpha(r) = r$ is a one-to-one homomorphism. Indeed,

$$\alpha(r+s) = r + s = \alpha(r) + \alpha(s) \quad \text{and} \quad \alpha(rs) = rs = \alpha(r)\alpha(s) \, .$$

Hence we can regard R as a subring of $R[x]$, by identifying any element $r \in R$ with the corresponding constant polynomial $r \in R[x]$.

Theorem

Let R be an integral domain. Then $R[x]$ is an integral domain and for $f, g \in R[x] \setminus \{0\}$

$$\deg(fg) = \deg f + \deg g\,. \tag{$*$}$$

Proof

By definition, our R is a commutative ring with an identity 1 such that $ZD(R) = \{0\}$. By the above Proposition we already know that $R[x]$ is a commutative ring with an identity 1 . Now let $f, g \in R[x] \setminus \{0\}$. Then we can write

$$f = a_0 + \ldots + a_n\, x^n \quad \text{and} \quad g = b_0 + \ldots + b_m\, x^m$$

where $a_n, b_m \neq 0$. Here

$$n = \deg f \quad \text{and} \quad m = \deg g\,.$$

By definition,

$$fg = a_0\, b_0 + \ldots + a_n\, b_m\, x^{n+m}\,.$$

Since $ZD(R) = \{0\}$, we have $a_n\, b_m \neq 0$. Therefore the product $f\, g \neq 0$ and

$$\deg(fg) = n + m = \deg f + \deg g\,.$$

It also follows that $ZD(R[x]) = \{0\}$. Hence $R[x]$ is an integral domain. □

Now consider the set $U(R)$ of units the ring R. By definition, $a \in U(R)$ if and only if $ab = ba = 1$ for some $b \in R$. The equality $ab = ba$ also follows from commutativity of R.

Corollary

Suppose that R is an integral domain. Then $U(R[x]) = U(R)$.

Proof

Take any $a \in U(R)$. Then a has an inverse $b \in R$ such that $ab = 1$. Both $a, b \in R[x]$ as constant polynomials, so that $a \in U(R[x])$. Conversely, let $f \in U(R[x])$ so that there exists $g \in R[x]$ such that $fg = 1$. Then $f, g \neq 0$. By our Theorem

$$0 = \deg 1 = \deg(fg) = \deg f + \deg g\,,$$

so that $\deg f = \deg g = 0$ and therefore $f, g \in R$. Clearly, then $f \in U(R)$. □

The proof of the above Corollary demonstrates that $U(R) \subseteq U(R[x])$ for any commutative ring R with 1. However, the opposite inclusion and the equality $(*)$ are **not** true in general.

Example

Let $R = \mathbb{Z}/4\mathbb{Z}$. This is a commutative ring with an identity 1, but not an integral domain: in this ring $[2]\,[2] = [4] = 0$. Take the polynomial $f = [1]+[2]x$ with coefficients in R. Then

$$f^2 = ([1] + [2]x)([1] + [2]x) = [1] + [4]x + [4]x^2 = [1] = 1$$

so that $\deg f^2 = 0 \neq \deg f + \deg f$. Moreover, $f \in U(R[x])$. But $f \notin R$, hence $f \notin U(R)$.

Polynomial functions (3-2)

Let r range over R. Let $f \in R[x]$ where R is any commutative ring with identity 1. Then

$$f = a_0 + a_1 x + \ldots + a_n x^n$$

where $a_0, a_1, \ldots, a_n \in R$. Define a **polynomial function** $f(r)$ with values in R by

$$f(r) = a_0 + a_1 r + \ldots + a_n r^n$$

for every $r \in R$. Thus $f(r)$ is the result of substituting the element $r \in R$ for x in f, and then calculating with $+$ and $\times$ in R. Constant polynomials give rise to constant functions. That is, if $f = a$ with $a \in R$ is a constant polynomial, then $f(r) = a$ for all $r \in R$.

In the particular case when $R = \mathbb{R}$ or $R = \mathbb{C}$ we know that for any $f, g \in R[x]$ the equality $f(r) = g(r)$ of functions implies the equality $f = g$ of polynomials. So the correspondence $f \mapsto f(r)$ is one-to-one in this case. This is **not** true for an arbitrary ring R, even for a field.

Example

Let $R = \mathbb{Z}/2\,\mathbb{Z}$ so that R is a finite field. The elements of R are just $[0]$ and $[1]$. Consider

$$f = [1] + x \quad \text{and} \quad g = [1] + x + x^2 + x^4$$

in $R[x]$. Then

$$f([0]) = [1] = g([0]) \quad \text{and} \quad f([1]) = [0] = g([1])$$

so that $f(r) = g(r)$ as functions of $r \in \mathbb{Z}/2\,\mathbb{Z}$. However $f \neq g$ in $R[x]$.

Division Algorithm for polynomials (3-3)

Let F be any field. So F is a commutative ring with an identity 1 such that $U(F) = F \backslash \{0\}$.

Theorem

Let $f, g \in F[x]$ with $g \neq 0$. Then there exist unique $q, r \in F[x]$ with $r = 0$ or with $r \neq 0$ and $\deg r < \deg g$, such that

$$f = g\,q + r\,.$$

Proof of existence

If $\deg g = 0$, then $g \in U(F)$. Write $f = g\,(g^{-1}f) + 0$. Hence we can take

$$q = g^{-1}f \quad \text{and} \quad r = 0\,.$$

Now suppose that $\deg g = m > 0$. Let

$$L = \{f - g\,q : q \in F[x]\}.$$

If $0 \in L$ then for some q we get the equality $f - g\,q = 0$. Hence $f = g\,q + 0$ so that $r = 0$.

Suppose $0 \notin L$. Let

$$k = \min\{\,\deg s : s \neq 0,\ s \in L\,\}.$$

Take any $r \in L$ with $r \neq 0$ and $\deg r = k$, so that $r = f - g\,q$ for some q and hence

$$f = g\,q + r\,.$$

Write

$$g = b_0 + b_1\, x + \ldots + b_m\, x^m$$

and

$$r = c_0 + c_1\, x + \ldots + c_k\, x^k\,.$$

Here $b_m \neq 0$ and $c_k \neq 0$, because $m = \deg g$ and $k = \deg r$. Suppose that $k \geqslant m$. Then

$$c_k\, b_m^{-1}\, x^{k-m} \in F[x]\,.$$

Consider the polynomial

$$s = r - c_k\, b_m^{-1}\, x^{k-m}\, g\,.$$

Then $s = 0$ or $s \neq 0$ with $\deg s < k$, because the leading terms of r and g are $c_k\, x^k$ and $b_m\, x^m$ respectively, while $k \geqslant m$. On the other hand,

$$s = f - g\, q - c_k\, b_m^{-1}\, x^{k-m}\, g = f - g\,(\, q + c_k\, b_m^{-1}\, x^{k-m}\,) \in L\,.$$

This contradicts either to $0 \notin L$ or to the minimality of k. So $\deg r = k < m = \deg g$. □

Proof of uniqueness

Suppose that

$$f = g\, q + r = g\, q' + r'$$

where $q, q' \in F[x]$ while

$$r = 0 \quad \text{or} \quad \deg r < \deg g\,,$$

$$r' = 0 \quad \text{or} \quad \deg r' < \deg g\,.$$

Then

$$g\,(q - q'\,) = r' - r\,.$$

If $r' - r \neq 0$, then

$$\deg\,(r' - r) < \deg g\,.$$

But the latter is impossible, since the polynomial g is a factor of $r' - r$. Hence $r' - r = 0$, that is $r' = r$. Also, then

$$g\,(q - q'\,) = 0\,.$$

But $g \neq 0$ while $ZD(F[x]) = \{0\}$ since F is a field, hence an integral domain in particular. Therefore $q - q' = 0$ and $q = q'$ as required. □

Example

Let $F = \mathbb{Z}/5\mathbb{Z}$. Consider the polynomials in x with coefficiends from F

$$f = x^5 + [3]x^4 + [2]x^2 + [4] \quad \text{and} \quad g = [2]x^2 + [1]\,.$$

Find the polynomials $q, r \in F[x]$ with $r = 0$ or with $r \neq 0$ and $\deg r < \deg g$, such that

$$f = g\,q + r\,.$$

Solution

We know that $r = 0$, or $r \neq 0$ with $\deg r < \deg g = 2$. We also know that

$$\deg q = \deg f - \deg g = 5 - 2 = 3\,.$$

So we can write

$$q = a\,x^3 + b\,x^2 + c\,x + d\,, \quad r = u\,x + v$$

where $a, b, c, d, u, v \in F$. By using the above expressions for q, r we get the equation

$$x^5 + [3]x^4 + [2]x^2 + [4] = ([2]x^2 + [1])(ax^3 + bx^2 + cx + d) + (ux + v)\,.$$

By opening the brackets, equating respective coefficients at both sides and using $[3][2] = [1]$,

$$\begin{array}{lll}
[1] = [2]\,a & [3] = a & a = [3] \\
[3] = [2]\,b & [9] = b & b = [4] \\
[0] = [2]\,c + a & [0] = c + [3]\,a & c = -[3][3] = [1] \\
[2] = [2]\,d + b & [6] = d + [3]\,b & d = [6] - [3][4] = [4] \\
[0] = c + u & [0] = c + u & u = -[1] = [4] \\
[4] = d + v & [4] = d + v & v = [4] - [4] = [0]
\end{array}$$

Here in the second column the top four equations are obtained by multiplying by [3] the top four equations in the first column. In the third column we solve the so obtained equations one by one, starting from the top. Hence we find

$$q = [3]x^3 + [4]x^2 + x + [4]\,, \quad r = [4]x\,.$$

Principal ideal domains (3-4)

Let R be any commutative ring with an identity 1.

Lemma

For any $a \in R$ the set

$$aR = \{\, a\, r : r \in R\,\}$$

is an ideal of R containing a. And if $I \subseteq R$ is another ideal containing a, then $aR \subseteq I$.

Proof

We have $0 = a0 \in aR$. If $b = ax$, $c = ay \in aR$ and $r \in R$ then

$$-b = -(ax) = a(-x), \quad b + c = ax + ay = a(x + y), \quad br = (ax)r = a(xr) \in aR\,.$$

Hence aR is an ideal of R. Further, $a = a1 \in aR$ and if $a \in I$ where I is an ideal, then for any $r \in R$ we have $ar \in I$. Thus $aR \subseteq I$. □

The ideal aR of R is called the **principal ideal** generated by the element $a \in R$.

Examples

(1) For any R, the zero ideal $\{0\} \subseteq R$ is the principal ideal generated by $0 \in R$.

(2) In the ring $R = \mathbb{Z}$, for any $n \in \mathbb{N}$ we have the principal ideal $n\,\mathbb{Z} \subseteq \mathbb{Z}$.

Definition

A **principal ideal domain (PID)** is an integral domain where every ideal is principal.

Proposition

The ring $\mathbb{Z}$ is a principal ideal domain.

Proof

We already know $\mathbb{Z}$ is an integral domain. Hence we need to prove that each ideal of $\mathbb{Z}$ is principal. By (1) the zero ideal $\{0\} \subseteq \mathbb{Z}$ is principal. Now let $S \subseteq \mathbb{Z}$ be a non-zero subring. We will prove that then $S = n\,\mathbb{Z}$ for some $n \in \mathbb{N}$.

Pick any $a \in S \setminus \{0\}$. Then $a, -a \in S$ so that $S \cap \mathbb{N} \neq \varnothing$. Let n be the minimal natural number in S. Then $n\,\mathbb{Z} \subseteq S$ as S is closed under addition and negation. On the other hand, for any $u \in S$, by the Division Algorithm for $\mathbb{Z}$ we have

$$u = n\,q + r$$

where $q, r \in \mathbb{Z}$ and $0 \leqslant r < n$. Then we get

$$r = u - n\,q \in S$$

and to avoid a contradiction with the minimality of n we must have $r = 0$. Hence $u \in n\,\mathbb{Z}$ and $S \subseteq n\,\mathbb{Z}$. Therefore $S = n\,\mathbb{Z}$ as required. $\square$

Theorem

Let F be any field. Then the ring $F[x]$ is a principal ideal domain.

Proof

We already know that $F[x]$ is an integral domain. We need to show that every ideal of $F[x]$ is principal. Let I be an ideal of $F[x]$. If $I = \{0\}$, then I is principal by (1) above. Suppose that $I \neq \{0\}$ and let $g \in I$ be such that $g \neq 0$ and $\deg g$ is minimal for all elements of I. By the definition of an ideal,

$$gF[x] \subseteq I\,.$$

Now take any $f \in I$. By the Division Algorithm for $F[x]$,

$$f = g\,q + r$$

where $q, r \in F[x]$ and either $r = 0$, or $r \neq 0$ and $\deg r < \deg g$. But

$$r = f - g\,q \in I,$$

and to avoid a contradiction with the minimality of $\deg g$ we must have $r = 0$. Thus

$$f = g\,q \in gF[x]\,.$$

Hence

$$I \subseteq gF[x]$$

and we conclude that $I = gF[x]$. □

Divisibility in integral domains (4-1)

Throughout this section, D denotes any integral domain. Hence D is a commutative ring with an identity 1, such that 0 is the only zero divisor in D. For example, our D can be

$$\mathbb{Z}\,,\mathbb{Z}[\sqrt{d}\,] \quad \text{or} \quad F\,,F[x]$$

where F is any field. For any square free $d \in \mathbb{Z} \setminus \{1\}$ the ring $\mathbb{Z}[\sqrt{d}\,]$ is an integral domain, because it is a subring of $\mathbb{C}$ containing 1. And we know that $\mathbb{C}$ is an integral domain itself.

We will say that $b \in D$ **divides** $a \in D$ if $a = b\,c$ for some $c \in D$. We will write $b \,|\, a$ then.

Note that if $b \in U(D)$ then for any $a \in D$ we have $a = b\,(b^{-1}a)$ and so $b \,|\, a$. Here $c = b^{-1}a$. In particular, if D is a field then every non-zero element divides every element.

Definitions

(i) An element $a \in D$ is **irreducible** if $a \neq 0$, $a \notin U(D)$ and for any $b, c \in D$

$$a = b\,c \;\Rightarrow\; b \in U(D) \text{ or } c \in U(D)\,.$$

(ii) An element $p \in D$ is **prime** if $p \neq 0$, $p \notin U(D)$ and for any $a, b \in D$

$$p \,|\, ab \;\Rightarrow\; p \,|\, a \text{ or } p \,|\, b\,.$$

(iii) Elements $a, b \in D$ are **associates** if $a = b\,u$ for some $u \in U(D)$. Write $a \sim b$ then.

Remarks

(1) If $a \in D$ is irreducible and $a = b\,c$, then $a \sim b$ or $a \sim c$.

(2) By induction on $n \in \mathbb{N}$, if $p \in D$ is prime and

$$p \,|\, a_1 \ldots a_n$$

then $p \,|\, a_i$ for some $1 \leqslant i \leqslant n$. In particular, then for any $a \in D$

$$p \,|\, a^n \;\Rightarrow\; p \,|\, a.$$

(3) If $b \,|\, a$ where $a \in U(D)$, then $a = b\,c$ so that $1 = b\,(ca^{-1})$ and hence $b \in U(D)$.

Lemma

(a) The relation $\sim$ is an equivalence.
(b) The equivalence classes of 0 and 1 in D are $\{0\}$ and $U(D)$ respectively.

Proof

For any $a \in D$ we have $a = a1$ so that $a \sim a$. Now let $a, b, c \in D$. If $a \sim b$ then $a = b\,u$ where $u \in U(D)$. Hence $b = au^{-1}$ so that $b \sim a$. Suppose that also $b \sim c$, then $b = c\,v$ for some $v \in U(D)$. Hence

$$a = b\,u = (c\,v)\,u = c\,(v\,u)$$

and $v\,u \in U(D)$. Therefore $a \sim c$. Thus we get (a). The proof of (b) is an exercise. $\square$

Example

In $\mathbb{Z}$ the units are $\{1, -1\}$. It follows that the equivalence classes are

$$\{0\}, \{1, -1\}, \{2, -2\}, \ldots$$

Remarks (continued)

(4) If $b \,|\, a$ and $a \,|\, b$, then $a \sim b$. Indeed, if $a = b\,c$ and $b = a\,d$ for some $c, d \in D$ then

$$a\,1 = a = b\,c = a\,d\,c\,.$$

If $a = 0$ then also $b = 0$ and hence $a \sim b$. If $a \neq 0$ then a is not a zero divisor because D is an integral domain. But then by the Cancellation Property

$$1 = d\,c$$

and so $c, d \in U(D)$. Hence $a \sim b$ again.

(5) If $p, q \in D$ are primes and $p \,|\, q$, then $p \sim q$. Indeed, here we have

$$q = q1 = p\,r$$

for some $r \in D$. Since q is prime, here $q \,|\, p$ or $q \,|\, r$. If $q \,|\, r$ then $r = q\,s$ for some $s \in D$,

$$q = p\,r = p\,q\,s = q\,p\,s$$

so that $1 = p\,s$ and $p \in U(D)$, which is a contradiction. So $q \,|\, p$ and $p \sim q$ by (4) above.

(6) It is an easy exercise to check that for $a \sim a'$ and $b \sim b'$ in D we have

$$a \,|\, b \;\Leftrightarrow\; a' \,|\, b'.$$

(7) If p is prime and $p \sim q$ in D, then q is prime too. Indeed, if $p \in D$ is prime then $p \neq 0$ and $p \notin U(D)$ by definition. Then for $p \sim q$ we also have $q \neq 0$ and $q \notin U(D)$ by using Part (b) of our Lemma Now suppose that $q \,|\, ab$ for some $a, b \in D$. Then by (6) we also have $p \,|\, ab$. Since p is prime, then $p \,|\, a$ or $p \,|\, b$. Again by (6) we have $q \,|\, a$ or $q \,|\, b$ as needed.

(8) If a is irreducible and $a \sim b$ in D, then b is irreducible too. Indeed, if $a \in D$ is irreducible then $a \neq 0$ and $a \notin U(D)$ by definition. Then for $a \sim b$ we also have $b \neq 0$ and $b \notin U(D)$ by again using Part (b) of our Lemma Further, then $a = b\,u$ where $u \in U(D)$. Now suppose that $b = c\,d$ for some $c, d \in D$. Then

$$a = b\,u = (c\,d)\,u = c\,(d\,u)\,.$$

Since a is irreducible, then $c \in U(D)$ or $d\,u \in U(D)$. But if $d\,u \in U(D)$ here, then

$$d = (d\,u)\,u^{-1} \in U(D)\,.$$

Hence $c \in U(D)$ or $d \in U(D)$. Therefore b is irreducible.

Irreducible and prime elements (4-2)

Let D be any integral domain. Recall that an element $a \in D$ is called **irreducible** if $a \neq 0$, $a \notin U(D)$ and for any $b, c \in D$

$$a = b\,c \;\Rightarrow\; b \in U(D) \text{ or } c \in U(D)\,.$$

Also recall that an element $p \in D$ is **prime** if $p \neq 0$, $p \notin U(D)$ and for any $a, b \in D$

$$p \,|\, ab \;\Rightarrow\; p \,|\, a \text{ or } p \,|\, b\,.$$

Proposition

If $p \in D$ is prime, then p is irreducible.

Proof

If $p \in D$ is prime, then $p \neq 0$ and $p \notin U(D)$ by definition. Suppose that $p = b\,c$ for some $b, c \in D$. Then $p \,|\, bc$ so that $p \,|\, b$ or $p \,|\, c$. Suppose $p \,|\, b$. Then $b = p\,d$ for some $d \in D$ and

$$p = b\,c = p\,d\,c\,.$$

Then $1 = d\,c$. Hence $c \in U(D)$. Similarly, if $p \,|\, c$ then $b \in U(D)$. Thus p is irreducible. □

Remark

In the next section, we will show that the element $2 \in \mathbb{Z}[\sqrt{-3}\,]$ is irreducible but not prime. Hence the statement converse to the above Proposition is **not** true in general.

Examples

(1) Let $D = \mathbb{Z}$. We claim that then $p \in D$ is prime if and only if $p \in D$ is irreducible. Note that an element $p \in \mathbb{Z}$ is prime if and only if $|\,p\,|$ is prime in the sense of Number Theory. This is just because the prime numbers in $\mathbb{Z}$ are assumed to be positive. Now let $p \in \mathbb{Z}$ be irreducible. Then $p \neq 0$ and $p \notin U(\mathbb{Z}) = \{1, -1\}$. Moreover, if $p = b\,c$ with $b, c \in \mathbb{Z}$ then $b \in U(\mathbb{Z})$ or $c \in U(\mathbb{Z})$. Hence $b \in \{1, -1\}$ or $c \in \{1, -1\}$ respectively. Therefore up to a sign, $p \in \mathbb{Z}$ is prime in the sense of Number Theory. Hence p is also prime in the sense of Ring Theory. The converse statement holds true by our general Proposition

(2) Let $D = \mathbb{Z}[x]$. We claim that $x + b \in \mathbb{Z}[x]$ is irreducible for any $b \in \mathbb{Z}$. Indeed, if

$$x + b = f\,g$$

for some polynomials $f, g \in \mathbb{Z}[x]$ then

$$1 = \deg\,(x + b) = \deg f + \deg g$$

so that one of the degrees $\deg f, \deg g$ is 0. Suppose that $\deg f = 0$, then f is a constant polynomial, that is $f \in \mathbb{Z}$. Then $\deg g = 1$, that is $g = c\,x + d$ for $c, d \in \mathbb{Z}$ with $c \neq 0$. So

$$x + b = f\,(c\,x + d)$$

so that $1 = f\,c$ and hence $f \in U(\mathbb{Z}[x])$. Similarly, if $\deg g = 0$ then $g \in U(\mathbb{Z}[x])$.

(3) In the ring $\mathbb{Q}[x]$ the element $a\,x+b$ with $a,b\in\mathbb{Q}$ and $a\neq 0$ is irreducible. Indeed, let $a\,x+b=f\,g$ for $f,g\in\mathbb{Q}[x]$. Then again $\deg f=0$ while $\deg g=1$, or $\deg f=1$ while $\deg g=0$. Then $f\in\mathbb{Q}\setminus\{0\}$ or $g\in\mathbb{Q}\setminus\{0\}$ respectively. But $U(\mathbb{Q}[x])=U(\mathbb{Q})=\mathbb{Q}\setminus\{0\}$.

Note that the polynomial $ax+b$ with $a,b\in\mathbb{Z}$ is not necessarily irreducible in $\mathbb{Z}[x]$. For example, the polynomial $2x+4$ is not irreducible in $\mathbb{Z}[x]$. Indeed, $2x+4=2(x+2)$ where

$$2,x+2\notin U(\mathbb{Z}[x])=U(\mathbb{Z})=\{1,-1\}\,.$$

Unique Factorisation Theorem

Let D be any integral domain and $a\in D$. Suppose that

$$a=p_1\dots p_m=q_1\dots q_n$$

where p_i with $i=1,\dots,m$ and q_j with $j=1,\dots,n$ are prime elements of D . Then $m=n$ and we can relabel the q_j so that $p_i\sim q_i$ for each $i=1,\dots,m$. Hence a decomposition of $a\in D$ as a product of primes is **essentially unique**.

Proof

We will use the induction on m . First suppose that $m=1$. Then $p_1=q_1\dots q_n$. Since p_1 is prime, it is irreducible by our Proposition Hence $q_1\dots q_n$ is also irreducible. Suppose $n>1$. Since q_n is prime, it is not a unit. Then $q_1\dots q_{n-1}$ must be a unit. But then $q_1\dots q_{n-1}\,r=1$ for some $r\in D$, so that each q_j with $j<n$ is a unit. This is a contradiction, because each q_j is prime. Thus $n=1$ and $p_1=q_1$.

Now suppose that $m > 1$ and the statement of Theorem holds for $m-1$ instead of m. Let

$$p_1 \dots p_m = q_1 \dots q_n$$

where all factors are prime elements of D. Here $p_1 \mid q_1 \dots q_n$ and p_1 is prime. So $p_1 \mid q_j$ for some index j, by Remark (2) from the previous section. Without loss of generality, assume that $j = 1$. By Remark (5) then $p_1 \sim q_1$ so that $q_1 = p_1 \, u$ for some $u \in U(D)$. Then

$$p_1 \dots p_m = p_1 \, u \, q_2 \dots q_n$$

and by cancelling $p_1 \neq 0$,

$$p_2 \dots p_m = (u \, q_2) \, q_3 \dots q_n \, .$$

But $u \, q_2$ is prime by Remark (7) By our assumption, then $m-1 = n-1$ so that $m = n$, and by relabelling $q_2, q_3, \dots, q_m$ we get $p_2 \sim uq_2 \sim q_2$ and $p_i \sim q_i$ for $i = 3, \dots, m$. □

Remark

Suppose that an element $a \in D$ is irreducible but not prime. Then a does **not** decompose as a product of prime factors. Indeed, if it does then $a = p \, q$ where $p, q \in D$ and p is prime. Hence $p \notin U(D)$. But then $q \in U(D)$ because a is irreducible. Then $a \sim p$ and a is prime, a contradiction. For example, 2 does not decompose as a product of primes in $\mathbb{Z}[\sqrt{-3}\,]$.

Proposition

Let D be a PID and $p \in D$. Then p is irreducible if and only if p is prime.

Proof

We already proved that in any integral domain D, the prime elements are irreducible. Now let D be a PID and $p \in D$ be irreducible. Then $p \neq 0$ and $p \notin U(D)$. Suppose that $p \,|\, b\,c$ for some $b, c \in D$ so that $b\,c = p\,a$ for some $a \in D$. Consider the sum of principal ideals $p\,D$ and $b\,D$, that is

$$p\,D + b\,D = \{\, s\,p + t\,b \mid s, t \in D \,\}\,.$$

We know that the sum of ideals is an ideal. As D is a PID, the ideal $p\,D + b\,D$ is principal :

$$p\,D + b\,D = d\,D$$

for some $d \in D$. Then $p, b \in d\,D$. In particular, then $d \mid p$ so that $p = d\,q$ for some $q \in D$. Then d or q is a unit, because p is irreducible. Consider the two cases.

(a) If q is a unit, then $p \sim d$. But then our Remark (6) gives $p \,|\, b$, because $d \,|\, b$.

(b) Let d be a unit. Since $d \in p\,D + b\,D$, we have $d = s\,p + t\,b$ for some $s, t \in D$. Hence

$$c = d\,d^{-1}c = (s\,p + t\,b)\,d^{-1}c = s\,p\,d^{-1}c + t\,b\,c\,d^{-1} = p\,(s\,d^{-1}c + t\,a\,d^{-1})$$

where we use the equality $b\,c = p\,a$ obtained above. Thus $p \,|\, c$ in this case.

So in both cases (a) and (b), either $p \,|\, b$ or $p \,|\, c$. Hence p is prime by definition. $\square$

Examples of irreducible elements (4-3)

Let $d \in \mathbb{Z} \setminus \{1\}$ be **square free**, that is d is not divisible by p^2 for all prime numbers p. Note that then $d \neq 0$. Recall that the ring

$$\mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$ with the identity

$$1 = 1 + 0\sqrt{d}\,.$$

Hence the $+$ and $\times$ operations on $\mathbb{Z}[\sqrt{d}\,]$ are the usual

$$(a + b\sqrt{d}\,) + (c + e\sqrt{d}\,) = (a + c) + (b + e)\sqrt{d}$$

and

$$(a + b\sqrt{d}\,) \times (c + e\sqrt{d}\,) = (ac + bed\,) + (ae + bc)\sqrt{d}\,.$$

Definition

The **norm** on $\mathbb{Z}[\sqrt{d}\,]$ is the function $N : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{N}^0 = \mathbb{N} \cup \{0\}$ is defined by

$$N(a + b\sqrt{d}\,) = |\, a^2 - d\, b^2 \,|\,.$$

Remarks

(a) $N(a + b\sqrt{d}\,) = |\,(a + b\sqrt{d}\,)(a - b\sqrt{d}\,)\,|$

(b) If $d < 0$ then $N(a + b\sqrt{d}\,) = a^2 - d\, b^2\,.$

Proposition

(i) Any $z \in \mathbb{Z}[\sqrt{d}\,]$ has a **unique** expression as $a + b\sqrt{d}$ for some $a, b \in \mathbb{Z}$.

(ii) $N(z) = 0$ if and only if $z = 0$;

(iii) $N(z\,w) = N(z)\,N(w)$ for any $z, w \in \mathbb{Z}[\sqrt{d}\,]$.

(iv) $z \in \mathbb{Z}[\sqrt{d}\,]$ is a unit if and only if $N(z) = 1$.

Proof

(i) If $z = a + b\sqrt{d} = c + e\sqrt{d}$ for some $a, b, c, e \in \mathbb{Z}$ then

$$a - c = (e - b)\sqrt{d}\,,$$

and so

$$(a - c)^2 = (e - b)^2 d.$$

Suppose $e - b \neq 0$. Then $d > 1$ and d has a prime factor, say $p \in \mathbb{N}$. But then $p \,|\, (a - c)$, so that p occurs to an even power on the left hand side and an odd power on the right hand side, which a contradiction. Thus $e - b = 0$, so that $e = b$ and $a = c$.

(ii) Let $z = a + b\sqrt{d}$. By using Remark (a) and Part (i) of our Proposition, we have

$$\begin{aligned} N(z) = 0 \;&\Leftrightarrow\; |\, a^2 - d\,b^2 \,| = 0 \;\Leftrightarrow\; |\,(a + b\sqrt{d}\,)\,(a - b\sqrt{d}\,)\,| = 0 \\ &\Leftrightarrow\; (a + b\sqrt{d}\,)(\,a - b\sqrt{d}\,) = 0 \;\Leftrightarrow\; a + b\sqrt{d} \;= 0 \text{ or } a - b\sqrt{d} \;= 0 \\ &\Leftrightarrow\; a = b = 0 \;\Leftrightarrow\; z = 0. \end{aligned}$$

(iii) Let $z = a + b\sqrt{d}$ and $w = c + e\sqrt{d}$ for some $a, b, c, e \in \mathbb{Z}$ as above. Then

$$\begin{aligned} N(z\,w) &= N((a + b\sqrt{d}\,)(c + e\sqrt{d}\,)) \\ &= N((ac + bed) + (bc + ae)\sqrt{d}\,) \\ &= |\,(ac + bed)^2 - d\,(bc + ae)^2\,| \\ &= |\,a^2c^2 + 2acbed + b^2e^2d^2 - db^2c^2 - 2bcaed - da^2e^2\,| \\ &= |\,a^2c^2 + b^2e^2d^2 - db^2c^2 - da^2e^2\,| \\ &= |\,(a^2 - d\,b^2)\,(c^2 - d\,e^2)\,| \\ &= |\,a^2 - d\,b^2\,| \times |\,c^2 - d\,e^2\,| \\ &= N(z)N(w)\,. \end{aligned}$$

(iv) If $z \in U(\mathbb{Z}[\sqrt{d}\,])$ then $z\,w = 1$ for some $w \in \mathbb{Z}[\sqrt{d}\,]$. Then by (iii)

$$1 = N(1) = N(z\,w) = N(z)\,N(w),$$

so $N(z) = 1$ and $N(w) = 1$. Conversely, let $z = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. If $N(z) = 1$ then

$$|\,a^2 - d\,b^2\,| = 1,$$

so that

$$|(a + b\sqrt{d}\,)\,(a - b\sqrt{d}\,)| = 1$$

giving

$$(a + b\sqrt{d}\,)\,(\pm(a - b\sqrt{d}\,)) = 1\,,$$

so that $z \in U(\mathbb{Z}[\sqrt{d}\,])$. □

Theorem

Let $d \in \mathbb{Z} \setminus \{1\}$ be square free. Let $i = \sqrt{-1}$ as usual. The units in the ring $\mathbb{Z}[\sqrt{d}\,]$ are:

$$\begin{aligned}
&1, -1, i, -i \text{ if } d = -1\,;\\
&1, -1 \text{ if } d < -1\,;\\
&1, -1 \text{ and infinitely many others if } d > 1\,.
\end{aligned}$$

Proof

First consider the case when $d = -1$. Let $z = a + i\,b$ where $a, b \in \mathbb{Z}$. Then

$$\begin{aligned}
z \in U(\mathbb{Z}[i]) &\Leftrightarrow N(z) = 1\\
&\Leftrightarrow a^2 + b^2 = 1\\
&\Leftrightarrow a = \pm 1\,,\ b = 0 \text{ or } a = 0\,,\ b = \pm 1\,.
\end{aligned}$$

Hence the units of the ring $\mathbb{Z}[i]$ of Gaussian integers are ± 1 and $\pm\, i$.

Next consider the case when $d < -1$. Let $z = a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$. Then

$$\begin{aligned}
z \in U(\mathbb{Z}[\sqrt{d}\,]) &\Leftrightarrow N(z) = 1\\
&\Leftrightarrow a^2 - d\,b^2 = 1\\
&\Leftrightarrow a = \pm 1\,,\ b = 0\,.
\end{aligned}$$

Finally, consider $d > 1$. Then $1, -1 \in U(\mathbb{Z}[\sqrt{d}\,])$. Further, $z = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ is a unit in $\mathbb{Z}[\sqrt{d}\,]$ if and only if $|\, a^2 - d\,b^2\,| = 1$. By Number Theory, the latter equation has a solution $(a, b) \neq (\pm 1, 0)$. Then $z = a + b\sqrt{d}$ and also $z^2, z^3, \ldots$ are distinct units. $\square$

Examples

(1) In the ring $\mathbb{Z}[\sqrt{3}\,]$ the element $z = 2 - \sqrt{3}$ is a unit, since $N(z) = |\,2^2 - 3 \times 1^2\,| = 1$. Since $z\,(2 + \sqrt{3}\,) = 1$, here $z^{-1} = 2 + \sqrt{3}$. But $z \neq \pm 1$ and $z, z^2, z^3, \ldots$ are distinct units.

(2) Consider the ring $\mathbb{Z}[\sqrt{-3}\,]$. Note that if $z = a + b\sqrt{-3}$ then $N(z) = a^2 + 3\,b^2 \neq 2$. Let $w \in \mathbb{Z}[\sqrt{-3}\,]$ be such that $N(w) = 4$. We claim that w is irreducible. Indeed, since $N(w) \neq 0, 1$ our Proposition implies that w is not zero and non a unit. For $x, y \in \mathbb{Z}[\sqrt{-3}\,]$

$$\begin{aligned} w = x\,y \;\; &\Rightarrow \;\; N(w) = N(x)\,N(y) \\ &\Rightarrow \;\; N(x) = 1\,,\; N(y) = 4 \;\;\text{ or }\;\; N(x) = 4\,,\; N(y) = 1 \\ &\Rightarrow \;\; x \in U(\mathbb{Z}[\sqrt{-3}\,]) \;\;\text{ or }\;\; y \in U(\mathbb{Z}[\sqrt{-3}\,])\,. \end{aligned}$$

The elements $1 + \sqrt{-3}\,, 1 - \sqrt{-3}\,,\; 2 \in \mathbb{Z}[\sqrt{-3}\,]$ have norm 4 and thus are irreducible. Now

$$(1 + \sqrt{-3}\,) \times (1 - \sqrt{-3}\,) = 4 = 2 \times 2\,.$$

Since the units of $\mathbb{Z}[\sqrt{-3}\,]$ are only 1 and -1, we have $2 \not\sim 1 + \sqrt{-3}$ and $2 \not\sim 1 - \sqrt{-3}$. So the decomposition of $4 \in \mathbb{Z}[\sqrt{-3}\,]$ as a product of irreducibles is essentially **not** unique.

There is no contradiction here with the Unique Factorisation Theorem because the elements $1 + \sqrt{-3}\,, 1 - \sqrt{-3}\,,\; 2$ are **not** prime. For instance, consider $1 + \sqrt{-3}$. It divides $4 = 2 \times 2$. If it was prime, then it would also divide 2 so that $2 = (1 + \sqrt{-3})\,z$ for some $z \in \mathbb{Z}[\sqrt{-3}\,]$ Taking the norms gives $N(z) = 1$, so that z is a unit and $z = \pm\,1$. This is a contradiction. Hence $1 + \sqrt{-3}$ is not prime. Similarly, the elements $1 - \sqrt{-3}$ and 2 are not prime.

Unique factorisation domains (4-4)

Let D be an integral domain. It is called a **unique factorisation domain (UFD)** if :

(i) every element $a \in D \setminus \{0\}$ with $a \notin U(D)$ can be written as $a = p_1 \, p_2 \ldots p_m$ where $m \in \mathbb{N}$ and all p_i with $i = 1, \ldots m$ are irreducible in D ;

(ii) such a decomposition of a is **essentially unique**, that is if

$$a = p_1 \, p_2 \ldots p_m = q_1 \, q_2 \ldots q_n$$

where all p_i with $i = 1, \ldots m$ and all q_j with $j = 1, \ldots n$ are irreducible in D , then $m = n$ and we can relabel the q_j so that $p_i \sim q_i$ for each $i = 1, \ldots, m$.

Remark

If all irreducibles in D are prime, then (ii) holds by the Unique Factorisation Theorem

Examples

(1) The ring $\mathbb{Z}$ is a UFD. Indeed, the ring $\mathbb{Z}$ is an integral domain with $U(\mathbb{Z}) = \{1, -1\}$. The irreducibles in $\mathbb{Z}$ are the prime numbers in the sense of Number Theory, and also their negatives. Every $z \in \mathbb{Z} \setminus \{0, 1, -1\}$ can be written as product of these. So we have (i). All irreducibles in $\mathbb{Z}$ are prime in the sense of Ring Theory, so (ii) holds by the above Remark.

(2) The ring $\mathbb{Z}[\sqrt{-3}]$ is not a UFD because (ii) fails, please see the end of previous section.

Proposition

Let D be a UFD and $p \in D$. Then p is irreducible if and only if p is prime.

Proof

We already proved that in any integral domain D, the prime elements are irreducible. Now let D be a UFD and $p \in D$ be irreducible. Then $p \neq 0$ and $p \notin U(D)$. Suppose that $p \,|\, a\,b$ for some $a, b \in D$ so that $a\,b = p\,c$ for some $c \in D$. If $a = 0$ then $p \,|\, a$. If $b = 0$ then $p \,|\, b$. Suppose that $a, b \neq 0$. Then $a\,b \neq 0$, because $ZD(D) = \{0\}$. Hence $c \neq 0$ as well.

If $a \in U(D)$ then $p \,|\, b$ by Remark (6) Similarly, if $b \in U(D)$ then $p \,|\, a$. Let $a, b \notin U(D)$. Then $c \notin U(D)$ by Remark (8) because p is irreducible. Now by (i) we can write

$$a = a_1\, p_2 \ldots p_m \quad \text{and} \quad b = q_1\, q_2 \ldots q_n$$

where all p_i with $i = 1, \ldots m$ and all q_j with $j = 1, \ldots n$ are irreducible in D. Then

$$p\,c = a\,b = p_1\, p_2 \ldots p_m\, q_1\, q_2 \ldots q_n$$

is a factorisation of $p\,c$ as a product of $m+n$ irreducible elements. But c also factorises as a product of irreducible elements. Due to (ii) then c must have exactly $m+n-1$ irreducible factors, while $p \sim p_i$ or $p \sim q_j$ for one of the indices i or j. Then $p \,|\, a$ or $p \,|\, b$ respectively. Hence p is prime by definition. □

Theorem

Let D be a principal ideal domain. Then D is a unique factorisation domain.

Proof

By the Proposition, any element of D is irreducible if and only if it is prime. By the Unique Factorisation Theorem any decomposition into a product of primes is essentially unique. Therefore in our D, any decomposition into a product of irreducibles is essentially unique. It remains to show that every non-zero, non-unit element of D is a product of irreducibles.

We will need the following general fact. If $I_1, I_2, \ldots$ are ideals of any ring R such that

$$I_1 \subseteq I_2 \subseteq \ldots \,,$$

then an ideal of R is their union

$$I = \bigcup_{i \in \mathbb{N}} I_i \,.$$

Suppose that $a \in D \setminus \{0\}$ and $a \notin U(D)$ but a is **not** a product of irreducibles. Then a is not irreducible, so $a = a_1 \, b_1$ where $a_1, b_1 \in D \setminus \{0\}$ are not units and not both products of irreducibles. Say a_1 is not a product of irreducibles. Then a_1 is not irreducible, so $a_1 = a_2 \, b_2$ for some $a_2, b_2 \in D \setminus \{0\}$ not units and not both products of irreducibles. Say a_2 is not a product of irreducibles. Continuing in this manner we obtain non-zero non-unit elements $a_1, b_1, a_2, b_2, \ldots$ such that $a_i = a_{i+1} \, b_{i+1}$ and a_i not a product of irreducibles for any index i .

Since $a_i = a_{i+1}\, b_{i+1}$, we have $a_i \in a_{i+1}D$ and so so that $a_i\, D \subseteq a_{i+1}D$. So we have

$$a_1 D \subseteq a_2 D \subseteq \dots .$$

Let

$$I = \bigcup_{i \in \mathbb{N}} a_i\, D\,.$$

By the above general fact, I is an ideal of D. But D is a PID, so $I = c\, D$ for some $c \in D$. In particular, we have

$$c \in c\, D = I = \bigcup_{i \in \mathbb{N}} a_i\, D\,,$$

so there exists $n \in \mathbb{N}$ with $c \in a_n D$. Then

$$a_n D \subseteq I = c\, D \subseteq a_n D\,,$$

giving

$$I = a_n D\,.$$

Then $a_{n+1} \in a_n D$, so that $a_{n+1} = a_n\, b$ for some $b \in D$. Hence

$$a_n = a_{n+1}\, b_{n+1} = a_n\, b\, b_{n+1}\,.$$

Cancelling a_n here gives

$$1 = b\, b_{n+1}$$

so that b_{n+1} is a unit. This is a contradiction, showing that a is a product of irreducibles. □

Examples

(1) The rings $\mathbb{Z}$ and $F[x]$ for any field F are PID, hence UFD.

(2) It is possible although hard to prove that the ring $\mathbb{Z}[x]$ is a UFD. Let us prove that $\mathbb{Z}[x]$ is **not** a PID. In particular, this will show that the converse to our Theorem is **not** true.

Recall that if I, J are ideals of any ring R, then

$$I + J = \{a + b : a \in I, b \in J\}$$

is an ideal of R. Now choose $R = \mathbb{Z}[x]$. Let $I = 2\,\mathbb{Z}[x]$ and $J = x\,\mathbb{Z}[x]$. Suppose that

$$I + J = f\,\mathbb{Z}[x]$$

for some $f \in \mathbb{Z}[x]$. Then

$$2 = 2 \times 1 + x \times 0 \in I + J$$

so that $2 = f\,g$ for some $g \in \mathbb{Z}[x]$. Hence $\deg f = \deg g = 0$ and $f \in \mathbb{Z}$ is a constant. Also

$$x = 2 \times 0 + x \times 1 \in I + J$$

so that $x = f\,h$ for some $h \in \mathbb{Z}[x]$. Since f is a constant, here we must have $f = \pm 1$. This implies that $1 \in I + J$ so that

$$1 = 2\,u + x\,v$$

for some $u, v \in \mathbb{Z}[x]$. Let $a \in \mathbb{Z}$ be the constant term of the polynomial u. Then $1 = 2\,a$, which is contradiction. Hence the ideal $2\,\mathbb{Z}[x] + x\,\mathbb{Z}[x]$ of $\mathbb{Z}[x]$ is not principal.

Prime ideals (5-1)

Let R be any ring. We say that an ideal I of R is **proper** if $I \neq R$. An ideal P of a ring R is called **prime** if P is proper and for any $a, b \in R$

$$ab \in P \;\Rightarrow\; a \in P \text{ or } b \in P\,.$$

Examples

(1) If $R \neq \{0\}$ but $ZD(R) = \{0\}$, then $\{0\}$ is prime since $ab = 0$ implies $a = 0$ or $b = 0$.

(2) Let $R = \mathbb{Z}$ and I be a non-zero ideal of $\mathbb{Z}$. Then $I = n\,\mathbb{Z}$ for some $n \in \mathbb{N}$. Let us show that I is prime if and only if n is a prime number. If $n = 1$ then $I = \mathbb{Z}$ so is not prime. Suppose n is composite, so that $n = ab$ for some $a, b \in \mathbb{N}$ where $1 < a < n$ and $1 < b < n$. Then $ab \in I$ but neither a nor b lies in I, as $z \in I \;\Leftrightarrow\; n \,|\, z$. So I is not prime in this case. Conversely, if $n = p$ is prime then the ideal $I = p\,\mathbb{Z}$ is prime, because for any $a, b \in \mathbb{Z}$

$$ab \in I \;\Rightarrow\; p \,|\, ab \;\Rightarrow\; p \,|\, a \text{ or } p \,|\, b \;\Rightarrow\; a \in I \text{ or } b \in I\,.$$

Theorem

Let P be a proper ideal of R. Then P is prime if and only if $ZD(R/P) = \{0\}$.

Proof

Suppose that $ZD(R/P) = \{0\}$. Let $a, b \in R$ be such that $ab \in P$. In the factor ring R/P

$$(a + P)(b + P) = ab + P = P = 0 + P\,.$$

It follows that $a + P = P$ or $b + P = P$. Thus either $a \in P$ or $b \in P$ and P is prime.

Conversely, suppose that P is a prime ideal. Let $a + P, b + P \in R/P$ and

$$(a + P)(b + P) = P\,.$$

Then

$$ab + P = P$$

so that $ab \in P$. But the ideal P is prime, so that either $a \in P$ or $b \in P$. Hence $a + P = P$ or $b + P = P$. Thus $ZD(R/P) = \{0\}$. □

Corollary

Let R be a commutative ring with an identity 1. Then P is prime if and only if the ring R/P is an integral domain.

Proof

Since R is commutative, the ring R/P is also commutative. Let us show that $1 + P \in R/P$ is an identity if and only if the ideal P is proper. Indeed,

$$1 + P \neq 0 + P \;\Leftrightarrow\; 1 \notin P \;\Leftrightarrow\; P \neq R\,.$$

Also for any $a \in R$

$$(1 + P)(a + P) = 1a + P = a + P\,.$$

Using the definition of an integral domain, the Corollary now follows from our Theorem □

Proposition

Let D be an integral domain. Then for any $a \in D$ we have:

(i) $aD = \{0\}$ if and only if $a = 0\,;$
(ii) $aD = D$ if and only if $a \in U(D)\,;$
(iii) aD is a non-zero prime ideal of D if and only if the element a is prime.

Proof

(i) If $a = 0$ then $aD = \{0\}$. Conversely, if $a \neq 0$ then $aD \neq \{0\}$ because $a = a1 \in aD$.

(ii) Suppose that $aD = D$. Then $1 \in aD$. So $1 = ab$ for some $b \in D$. Hence $a \in U(D)$. Conversely, if $a \in U(D)$ then for any $d \in D$ we have

$$d = a(a^{-1}d) \in aD,$$

so that $d \in aD$. Hence $aD = D$.

(iii) Due to (i) we have $aD \neq \{0\}$ if and only if $a \neq 0$. Further, due to (ii) we have $aD \neq D$ if and only if $a \notin U(D)$. Now let $a \neq 0\,, a \notin U(D)$. Then

$$\begin{aligned} a \text{ is prime} \quad &\Leftrightarrow \quad (\ a \,|\, bc \ \text{ implies that } a \,|\, b \text{ or } a \,|\, c\ ) \\ &\Leftrightarrow \quad (\ bc = ad \ \text{ for some } d \in D \ \text{ imples that } b = au \text{ or } c = av\ ) \\ &\Leftrightarrow \quad (\ bc \in aD \ \text{ imples that } b \in aD \text{ or } c \in aD\ ) \\ &\Leftrightarrow \quad (\ aD \text{ is prime. })\qquad \square \end{aligned}$$

Maximal ideals (5-2)

Let R be any ring. Recall that an ideal I of R is **proper** if $I \neq R$. An ideal M of the ring R is called **maximal** if M is proper and for any ideal I of R

$$M \subseteq I \subseteq R \quad \Rightarrow \quad I = M \text{ or } I = R\,.$$

The above means that there is **no** ideal I of R with $M \subset I \subset R$.

Proposition

Let D be an integral domain. Then for any $a \in D \setminus \{0\}$:

(i) if the ideal aD of D is maximal, then a is irreducible;

(ii) if D is a PID and a is irreducible, then the ideal aD is maximal.

Proof

(i) Suppose that aD is maximal. Then $aD \neq D$, so by the previous Proposition $a \notin U(D)$. If $a = bc$ then $aD = bcD \subseteq bD$ and so $bD = aD$ or $bD = D$. In the latter case, $b \in U(D)$ by the previous Proposition In the former, $b \in bD = aD$ so that $b = ad$ for some $d \in D$. Then $a = bc = adc$. Cancelling a gives $1 = dc$, so that $c \in U(D)$. Hence a is irreducible.

(ii) If a is irreducible then $a \notin U(D)$, so $aD \neq D$. Let I be an ideal such that $aD \subseteq I \subseteq D$. We have $I = bD$ since D is a PID. Now $aD \subseteq bD$ and so $a = bc$ for some $c \in D$. This gives $b \in U(D)$ or $c \in U(D)$. In the former case, $bD = D$. In the latter case, $b = ac^{-1} \in aD$ and so $bD \subseteq aD$. Hence $bD = aD$. Thus the ideal aD is maximal. □

Corollary

Let D be PID and I be a non-zero ideal. Then I is maximal if and only if I is prime.

Proof

As D is a PID, there exists $a \in D$ such that $I = aD$. Then $a \neq 0$ because aD is non-zero, please see the previous lecture. The non-zero ideal aD is prime if and only if the element a is prime, see again the previous lecture. By our Proposition the ideal aD is maximal if and only if a is irreducible. But we know that because D is a PID, the element a is irreducible if and only if a is prime. Hence we get the Corollary. □

Theorem

Let R be a commutative ring with an identity 1 and let M be an ideal of R. Then the ideal M is maximal if and only if R/M is a field.

Proof

Suppose that R/M is a field. Then $|R/M| > 1$ because the zero and the identity elements are different in any field. Thus $M \neq R$. Let I be an ideal such that $M \subset I \subseteq R$. Let $x \in I$ but $x \notin M$, so that the coset $x + M \neq 0 + M$. Since R/M is a field, there exists another coset $y + M$ such that $(x + M)(y + M) = 1 + M$. This gives $xy + M = 1 + M$ and so $1 = xy + z$ for some $y \in R$ and $z \in M$. But $xy \in I$ while $z \in M \subset I$. This gives $1 \in I$ and hence $I = R$. Thus M is maximal.

Conversely, suppose that M is maximal. Then $M \neq R$ so that $|R/M| > 1$ and R/M is a commutative ring with an identity. Let $a + M \neq M$ in R/M, then $a \notin M$. Consider $I = M + aR$. We have I is an ideal, $M \subseteq I$ and $a = a1 \in I$. Hence $M \subset I$. Then $I = R$, because M is maximal. This gives that $1 = c + ab$ for some $b \in R$ and $c \in M$. Hence

$$(a + M)(b + M) = ab + M = 1 + M,$$

so that $a + M \in R/M$ is invertible and R/M is a field. □

Corollary

Let R be a commutative ring with an identity 1 and let P be an ideal of R. If P is maximal, then P is prime.

Proof

If P is maximal, then R/P is a field by our Theorem. In particular, then R/P is an integral domain. Hence P is prime by the Corollary in the previous lecture. □

Example

Suppose that D is a PID, for instance $D = F[x]$ where F is a field. Let $a \in D$ and $I = aD$. If $a = 0$ then $I = \{0\}$ then $D/I \cong D$. If $a \in U(D)$ then $I = D$ and $D/I = \{0\}$. Suppose that $a \neq 0$ and $a \notin U(D)$, then $\{0\} \subset I = aD \subset D$. If the element $a \in D$ is irreducible, then I is maximal by our Proposition Then $D/I = D/aD$ is a field by our Theorem

Irreducible polynomials (5-3)

Let F be a field. We know that $F[x]$ is a PID and so for any polynomial $f \in F[x]$

$$f \text{ is prime} \quad \Leftrightarrow \quad f \text{ is irreducible}$$

by the Proposition we have proved for any PID. Note that f is constant if and only if either $f = 0$ in which case f has no degree at all, or f is a unit in which case f has degree 0. Hence f is irreducible in $F[x]$ if and and only if f is **not** a constant and for any $g, h \in F[x]$

$$f = g\,h \quad \Rightarrow \quad g \text{ or } h \text{ is a (non-zero) constant.}$$

Lemma 1

If $f \in F[x]$ and $\deg f = 1$, then f is irreducible.

Proof

We have $f = ax + b$ where $a, b \in F$ and $a \neq 0$. Clearly f is not a constant. If $f = g\,h$ then

$$1 = \deg f = \deg(g\,h) = \deg g + \deg h\,.$$

Therefore one of g, h has degree 0 and hence is a constant. Thus f is irreducible. □

We say that f has a **root** in F if there exists $a \in F$ such that the substitution $f(a) = 0$.

Lemma 2

Let $f \in F[x]$ with $\deg f = 2$ or 3. Then f is irreducible if and only if f has **no** root in F.

Proof

Suppose that f has a root $a \in F$. By Question 8 of Problem Sheet II we have $f = (x - a)\, g$ for some $g \in F[x]$. Here $\deg g = 1$ or 2 because $\deg(x - a) = 1$. Hence f is not irreducible.

Conversely, suppose that f is not irreducible. Then $f = u\, v$ where u and v are not constants. Hence $\deg u \geqslant 1$ and $\deg v \geqslant 1$. We also have

$$\deg f = \deg(uv) = \deg u + \deg v\,.$$

If $\deg f = 2$ then $\deg u = \deg v = 1$. If $\deg f = 3$ then $\deg u = 1\,, \deg v = 2$ or vice versa.

Suppose that $\deg u = 1$, so that $u = cx + d$ where $c, d \in F$ and $c \neq 0$. Then

$$f = (cx + d)\, v = c(x + c^{-1}d)\, v$$

so that $-\,c^{-1}d$ is a root of f. The case of $\deg v = 1$ is very similar. □

Proposition

Let $f \in F[x]$ be irreducible. Put $I = f F[x]$. Then $F[x]\,/I$ is a field. Moreover, the map $\theta : F \to F[x]\,/I$ given by

$$\theta : a \mapsto a + I$$

is a one-to-one homomorphism.

Proof

By the Proposition from the previous lecture, the ideal $I = fF[x]$ of $F[x]$ is maximal. Then by the Theorem from the same lecture, the factor ring $F[x]\,/I$ is a field.

The map θ is a homomorphism by the definition of a factor ring. Furthermore for $a, b \in F$

$$\begin{aligned}\theta(a) = \theta(b) &\Leftrightarrow a + I = b + I \\ &\Leftrightarrow a - b \in I = f\,F[x] \\ &\Leftrightarrow a - b = f\,g \text{ for some } g \in F[x] \\ &\Leftrightarrow a - b = 0 \text{ since } f \text{ is not a constant} \\ &\Leftrightarrow a = b \qquad \square\end{aligned}$$

Example

Suppose that $f = cx + d$ where $c, d \in F$ and $c \neq 0$. Then f is irreducible by Lemma 1 By the last Proposition the factor ring $F[x]\,/fF[x]$ is a field. We claim that $F[x]\,/fF[x] \cong F$.

We already know that for $I = fF[x]$ the map

$$\theta : F \to F[x]\,/I : a \mapsto a + I$$

is a one-to-one homomorphism. Let us show that θ is also onto, hence a ring isomorphism. Indeed, using the Division Algorithm for $F[x]$, any polynomial $u \in F[x]$ can be written as

$$u = (cx + d)\,q + r$$

where the remainder $r \in F$ is a constant. Here $(cx + d)\,q \in I$. Hence $u + I = r + I$.

Theorem

Let $f \in F[x]$ be irreducible with $\deg f = n$. Put $I = f F[x]$.

(i) The factor ring $F[x]\,/I$ is a field.

(ii) $F[x]\,/I$ is also a vector space of dimension n over the field F under the operations

$$(u + I) + (v + I) = (u + v) + I\,,$$

$$a \times (u + I) = a\,u + I$$

for any $u, v \in F[x]$ and $a \in F$.

(iii) The vector space $F[x]\,/I$ has a basis

$$1 + I,\;\; x + I,\;\; \ldots\;,\;\; x^{n-1} + I\,.$$

(iv) If $|F| < \infty$ then

$$|\,F[x]\,/I\,| = |F|^{\,n}\,.$$

(v) In particular, if $F = \mathbb{Z}\,/p\,\mathbb{Z}$ for a prime number p , then

$$|\,(\mathbb{Z}\,/p\,\mathbb{Z})\,[x]\,/I\,| = p^n\,.$$

Proof

The first claim of the theorem holds true by our Proposition Further, observe that

$$a \times (u + I) = a\,u + I = (a + I)(u + I)\,.$$

It is then easy to check all the vector space axioms, by using the ring axioms for $F[x]\,/I$.

Now let $u \in F[x]$. Then

$$u = f\,q + r$$

where either $r = 0$ or $r \neq 0$ with $\deg r < \deg f = n$. Then

$$u - r = f\,q \in I$$

so $u + I = r + I$. Write

$$r = a_0 + a_1\,x + \ldots + a_{n-1}\,x^{n-1}$$

where $a_0\,, a_1\,, \ldots, a_{n-1} \in F$. By using the equality $u + I = r + I$ we get

$$\begin{aligned} F[x]\,/I &= \{\,(a_0 + a_1\,x + \ldots + a_{n-1}\,x^{n-1}) + I : a_i \in F\,\} \\ &= \{\,a_0\,(1 + I) + a_1\,(x + I) + \ldots + a_{n-1}\,(x^{n-1} + I) : a_i \in F\,\} \end{aligned}$$

so that the n cosets

$$1 + I, x + I, \ldots, x^{n-1} + I$$

span $F[x]\,/I$. On the other hand, if

$$a_0\,(1 + I) + a_1\,(x + I) + \ldots + a_{n-1}\,(x^{n-1} + I) = I$$

then

$$(a_0 + a_1\,x + \ldots + a_{n-1}\,x^{n-1}) + I = I$$

and

$$a_0 + a_1\,x + \ldots + a_{n-1}\,x^{n-1} = f\,g$$

for some $g \in F[x]$. But $\deg f = n$, so this is only possible if $g = 0$ and hence

$$a_0 + a_1\,x + \ldots + a_{n-1}\,x^{n-1} = 0\,.$$

Then

$$a_0 = a_1 = \ldots = a_{n-1} = 0\,.$$

Hence the n cosets

$$1 + I, x + I, \ldots, x^{n-1} + I$$

are linearly independent over F and so form a basis for $F[x]/I$.

We know that a vector space over F of dimension n is linearly isomorphic to

$$F^{\,n} = \{\,(\,a_0\,, a_1\,, \ldots, a_{n-1}\,) : a_i \in F\,\}\,.$$

Hence if the field F is finite with $|F|$ elements, then $|\,F[x]\,/I\,| = |F|^{\,n}\,.$ □

Classification Theorem (without proof)

(i) The multiplicative group of all units (the non-zero elements) of any finite field is cyclic.
(ii) All finite fields with the same number of elements are isomorphic to each other as rings.
(iii) The number of elements of a finite field equals p^n for some $n \in \mathbb{N}$ and a prime $p \in \mathbb{N}$.
(iv) For any $n \in \mathbb{N}$ and a prime $p \in \mathbb{N}$ there is an irreducible $f \in (\mathbb{Z}\,/p\,\mathbb{Z})\,[x]$ of degree n.

Remark

Part (iv) of the Classification Theorem implies that for any $n \in \mathbb{N}$ and a prime $p \in \mathbb{N}$ there is a field with p^n elements. It can be constructed as $(\mathbb{Z}\,/p\,\mathbb{Z})\,[x]\,/I$ where $I = f\,(\mathbb{Z}\,/p\,\mathbb{Z})\,[x]\,.$

Examples of irreducible polynomials (5-4)

Let F be a field and $f \in F[x]$ be irreducible. Consider the field $F[x]\,/I$ where $I = f\,F[x]$. Let $X = x + I$. Then for any $g = b_0 + b_1\,x + \ldots + b_m\,x^m \in F[x]$ its coset in $F[x]\,/I$ equals

$$g(X) = b_0 + b_1(x+I) + \ldots + b_m(x+I)^m\,.$$

Example 1

Let $F = \mathbb{Z}\,/2\,\mathbb{Z}$ and $f = x^2 + x + [1]$. Then f is irreducible in $F[x]$. Indeed, here $\deg f = 2$. By Lemma 2 the polynomial f is irreducible if and only if f has no root in F. But we have $f([0]) = f([1]) = [1] \neq [0]$. In fact f is the **only** irreducible polynomial of degree 2 in $F[x]$.

The field $F[x]\,/I$ has $2^2 = 4$ elements. They are the cosets

$$[0] + I,\;\; [1] + I,\;\; x + I,\;\; (\,[1] + x\,) + I\,.$$

The cosets $[0] + I$ and $[1] + I$ are the 0 and 1 of the ring $F[x]\,/I$. Let $X = x + I$. Then the elements of $F[x]\,/I$ can be written as $0, 1, X, X+1$. Calculating their addition is easy:

$+$	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

To calculate their multiplication, note that $x^2 - (\,x + [1]\,) = x^2 + x + [1] \in I$. Therefore

$$X^2 = (x+I)^2 = x^2 + I = (\,x + [1]\,) + I = (x+I) + (\,[1] + I\,) = X + 1\,.$$

By using this,

$$X(X+1) = X^2 + X = X + 1 + X = 1\,.$$

Hence we get

$\times$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

Example 2

Let $F = \mathbb{Q}$ and $f = x^3 - 2$. Then f is irreducible in $\mathbb{Q}[x]$. This again follows from Lemma 2 because $\deg f = 3$ and f has no root in $\mathbb{Q}$. Here we used the fact that $2^{\frac{1}{3}} \in \mathbb{R}$ is irrational. By our Theorem the set $\mathbb{Q}[x]\,/I$ is also a vector space of dimension 3 over $\mathbb{Q}$ with a basis

$$1 + I,\ x + I,\ x^2 + I\,.$$

Let $X = x + I$. For $a \in \mathbb{Q}$ denote $a + I$ by $\widetilde{a}$. Then the basis elements of the vector space $\mathbb{Q}[x]\,/I$ can be written as $\widetilde{1}, X, X^2$. Here $\widetilde{1} \times X = X$ and $\widetilde{1} \times X^2 = X^2$. Since $x^3 - 2 \in I$,

$$X \times X^2 = X^3 = (x+I)^3 = x^3 + I = 2 + I = \widetilde{2} \quad \text{and} \quad X^2 \times X^2 = X^4 = X^3 \times X = 2\,X\,.$$

Characteristic of rings and fields (5-5)

Let R be a ring with identity 1. Let C be the subset of R consisting of all elements $z\,1$ where $z \in \mathbb{Z}$. Note that they are not all different in general. Explicitly, these elements are

$$\ldots, (-2)\,1\,, (-1)\,1\,, (0)\,1\,, (1)\,1\,, (2)\,1\,, \ldots$$

Here $(0)\,1 = 0$ is the zero element of R, while for $z \in \mathbb{N}$

$$z\,1 = \underbrace{1 + \ldots + 1}_{z \text{ times}} \quad \text{and} \quad (-z)\,1 = \underbrace{(-1) + \ldots + (-1)}_{z \text{ times}}\,.$$

For example, if $R = \mathbb{R}$ or $R = \mathbb{C}$ then $C = \mathbb{Z}$. However, if $R = \mathbb{Z}/n\,\mathbb{Z}$ then $C = \mathbb{Z}/n\,\mathbb{Z}$.

Proposition

Let R be a ring with an identity 1. Then C is a subring of R.

Proof

We have $0 \in C$ by definition. For any $z\,1 \in C$ we also have $-z\,1 \in C$. Further, for any $z, w \in \mathbb{Z}$ we can check that $z\,1 + w\,1 = (z + w)\,1$ and $(z\,1)(w\,1) = (zw)\,1$. Hence the subset $C \subseteq R$ is closed with respect to addition and multiplication. □

Suppose that R is an integral domain. Consider the subset $C \subseteq R$ as an addititive group. This is a cyclic group generated by the element $1 \in C$. If the group C is finite, then the **characteristic** $\operatorname{char} R = |C|$. However, if the group C is infinite, then we set $\operatorname{char} R = 0$.

Note that if C is infinite then by Group Theory all elements $z\,1$ of R with $z \in \mathbb{Z}$ must be different, so that $C = \mathbb{Z}$. If C finite, then $C = \mathbb{Z}\,/n\,\mathbb{Z}$ where $n = |C|$. Moreover, then

$$\operatorname{char} R = |C| = \min\{\, z : z > 0 \ \text{ and } \ z\,1 = 0 \ \text{ in } \ C \,\}\,.$$

Theorem

The characteristic $\operatorname{char} R$ is a prime number or 0.

Proof

If the group C is infinite then $\operatorname{char} R = 0$. Suppose that C is finite but $|C| = k\,l$ where $k, l \in \mathbb{N}$ and $k, l > 1$. As in the proof of the last Proposition we have the equalities in R

$$(k\,1)(l\,1) = (k\,l)\,1 = |C| \cdot 1 = 0\,.$$

Since R is an integral domain, we get $k\,1 = 0$ or $l\,1 = 0$. But here $k, l < |C|$. This contradicts to $|C|$ being the minimal $z > 0$ such that $z\,1 = 0$ in C. Hence $|C|$ is prime. □

Now let $z \in \mathbb{Z}$ and $b \in R$. Then we have defined the element $z\,b \in C$. By using the equality $(z\,a)\,(w\,b) = (z\,w)\,(a\,b)$ with $a = 1 \in R$ and $w = 1 \in \mathbb{Z}$

$$(z\,1)\,b = (z\,1)(1\,b) = z\,(1\,b) = z\,b\,.$$

Suppose that $b \neq 0$. If $\operatorname{char} R = 0$ then $z\,b = 0 \ \Leftrightarrow \ (z\,1)\,b = 0 \ \Leftrightarrow \ z\,1 = 0 \ \Leftrightarrow \ z = 0$. However, if $\operatorname{char} R = p$ then $z\,b = 0 \ \Leftrightarrow \ (z\,1)\,b = 0 \ \Leftrightarrow \ z\,1 = 0 \ \Leftrightarrow \ p \,|\, z$.

Examples

(1) The ring $\mathbb{Z}$ and the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are integral domains. They all have characteristic 0.

(2) The field $\mathbb{Z}/p\,\mathbb{Z}$ with prime p has characteristic p, since for $n \in \mathbb{N}$ we have

$$n[1] = \underbrace{[1] \oplus \ldots \oplus [1]}_{n \text{ times}} = [n] = [0] \;\Leftrightarrow\; p \,|\, n\,.$$

(3) Let $f \in (\mathbb{Z}/p\,\mathbb{Z})[x]$ be an irreducible polynomial and $I = f\,(\mathbb{Z}/p\,\mathbb{Z})[x]$. Then the field $(\mathbb{Z}/p\,\mathbb{Z})[x]\,/I$ also has characteristic p, since

$$\begin{aligned} ([1]+I) &\neq I\,, \\ 2\,([1]+I) &= ([1]+I)+([1]+I) = [2]+I \neq I\,, \\ &\vdots \\ (p-1)\,([1]+I) &= [p-1]+I \neq I\,, \\ p\,([1]+I) &= [p]+I = [0]+I = I\,. \end{aligned}$$

By the observation made after the last proof, we have $p\,(g+I) = I$ for any $g \in (\mathbb{Z}/p\,\mathbb{Z})[x]$.

(4) We know that if R is any integral domain, then the ring $R[x]$ is also in integral domain. One can show that then

$$\operatorname{char}(R[x]) = \operatorname{char} R\,.$$