MAU22102
Rings, Fields, and Modules
2 - Arithmetic in domains

Nicolas Mascot
mascotn@tcd.ie
Module web page

Hilary 2020–2021
Version: March 25, 2021

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Main goal of this chapter

We shift our attention to commutative domains. All rings considered are commutative.

We will establish the following classification:

$$\text{Fields} \subsetneq \text{ED's} \subsetneq \text{PID's} \subsetneq \text{UFD's} \subsetneq \text{Domains}.$$

We will also study statements such as: If R is a UFD, then so is $R[x]$.

The field of fractions of a domain

Field of fractions of a domain

Idea: $\mathbb{Z}$ is not a field, but it can be embedded into the field $\mathbb{Q}$.

Definition (Field of fractions of a domain)

Let D be a domain. Its field of fractions is

$$\operatorname{Frac} D = \{(a,b) \mid a,b \in D,\ b \neq 0\}/\sim$$

where $(a,b) \sim (a',b')$ iff. $ab' = ba'$ in D (think $(a,b) \leftrightarrow a/b$).

Theorem (It really is a field)

$F = \operatorname{Frac} D$, equipped with $(a,b)+(c,d) = (ad+bc, bd)$ and $(a,b)(c,d) = (ac,bd)$, is a field, with $0_F = (0,1)$, $1_F = (1,1)$.

The map $\iota : \begin{array}{ccc} D & \longrightarrow & F \\ d & \longmapsto & (d,1) \end{array}$ *is an injective ring morphism.*

Field of fractions of a domain

Theorem (It really is a field)

$F = \operatorname{Frac} D$, equipped with $(a,b)+(c,d) = (ad+bc, bd)$ and $(a,b)(c,d) = (ac, bd)$, is a <u>*field*</u>*, with $0_F = (0,1)$, $1_F = (1,1)$.*

The map $\iota : \begin{array}{ccc} D & \longrightarrow & F \\ d & \longmapsto & (d,1) \end{array}$ *is an injective ring morphism.*

Proof.

Suppose that $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$. Then also $(a'd'+b'c', b'd') \sim (ad+bc, bd)$, because $(a'd'+b'c')(bd) = \underbrace{a'b}\, dd' + bb' \underbrace{c'd} = \underbrace{ab'}\, dd' + bb' \underbrace{cd'} = (ad+bc)(b'd')$.
Besides, $b, d \neq 0$ so $bd \neq 0$ so $(ad+bc, bd) \in F$; thus $+$ is well-defined. Similarly $\times$ is well-defined, and one can check that the ring axioms are satisfied.
We have $(a,b)+(0,1) = (a1+0b, b1) = (a,b)$ so $0_F = (0,1)$, and $(a,b)(1,1) = (a1, b1) = (a,b)$, so $1_F = (1,1)$.

□

Field of fractions of a domain

Theorem (It really is a field)

$F = \operatorname{Frac} D$, equipped with $(a,b)+(c,d) = (ad+bc, bd)$ and $(a,b)(c,d) = (ac, bd)$, is a field, with $0_F = (0,1)$, $1_F = (1,1)$.

The map $\iota : \begin{array}{ccc} D & \longrightarrow & F \\ d & \longmapsto & (d,1) \end{array}$ is an injective ring morphism.

Proof.

We have $(a,b) = 0_F = (0,1)$ iff. $a1 = b0$ iff. $a = 0$.
Thus if $(a,b) \neq 0_F$, then $a \neq 0$, so $(b,a) \in F$;
and $(a,b)(b,a) = (ab,ab) \sim (1,1) = 1_F$ so $(b,a) = (a,b)^{-1}$, so F is a field.
Finally $(a,1)+(b,1) = (a+b,1)$ and $(a,1)(b,1) = (ab,1)$ so ι is a morphism. If $a \in \operatorname{Ker} \iota$ then $(a,1) = 0_F$ so $a = 0$, so ι is injective. $\square$

Field of fractions of a domain

Theorem (It really is a field)

$F = \operatorname{Frac} D$, *equipped with* $(a,b)+(c,d) = (ad+bc, bd)$ *and* $(a,b)(c,d) = (ac, bd)$, *is a* *field, with* $0_F = (0,1)$, $1_F = (1,1)$.

The map $\iota : \begin{array}{ccc} D & \longrightarrow & F \\ d & \longmapsto & (d,1) \end{array}$ *is an injective ring morphism.*

Remark

ι is an isomorphism iff. D is already a field.

Example

$\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$.

$\operatorname{Frac} \mathbb{R}[x] = \mathbb{R}(x) = \{P(x)/Q(x),\ P, Q \in \mathbb{R}[x],\ Q(x) \neq 0\}$.

$\operatorname{Frac} \mathbb{Z}[x] = \mathbb{Q}(x)$.

Euclidean domains

Prototype: $\mathbb{Z}$

Recall that in the ring $\mathbb{Z}$ of integers, we have the notion of Euclidean division (division with remainder):

Theorem ($\mathbb{Z}$ is Euclidean)

For all $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist $q, r \in \mathbb{Z}$ such that

$$\begin{cases} a = bq + r, \\ 0 \leq r < |b|. \end{cases}$$

Example

For $a = 22$ and $b = 7$, we find $q = 3$ and $r = 1$.

Remark

Actually, the pair (q, r) is unique; but this is irrelevant for us.

Euclidean domains

Definition

An <u>*ED*</u> *(Euclidean Domain) is a domain D equipped with a "size" function $\sigma : D \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ such that for all $a, b \in D$ with $b \neq 0$, there exist $q, r \in D$ such that*

$$\begin{cases} a = bq + r, \\ \textit{Either } r = 0 \textit{ or } \sigma(r) < \sigma(b). \end{cases}$$

Example

$D = \mathbb{Z}$ is Euclidean with respect to $\sigma(x) = |x|$.

Remark

Every field is an ED: we can always take $r = 0$.

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{l|l}
A \quad x^5 \quad +x^3 \ +2x^2 + 3x + 5 & x^2 + x + 2 \quad B \\
\hline
 & Q \\
\\
\hline
\\
\hline
\\
\hline
R &
\end{array}
$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$\begin{array}{ll|ll} A & x^5 \quad +x^3 \;\; +2x^2 + 3x + 5 & x^2 + x + 2 & B \\ \cline{3-4} & & \underbrace{x^3}_{Q_1} & \\ \cline{2-2} & & & \\ \cline{2-2} & & & \\ \cline{2-2} \end{array}$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{lll|ll}
A & & x^5 \quad +x^3 \; +2x^2 +3x +5 & x^2 + x + 2 & B \\
\hline
Q_1 B & & x^5 + x^4 + 2x^3 & \underbrace{x^3}_{Q_1} & \\
\hline
 & & & & \\
\hline
 & & & & \\
\hline
\end{array}
$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$\begin{array}{ll|l}
A & x^5 \quad\quad +x^3 \;\; +2x^2 + 3x + 5 & x^2 + x + 2 \qquad B \\ \hline
Q_1 B & x^5 + x^4 + 2x^3 & \underbrace{x^3}_{Q_1} \\
\cline{2-2}
A - Q_1 B & \quad -x^4 - x^3 \;\; +2x^2 + 3x + 5 & \\
\cline{2-2}
& & \\
\cline{2-2}
& &
\end{array}$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{ll|ll}
A & x^5 \quad +x^3 \ +2x^2+3x+5 & x^2+x+2 & B \\
\hline
Q_1 B & x^5+x^4+2x^3 & \underbrace{x^3}_{Q_1} \ \underbrace{-x^2}_{Q_2} & \\
\cline{2-2}
A - Q_1 B & \quad -x^4-x^3 \ +2x^2+3x+5 & & \\
\cline{2-2}
 & & & \\
\cline{2-2}
\end{array}
$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$\begin{array}{ll|l}
A & x^5 \quad +x^3 \; +2x^2 + 3x + 5 & x^2 + x + 2 \qquad B \\ \hline
Q_1 B & x^5 + x^4 + 2x^3 & \underbrace{x^3}_{Q_1} \; \underbrace{-x^2}_{Q_2} \\
\cline{2-2}
A - Q_1 B & \quad -x^4 - x^3 \; + 2x^2 + 3x + 5 & \\
Q_2 B & \quad -x^4 - x^3 \; -2x^2 & \\
\cline{2-2}
 & & \\
\cline{2-2}
\end{array}$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{l|cccccc|ll}
A & x^5 & & +x^3 & +2x^2 & +3x & +5 & x^2 + x + 2 & B \\
\cline{8-9}
Q_1 B & x^5 & +x^4 & +2x^3 & & & & \underbrace{x^3}_{Q_1} \; \underbrace{-x^2}_{Q_2} & \\
\cline{2-7}
A - Q_1 B & & -x^4 & -x^3 & +2x^2 & +3x & +5 & & \\
Q_2 B & & -x^4 & -x^3 & -2x^2 & & & & \\
\cline{2-7}
 & & & & 4x^2 & +3x & +5 & & \\
 & & & & & & & & \\
\cline{2-7}
 & & & & & & & &
\end{array}
$$

Euclidean domains

Theorem (Field$[x]$ is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{l|cccccc|l}
A & x^5 & & +x^3 & +2x^2 & +3x & +5 & x^2+x+2 \qquad B \\
\cline{8-8}
Q_1 B & x^5 & +x^4 & +2x^3 & & & & \underbrace{x^3}_{Q_1}\ \underbrace{-x^2}_{Q_2}\ \underbrace{+4}_{Q_3} \\
\cline{2-7}
A - Q_1 B & & -x^4 & -x^3 & +2x^2 & +3x & +5 & \\
Q_2 B & & -x^4 & -x^3 & -2x^2 & & & \\
\cline{2-7}
 & & & & 4x^2 & +3x & +5 & \\
 & & & & & & & \\
\cline{2-7}
 & & & & & & &
\end{array}
$$

Euclidean domains

Theorem (Field$[x]$ is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{lrrrrrr|lr}
A & x^5 & & +x^3 & +2x^2 & +3x & +5 & x^2 + x + 2 & B \\
\cline{8-9}
Q_1 B & x^5 & +x^4 & +2x^3 & & & & \underbrace{x^3}_{Q_1} \; \underbrace{-x^2}_{Q_2} \; \underbrace{+4}_{Q_3} & \\
\cline{2-7}
A - Q_1 B & & -x^4 & -x^3 & +2x^2 & +3x & +5 & & \\
Q_2 B & & -x^4 & -x^3 & -2x^2 & & & & \\
\cline{2-7}
 & & & & 4x^2 & +3x & +5 & & \\
Q_3 B & & & & 4x^2 & +4x & +8 & & \\
\cline{2-7}
\end{array}
$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{l|rrrrrr|l}
A & x^5 & & +x^3 & +2x^2 & +3x & +5 & x^2 + x + 2 \qquad B \\
\cline{8-8}
Q_1 B & x^5 & +x^4 & +2x^3 & & & & \underbrace{x^3}_{Q_1} \ \underbrace{-x^2}_{Q_2} \ \underbrace{+4}_{Q_3} \\
\cline{2-7}
A - Q_1 B & & -x^4 & -x^3 & +2x^2 & +3x & +5 & \\
Q_2 B & & -x^4 & -x^3 & -2x^2 & & & \\
\cline{2-7}
 & & & & 4x^2 & +3x & +5 & \\
Q_3 B & & & & 4x^2 & +4x & +8 & \\
\cline{2-7}
 & & & & & -x & -3 & \\
\end{array}
$$

Euclidean domains

Theorem (Field[x] is Euclidean)

If F is a field, then $F[x]$ is Euclidean with respect to $\sigma = \deg$.

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{ll|ll}
A & x^5 \qquad +x^3 \; +2x^2+3x+5 & x^2+x+2 & B \\
\cline{3-4}
Q_1B & x^5+x^4+2x^3 & \underbrace{x^3}_{Q_1} \; \underbrace{-x^2}_{Q_2} \; \underbrace{+4}_{Q_3} & Q \\
\cline{2-2}
A-Q_1B & \quad -x^4-x^3 \; +2x^2+3x+5 & & \\
Q_2B & \quad -x^4-x^3 \; -2x^2 & & \\
\cline{2-2}
 & \qquad\qquad 4x^2+3x+5 & & \\
Q_3B & \qquad\qquad 4x^2+4x+8 & & \\
\cline{2-2}
R & \qquad\qquad\quad -x-3 & &
\end{array}
$$

Euclidean domains

Example

We divide $A = x^5 + x^3 + 2x^2 + 3x + 5$ by $B = x^2 + x + 2$:

$$
\begin{array}{ll|l}
A & x^5 +x^3 +2x^2 +3x +5 & x^2 + x + 2 \qquad B \\
\cline{3-3}
Q_1 B & x^5 +x^4 +2x^3 & \underbrace{x^3}_{Q_1} \ \underbrace{-x^2}_{Q_2} \ \underbrace{+4}_{Q_3} \\
\cline{2-2}
A - Q_1 B & -x^4 -x^3 +2x^2 +3x +5 & \\
Q_2 B & -x^4 -x^3 -2x^2 & \\
\cline{2-2}
 & 4x^2 +3x +5 & \\
Q_3 B & 4x^2 +4x +8 & \\
\cline{2-2}
 & -x -3 &
\end{array}
$$

Remark

Even if R is not a field, Euclidean division by $B(x) \in R[x]$ is possible <u>if</u> the leading coefficient of B is <u>invertible</u>.

Uniqueness

Let D be a domain.

Theorem

Let $A, B \in D[x]$, $B \neq 0$. If there exists $Q, R \in D[x]$ such that $A = BQ + R$ and ($R = 0$ or $\deg R < \deg B$), then this pair (Q, R) is unique.

Remark

If is convenient to define $\deg 0 = -\infty$, so that $\deg PQ = \deg P + \deg Q$.

Proof.

If $A = BQ + R = BQ' + R'$, then $B(Q - Q') = R' - R$ has degree $< \deg B$. If $Q \neq Q'$, then $\deg B(Q - Q') = \deg B + \deg(Q - Q') \geq \deg B$, absurd. So $Q = Q'$ and $R = A - BQ = A - BQ' = R'$. $\square$

Roots vs. division by $x - \alpha$

Let R be a ring.

Definition (Root of a polynomial)

Let $P(x) \in R[x]$. We say that $\alpha \in R$ is a <u>root</u> of $P(x)$ if $P(\alpha) = 0$.

Let $A \in R[x]$, and $B(x) = (x - \alpha)$, $\alpha \in R$. We can divide A by B; the remainder will be a constant $r \in R$. Evaluating $A(x) = (x - \alpha)Q(x) + r$ at $x = \alpha$, we get

$$r = A(\alpha).$$

Corollary

$A(\alpha) = 0$ iff. $A(x) = (x - \alpha)Q(x)$ for some $Q(x) \in R[x]$.

Roots vs. degree

Theorem (# roots $\leq$ deg)

Let D be a domain, and $P(x) \in D[x]$, $P \neq 0$. If P has at least n distinct roots in D, then $n \leq \deg P$.

Proof.

Induction on n. For $n = 0$, nothing to prove.
Suppose $\alpha_1, \cdots, \alpha_n \in D$ are distinct roots of $P(x)$. Then $P(x) = (x - \alpha_n)Q(x)$ for some $Q(x) \in D[x]$. For all $j < n$, $0 = P(\alpha_j) = (\alpha_j - \alpha_n)Q(\alpha_j)$, so $Q(\alpha_j) = 0$ as D is a domain.
By induction, $\deg Q \geq n - 1$, whence
$\deg P = \deg(x - \alpha_n)Q = \deg(x - \alpha_n) + \deg Q \geq n$. $\square$

Roots vs. degree

Theorem (# roots $\leq$ deg)

Let D be a domain, and $P(x) \in D[x]$, $P \neq 0$. If P has at least n distinct roots in D, then $n \leq \deg P$.

Example

If $P \in \mathbb{R}[x]$ has degree ≤ 10 and vanishes at $x = 0, 1, \cdots, 10$, then $P = 0$.

Remark

Let $D = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, and $P(x) = x^2 - x \in D[x]$.
Then $P(\alpha) = 0$ for all $\alpha \in D$, even though $P(x) \neq 0$ in $D[x]$!

Roots vs. degree

Theorem ($\#$ roots $\leq$ deg)

Let D be a domain, and $P(x) \in D[x]$, $P \neq 0$. If P has at least n distinct roots in D, then $n \leq \deg P$.

Counter-example

Let $R = \mathbb{Z}/8\mathbb{Z}$, and $P(x) = x^2 - 1 \in R[x]$. Then $\deg P = 2$, and yet P has 4 roots in R, namely $1, -1, 3, -3$.
In particular, $(x-3) \mid P(x) = (x-1)(x+1)$!

Principal Ideal Domains

Principal Ideal Domains

Definition (PID)

A PID (Principal Ideal Domain) is a domain D whose ideals are all principal, that is to say of the form

$$(x) = xD = \{xd,\ d \in D\}$$

for some $x \in D$.

Counter-example

We have seen that in $D = \mathbb{Z}[x]$, the ideal

$$I = \{P(x) \in \mathbb{Z}[x] \mid P(0) \text{ is even}\}$$

is not principal. Therefore $\mathbb{Z}[x]$ is not a PID.

ED $\implies$ PID

Theorem

Every ED is a PID.

Proof.

Let E be Euclidean with respect to σ, and let $I \triangleleft E$ be an ideal.
If $I = \{0\}$, then $I = (0)$ is principal.
Else, let $0 \neq i \in I$ be such that $\sigma(i) = \min\{\sigma(j),\ 0 \neq j \in I\}$.
We claim that $I = (i)$.
Clearly $(i) \subseteq I$. Conversely, take $j \in I$, and Euclidean-divide it by i : $j = iq + r$. If $r \neq 0$, then $\sigma(r) < \sigma(i)$,
yet $r = i - jq \in I$, absurd. So $r = 0$ and $j = iq \in (i)$,
which shows that $I \subseteq (i)$. □

Corollary

$\mathbb{Z}$ is a PID. If F is a field, then $F[x]$ is a PID.

ED $\implies$ PID

Theorem

Every ED is a PID.

Counter-example (Non-examinable)

Let $\alpha = \dfrac{1 + i\sqrt{19}}{2} \in \mathbb{C}$. As $\alpha^2 = \alpha - 5$,

$$\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

is a subring of $\mathbb{C}$. It can be proved that it is a PID but not an ED.

A semi-useless converse

Proposition

Let D be a domain. Then $D[x]$ is a PID $\iff$ D is a field.

Proof.

We already know $\Leftarrow$, so we prove $\Rightarrow$. Let $d \in D$, $d \neq 0$, and consider

$$I = (d, x) = \{dU(x) + xV(x) \mid U, V \in D[x]\} \lhd D[x].$$

As $D[x]$ is a PID, $I = (G(x))$ for some $G(x) \in D[x]$.
As $d \in I$, we have $d = G(x)P(x)$ for some $P(x) \in D[x]$;
by degrees, $G(x) = g \in D$ is a constant.
Similarly $x = G(x)Q(x) = gQ(x)$ for some $Q(x) \in D[x]$ of degree 1, say $Q(x) = ax + b$; then $ga = 1$.
Thus $1 = ga = Ga \in I$, so there exist $U, V \in D[x]$ such that $1 = dU(x) + xV(x)$; taking $x = 0$ yields $1 = dU(0)$. $\square$

Divisibility, associates, and irreducibles

Divisibility

Definition (Divisibility)

Let R be a ring, and $x, y \in R$. We say that x divides y, written $x \mid y$, if $y = xz$ for some $z \in R$.

Example

In $R = \mathbb{Z}$, $2 \nmid 5$; but in $R = \mathbb{Q}$, $2 \mid 5$.

Remark

$x \mid y \iff y \in (x) \iff (y) \subseteq (x)$.

Associates

Definition (Associates)

Let R be a ring. We say that $x, y \in R$ are associates if $x \mid y$ and $y \mid x$.

Remark

Equivalently, x and y are associates iff. $(x) = (y)$.

Remark

This is an equivalence relation.

Associates

Definition (Associates)

Let R be a ring. We say that $x, y \in R$ are <u>*associates*</u> *if $x \mid y$ and $y \mid x$.*

Proposition

Suppose R is a domain. Then

$$x \text{ and } y \text{ are associates} \iff x = uy \text{ for some } u \in R^\times.$$

Proof.

$\Rightarrow$ As $x \mid y$, we have $y = ax$ for some $a \in R$. Similarly, there exists $b \in R$ such that $x = by$. Then $x = by = bax$, so $x(1 - ba) = 0$. If $x = 0$, then $y = ax = 0 = 1x$; else, as R is a domain, $ab = 1$, so $a, b \in R^\times$.

$\Leftarrow$ Clear, since we also have $y = u^{-1}x$. $\square$

Associates

Definition (Associates)

Let R be a ring. We say that $x, y \in R$ are associates if $x \mid y$ and $y \mid x$.

Proposition

Suppose R is a domain. Then

$$x \text{ and } y \text{ are associates} \iff x = uy \text{ for some } u \in R^\times.$$

Example

In $R = \mathbb{Z}$, m and n are associates iff. $m = \pm n$.

In $R = \mathbb{R}[x]$, $P(x)$ and $Q(x)$ are associates iff. $P(x) = cQ(x)$ for some $c \in \mathbb{R}^\times$.

Irreducibles

Definition (Irreducible)

Let R be a ring. An element $x \in R$ is irreducible if $x \neq 0$, $x \notin R^\times$, and if whenever $x = yz$ with $y, z \in R$, then $y \in R^\times$ or $z \in R^\times$.

Example

In $R = \mathbb{Z}$, the irreducibles are the prime numbers and their negatives.

Remark

Any associate to an irreducible is also irreducible.

Unique Factorisation Domains: introduction

Unique Factorisation Domains

Definition (UFD)

A UFD (Unique Factorisation Domain) is a domain D in which for every $0 \neq d \in D$

- *d can be expressed as $d = up_1 \cdots p_r$ with $u \in R^\times$ and the $p_i \in D$ irreducible,*
- *this factorisation is unique: if $d = up_1 \cdots p_r = vq_1 \cdots q_s$, then $r = s$, and up to re-ordering, p_i is associate to q_i for all i.*

Example

We will see that $\mathbb{Z}$ is a UFD.
The fact that $6 = 2 \times 3 = 3 \times 2 = -2 \times -3$ does not contradict that! Neither does $210 = 10 \times 21 = 14 \times 15$.

Unique Factorisation Domains

Counter-example (Non-examinable)

Let $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.
Given $\alpha = a + bi\sqrt{5} \in R$, define

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + 5b^2 \in \mathbb{Z}_{\geq 0}.$$

Then $N(\alpha\beta) = N(\alpha)N(\beta)$, so

$$\alpha \in R^\times \iff N(\alpha) = 1 \iff \alpha = \pm 1.$$

The element $6 \in R$ can be factored as $6 = 2 \times 3$,
but also as $6 = \gamma\overline{\gamma}$, where $\gamma = 1 + i\sqrt{5}$.

γ is irreducible (if $\gamma = \alpha\beta$, then $N(\alpha)N(\beta) = N(\gamma) = 6$ so $N(\alpha) = 2$ or 3, absurd), and so are 2 and 3, so these factorisations are complete. They are also genuinely distinct since γ is not associate to 2 nor 3, as $R^\times = \{\pm 1\}$.

So R is not a UFD.

Unique Factorisation Domains

Another way to understand the uniqueness condition is to say that if we choose a set $P \subset D$ of irreducibles such that each irreducible is associate to exactly one $p \in P$, then each $0 \neq d \in D$ factors as $d = up_1 \cdots p_r$ with $u \in R^\times$, the $p_i \in P$, and this factorisation is unique up to the order of the factors.

Example

For $R = \mathbb{Z}$, we can take $P = \{\text{prime numbers}\}$, and then every $0 \neq n \in \mathbb{Z}$ factors uniquely as $n = \pm p_1 \cdots p_r$.

For $R = \mathbb{R}[x]$, we have $\mathbb{R}[x]^\times = \mathbb{R}^\times$, so we can take $P = \{\underline{\text{monic}} \text{ irreducible polynomials}\}$, and then every $0 \neq F(x) \in \mathbb{R}[x]$ factors uniquely as $F(x) = cP_1(x) \cdots P_r(x)$, where $c \in \mathbb{R}[x]^\times = \mathbb{R}^\times$.

Noetherian rings

Noetherian rings (Non-examinable)

Definition (Noetherian)

A ring R is Noetherian if every ideal $I \triangleleft R$ is finitely generated, meaning there exists a finite subset $S \subseteq I$ which generates I.

Example

Every PID is Noetherian.

Theorem

R is Noetherian $\iff$ there are no infinite increasing chains of ideals $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subseteq R$.

Noetherian rings (Non-examinable)

Theorem

R is Noetherian $\iff$ there are no infinite increasing chains of ideals $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subseteq R$.

Proof.

$\Rightarrow$ Suppose $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subseteq R$ are ideals. Then $I = \bigcup_{n \geq 0} I_n$ is an ideal; for instance if $i, j \in I$, then $i \in I_{n_i}$ and $j \in I_{n_j}$ for some $n_i, n_j \geq 0$, then $i, j \in I_n$ for $n = \max(n_i, n_j)$, so $i + j \in I_n \subset I$. As R is Noetherian, I is generated by $g_1, \cdots, g_s \in I$. For each $k \leq s$, let $m_k \geq 0$ such that $g_k \in I_{m_k}$, and let $m = \max_k m_k$; then $g_k \in I_m$ for all k, so $I \subseteq I_m$, absurd.

□

Noetherian rings (Non-examinable)

Theorem

R is Noetherian $\iff$ there are no infinite increasing chains of ideals $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subseteq R$.

Proof.

$\Leftarrow$ Let $I \lhd R$ be an ideal. Pick $i_1 \in I$; if $I = (i_1)$, done.
Else, pick $i_2 \in I \setminus (i_1)$; if $I = (i_1, i_2)$, done.
Else, pick $i_3 \in I \setminus (i_1, i_2)$, etc.
As $(i_1) \subsetneq (i_1, i_2) \subsetneq (i_1, i_2, i_3) \subsetneq \cdots$, this terminates. □

Noetherian rings (Non-examinable)

Theorem

R is Noetherian $\iff$ there are no infinite increasing chains of ideals $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subseteq R$.

Counter-example

Let $R =$ continuous functions $\mathbb{R} \to \mathbb{R}$, and

$$I_n = \{f \in R \mid f(x) = 0 \text{ for all } x \geq n\}.$$

The I_n form an infinite chain, so R is not Noetherian.
Indeed, we have

$$\bigcup_{n \geq 0} I_n = \{f \in R \mid \text{ there is } x_0 : \text{ for all } x \geq x_0, f(x) = 0\};$$

if we had $I = (f_1, \cdots, f_m)$, with $f_k(x) = 0$ for $x \geq x_k$, then all $f \in I$ have $f(x) = 0$ for $x \geq \max_k x_k$, absurd.

Noetherian rings (Non-examinable)

Theorem

R is Noetherian $\iff$ there are no infinite increasing chains of ideals $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subseteq R$.

Theorem (Hilbert's basis theorem)

If R is Noetherian, then so is $R[x]$.

Noetherian rings (Non-examinable)

Theorem (Hilbert's basis theorem)

If R is Noetherian, then so is $R[x]$.

Proof.

Suppose by contradiction that $I \triangleleft R[x]$ cannot be finitely generated. Let $0 \neq F_1(x) \in I$ of minimal degree, and let $J_1 = (F_1) \triangleleft R[x]$. As I cannot be finitely generated, $J_1 \subsetneq I$, so let $F_2(x) \in I$ but $\notin J_1$ of smallest possible degree, and let $J_2 = (F_1, F_2) \triangleleft R[x]$. Then $J_2 \subsetneq I$, so let $F_3(x) \in I$ but $\notin J_2$ of smallest possible degree, and $J_3 = (F_1, F_2, F_3)$, etc.
For each $n \in \mathbb{N}$, write $F_n(x) = a_n x^{d_n} + \cdots$ where $d_n = \deg F_n$ and $0 \neq a_n \in R$. Clearly, $d_1 \leq d_2 \leq d_3 \leq \cdots$; besides, the chain $(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3)$ of ideals of R must terminate as R Noetherian, so there exists $N \in \mathbb{N}$ such that $a_N \in (a_1, a_2, \cdots, a_{N-1})$, say $a_N = \sum_{i=1}^{N-1} r_i a_i$ for some $r_i \in R$.
Continued next slide... □

Noetherian rings (Non-examinable)

Theorem (Hilbert's basis theorem)

If R is Noetherian, then so is $R[x]$.

Proof.

$$\begin{aligned}\text{Then } I \ni G(x) &= F_N(x) - \sum_{i=1}^{N-1} x^{d_N - d_i} r_i F_i(x) \\ &= (a_N x^{d_N} + \cdots) - \sum_{i=1}^{N-1} (r_i a_i x^{d_N} + \cdots) \\ &= (a_N x^{d_N} + \cdots) - (a_N x^{d_N} + \cdots)\end{aligned}$$

as $d_N \geq d_i$ for all $i < N$, and $\deg G < d_N = \deg F_N$,
so $G \in J_{N-1}$ by definition of F_N.

But $F_N(x) = G(x) + \sum_{i=1}^{N-1} x^{d_N - d_i} r_i F_i(x) \in J_{N-1}$, absurd. $\square$

Noetherian vs. factorisation

Proposition (Non-examinable)

In a Noetherian domain, factorisations into irreducibles are possible (but need not be unique).

Proof.

Let R be Noetherian, and let $0 \neq x \in R$. If $x \in R^\times$, OK. If x is irreducible, OK. Else, we can write $x = yy'$, $y, y' \in R$ nonzero and not invertible. If y and y' are irreducible, OK. Else, if for instance y is reducible, $y = y_1 y_2$. If y_1 and y_2 are irreducible, OK; else... Since $\cdots \mid y_1 \mid y \mid x$, we have $(x) \subset (y) \subset (y_1) \subset \cdots$, and the inclusions are strict since z, y_2, $\cdots$ are not invertible. So this terminates. $\square$

Corollary (Examinable)

In a PID, factorisations into irreducibles are possible.

Prime ideals, Maximal ideals

Prime ideals

Let R be a ring, and let $I \neq R$ be an ideal.

Definition (Prime ideal)

I is prime if for all $x, y \in R$, $xy \in I \Longrightarrow x \in I$ or $y \in I$.

Equivalently, $x \notin I$ and $y \notin I \Longrightarrow xy \notin I$.

By convention, $I = R$ is not prime.

Proposition

I is prime $\Longleftrightarrow R/I$ is a domain.

Proof.

Let $I \neq R$, so that R/I is not the zero ring.

$$\begin{aligned} I \subsetneq R \text{ prime} &\Longleftrightarrow \text{ for all } x, y \in R,\ x, y \notin I \Rightarrow xy \notin I \\ &\Longleftrightarrow \text{ for all } \overline{x}, \overline{y} \in R/I,\ \overline{x}, \overline{y} \neq \overline{0} \Rightarrow \overline{xy} \neq \overline{0} \\ &\Longleftrightarrow R/I \text{ is a domain.} \end{aligned}$$

□

Maximal ideals

Definition (Maximal ideal)

Let again R be a ring and $I \lhd R$ an ideal. I is <u>maximal</u> if $I \neq R$ and whenever $J \supseteq I$ is an ideal, then $J = I$ or $J = R$.

So it is a <u>proper</u> ideal which is as large as possible.

Proposition

I is maximal $\iff R/I$ is a <u>field</u>.

Proof.

$\Rightarrow$: Let $\bar{0} \neq \bar{x} \in R/I$. Then $x \in R \setminus I$, so $J = (x) + I \supsetneq I$, so $J = R$, so $1 \in J$, so $1 = xy + i$ for some $y \in R$ and $i \in I$. Then $\bar{x}\,\bar{y} = \bar{1}$.

□

Maximal ideals

Definition (Maximal ideal)

Let again R be a ring and $I \lhd R$ an ideal. I is maximal if $I \neq R$ and whenever $J \supseteq I$ is an ideal, then $J = I$ or $J = R$.

Proposition

I is maximal $\Longleftrightarrow$ R/I is a field.

Proof.

$\Leftarrow$: Let $J \supsetneq I$ be an ideal, and let $j \in J \setminus I$. Then $\bar{j} \neq \bar{0} \in R/I$, so there exists $\bar{x} \in R/I$ such that $\bar{j}\,\bar{x} = \bar{1} \in R/I$, whence $jx = 1 + i$ for some $i \in I$. Then $1 = jx - i \in J$, so $J = R$. □

Maximal ideals

Definition (Maximal ideal)

Let again R be a ring and $I \triangleleft R$ an ideal. I is maximal if $I \neq R$ and whenever $J \supseteq I$ is an ideal, then $J = I$ or $J = R$.

Proposition

I is maximal $\iff$ R/I is a field.

Corollary

Every maximal ideal is prime.

Maximal ideals

Corollary

Every maximal ideal is prime.

Counter-example

Let $R = \mathbb{Z}[x]$ and $I = (x)$. As $I = \operatorname{Ker} \begin{array}{ccc} \mathbb{Z}[x] & \longrightarrow & \mathbb{Z} \\ P(x) & \longmapsto & P(0) \end{array}$, we have $R/I \simeq \mathbb{Z}$ by the isomorphism theorem. Thus R/I is a domain but not a field, so I is prime but not maximal.

The ideal $J = (5, x)$ strictly contains I, and is actually maximal: indeed $J = \operatorname{Ker} \begin{array}{ccc} \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}/5\mathbb{Z} \\ P(x) & \longmapsto & P(0) \bmod 5 \end{array}$ so $R/J \simeq \mathbb{Z}/5\mathbb{Z}$ is a field.

Application to $\mathbb{Z}/n\mathbb{Z}$

Theorem

Let $n \in \mathbb{N}$. TFAE:

1. *n is a prime number*
2. *$\mathbb{Z}/n\mathbb{Z}$ is a field*
3. *$\mathbb{Z}/n\mathbb{Z}$ is a domain*

Proof.

$1 \Rightarrow 2$: Let $J \supseteq n\mathbb{Z}$ be an ideal of $\mathbb{Z}$. As $\mathbb{Z}$ is a *PID*, $J = m\mathbb{Z}$ for some $m \in \mathbb{Z}$. As $n \in n\mathbb{Z} \subseteq J$, $n \in J$, so $m \mid n$; as n is prime, either $m = \pm 1$ and $J = \mathbb{Z}$, or $m = \pm n$ and $J = n\mathbb{Z}$. Thus $n\mathbb{Z}$ is maximal.
$2 \Rightarrow 3$: Every field is a domain.
$3 \Rightarrow 1$: Suppose n is not prime, so that $n = ab$ with $1 < a, b < n$. Then $\overline{0} = \overline{n} = \overline{a}\,\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ whereas $\overline{a}, \overline{b} \neq \overline{0}$, so $\mathbb{Z}/n\mathbb{Z}$ is not a domain. $\square$

Unique Factorisation Domains: theorems

Divisibility in a UFD

Remark

Let D be a UFD, and let $x, y \in D$. If x factors as $up_1 \cdots p_r$ and y as $vq_1 \cdots q_s$, where $u, v \in D^\times$ and the p_i, q_i irreducible, then the factorisation of xy is

$$xy = (uv)p_1 \cdots p_r q_1 \cdots q_s.$$

Usually, we pick our irreducibles only in a set of representatives up to associates, and we gather the repeated factors. Then factorisations are written $up_1^{a_1} \cdots p_r^{a_r}$ with the $a_i \in \mathbb{N}$.
Given $x, y \in D$, we may always assume that x and y have the same irreducible factors, by allowing exponents $a_i = 0$.

Example

In $D = \mathbb{Z}$, with $x = -6$ and $y = -45$, we have $x = (-1)2^1 3^1 5^0$ and $y = (-1)2^0 3^2 5^1$.

Divisibility in a UFD

Given $x, y \in D$, we may always assume that x and y have the same irreducible factors, by allowing exponents $a_i = 0$.

Example

In $D = \mathbb{Z}$, with $x = -6$ and $y = -45$, we have $x = (-1)2^1 3^1 5^0$ and $y = (-1)2^0 3^2 5^1$.

Then the factorisation of a product is obtained by multiplying the units and adding the exponents of the factors.

Example

$(-1)2^1 3^1 5^0 \times (-1)2^0 3^2 5^1 = (-1 \times -1)2^{1+0} 3^{1+2} 5^{0+1} = (1)2^1 3^3 5^1.$

Corollary (Read divisibility off factorisations)

Let D be a UFD, and $x = up_1^{a_1} \cdots p_r^{a_r}$, $y = vp_1^{b_1} \cdots p_r^{b_r} \in D$. Then $x \mid y \implies a_i \leq b_i$ for all i. Note that u, v play no role.

Prime elements

Definition

Let D be a domain, and let $x \in D$. We say that x is prime if the ideal (x) is a prime ideal.

Equivalently, this means that for all $y, z \in D$,

$$\text{if } x \mid yz, \text{ then } x \mid y \text{ or } x \mid z.$$

By convention, units are not prime, since R is not a prime ideal of itself.

Counter-example

$n = 4$ is not prime in $D = \mathbb{Z}$, since $4 \mid 2 \times 6$ whereas $4 \nmid 2$ and $4 \nmid 6$.

Example (Prime elements in $\mathbb{Z}$)

Take $D = \mathbb{Z}$. Then $n \in \mathbb{Z}$ is prime $\iff n\mathbb{Z}$ is a prime ideal $\iff \mathbb{Z}/n\mathbb{Z}$ is a domain $\iff n$ is $\pm$ a prime number or 0.

Prime $\Longrightarrow$ irreducible

Proposition (Prime $\Longrightarrow$ irreducible)

Let D be a domain, and let $0 \neq x \in D$. If x is prime, then x is irreducible.

Proof.

Contrapositive: Suppose x is reducible. Then $x = yz$ with $y, z \in D \setminus D^\times$. In $D/(x)$, we have $\overline{0} = \overline{x} = \overline{y}\,\overline{z}$.
If $\overline{y} = \overline{0}$, then $x \mid y$, so x and y would be associate, so $x = yu$ for some $u \in D^\times$, but then $yz = x = yu$ so $y(z - u) = 0$, yet $y \neq 0$ as $x \neq 0$, and $z \neq u$ as $z \notin D^\times$, absurd.
So $\overline{y} \neq \overline{0}$, and similarly $\overline{z} \neq \overline{0}$; thus $D/(x)$ is not a domain, so x is not prime. $\square$

Prime $\implies$ irreducible

Proposition (Prime $\implies$ irreducible)

Let D be a domain, and let $0 \neq x \in D$. If x is prime, then x is irreducible.

Counter-example

Consider again $D = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.
We saw that $2 \in D$ is irreducible; however 2 is **not** prime:
We have $2 \mid 6 = \gamma\overline{\gamma}$ where $\gamma = 1 + i\sqrt{5} \in D$, yet $2 \nmid \gamma, \overline{\gamma}$.

UFD $\iff$ (prime $\Leftarrow$ irreducible)

Lemma

Let D be a domain in which factorisations exist. Then D is a UFD $\iff$ for all $0 \neq p \in D$, if p is irreducible, then p is prime.

Proof.

$\Leftarrow$ Let $0 \neq x \in D$, and suppose $x = up_1 \cdots p_r = vq_1 \cdots q_s$ with $u, v \in D^\times$ and the p_i, q_i irreducible, hence prime. Then $p_1 \mid vq_1 \cdots q_s$, so $p_1 \mid v$ or $p_1 \mid q_i$ for some i. If $p_1 \mid v$, then $v = p_1 x$ for some $x \in D$, whence $1 = p_1(xv^{-1})$ so $p_1 \in D^\times$, absurd. So $p_1 \mid q_i$, WLOG $p_1 \mid q_1$, so $q_1 = p_1 y$ for some $y \in D$. As q_1 irreducible and $p_1 \notin D^\times$, we have $y \in D^\times$, so p_1 and q_1 are associates, WLOG $p_1 = q_1$. Thus $p_1(up_2 \cdots p_r - vq_2 \cdots q_s) = 0$, so $up_2 \cdots p_r = vq_2 \cdots q_s$; continue. $\square$

UFD $\iff$ (prime $\Leftarrow$ irreducible)

Lemma

Let D be a domain in which factorisations exist. Then D is a UFD $\iff$ for all $0 \neq p \in D$, if p is irreducible, then p is prime.

Proof.

$\Rightarrow$ Let $p \in D$ irreducible, and let $x, y \in D$. If $p \mid xy$, then p is an irreducible factor of xy, hence of x or of y, so $p \mid x$ or y. $\square$

UFD $\iff$ (prime $\Leftarrow$ irreducible)

Lemma

Let D be a domain in which factorisations exist. Then D is a UFD $\iff$ for all $0 \neq p \in D$, if p is irreducible, then p is prime.

Remark

So in a UFD, irreducible and prime are the same concept; and that characterises uniqueness of factorisation.

PID $\implies$ UFD

Theorem (PID $\implies$ UFD)

Every PID is a UFD.

Proof.

We already know that factorisations exist in a PID; we now show uniqueness.
Let D be a PID, let $p \in D$ irreducible and let $a, b \in D$ such that $p \mid ab$, say $ab = pz$, $z \in D$.
Since D is a PID, $(p, a) = (d)$ for some $d \in D$; in particular $p \in (d)$ so $p = cd$ for some $c \in D$. As p is irreducible, either $c \in D^\times$ or $d \in D^\times$.
If $c \in D^\times$, then p assoc. d, so $(p) = (d) \ni a$, whence $p \mid a$.
If $d \in D^\times$, then $(p, a) = (d) = D \ni 1$ so $1 = ax + py$ for some $x, y \in D$, and then
$p \mid p(zx + yb) = pzx + pyb = abx + pyb = (ax + py)b = b$. $\square$

PID $\implies$ UFD

Theorem (PID $\implies$ UFD)

Every PID is a UFD.

Corollary

$\mathbb{Z}$ *is a UFD.*
If F *is a field, then* $F[x]$ *is a UFD.*
(Note: the latter statement will be superseded soon.)

gcd and lcm in a UFD

Greatest common divisors

Definition (gcd)

Let R be a ring, and let $a, b \in R$. A gcd of a and b is a $g \in R$ such that $g \mid a, b$ and for all $d \in R$, if $d \mid a, b$, then $d \mid g$.

Theorem (In UFD, gcd exists and unique up to assoc.)

Let D be a UFD, and $a = up_1^{a_1} \cdots p_r^{a_r}$, $b = vp_1^{b_1} \cdots p_r^{b_r} \in D$. Then $g = p_1^{\min(a_1,b_1)} \cdots p_r^{\min(a_r,b_r)}$ is a gcd of a and b, and $g' \in R$ is another gcd iff. g' assoc. g.

Proof.

Recall that $wp_1^{e_1} \cdots p_r^{e_r} \mid w' p_1^{f_1} \cdots p_r^{f_r} \iff e_i \leq f_i$ for all i.
We want that for all $d \in D$, $d \mid a, b \iff d \mid g$.
Writing $d = wp_1^{d_1} \cdots p_r^{d_r}$ and $g = w' p_1^{g_1} \cdots p_r^{g_r}$, this translates into $d_i \leq a_i, b_i$ for all $i \iff d_i \leq g_i$ for all i. $\square$

Greatest common divisors

Definition (gcd)

Let R be a ring, and let $a, b \in R$. A gcd of a and b is a $g \in R$ such that $g \mid a, b$ and for all $d \in R$, if $d \mid a, b$, then $d \mid g$.

Theorem (In UFD, gcd exists and unique up to assoc.)

Let D be a UFD, and $a = u p_1^{a_1} \cdots p_r^{a_r}$, $b = v p_1^{b_1} \cdots p_r^{b_r} \in D$. Then $g = p_1^{\min(a_1, b_1)} \cdots p_r^{\min(a_r, b_r)}$ is a gcd of a and b, and $g' \in R$ is another gcd iff. g' assoc. g.

Example

In $\mathbb{Z}$, $\gcd(-6, 45) = \gcd\left((-1)2^1 3^1 5^0, 2^0 3^2 5^1\right) = u 2^0 3^1 5^0 = \pm 3.$

Greatest common divisors

Definition (gcd)

Let R be a ring, and let $a, b \in R$. A gcd of a and b is a $g \in R$ such that $g \mid a, b$ and for all $d \in R$, if $d \mid a, b$, then $d \mid g$.

Theorem (In UFD, gcd exists and unique up to assoc.)

Let D be a UFD, and $a = up_1^{a_1} \cdots p_r^{a_r}$, $b = vp_1^{b_1} \cdots p_r^{b_r} \in D$. Then $g = p_1^{\min(a_1, b_1)} \cdots p_r^{\min(a_r, b_r)}$ is a gcd of a and b, and $g' \in R$ is another gcd iff. g' assoc. g.

Definition (Coprime)

We say that a and b are coprime if 1 is a gcd of a and b.

So a and b are coprime iff. they have no non-unit common factor.

Lowest common multiples

Definition (lcm)

Let R be a ring, and let $a, b \in R$. An lcm of a and b is a $\ell \in R$ such that $a, b \mid \ell$, and for all $m \in R$, if $a, b \mid m$, then $\ell \mid m$.

Theorem (In UFD, lcm exists and unique up to assoc.)

Let D be a UFD, and $a = up_1^{a_1} \cdots p_r^{a_r}$, $b = vp_1^{b_1} \cdots p_r^{b_r} \in D$. Then $\ell = p_1^{\max(a_1,b_1)} \cdots p_r^{\max(a_r,b_r)}$ is an lcm of a and b, and $\ell' \in R$ is another lcm iff. ℓ' assoc. ℓ.

Proof.

We want the for all $m \in D$, $a, b \mid m \iff l \mid m$. Writing $m = wp_1^{m_1} \cdots p_r^{m_r}$ and $\ell = w' p_1^{\ell_1} \cdots p_r^{\ell_r}$, this translates into $a_i, b_i \leq m_i$ for all $i \iff \ell_i \leq m_i$ for all i. □

Lowest common multiples

Definition (lcm)

Let R be a ring, and let $a, b \in R$. An lcm of a and b is a $\ell \in R$ such that $a, b \mid \ell$, and for all $m \in R$, if $a, b \mid m$, then $\ell \mid m$.

Theorem (In UFD, lcm exists and unique up to assoc.)

Let D be a UFD, and $a = up_1^{a_1} \cdots p_r^{a_r}$, $b = vp_1^{b_1} \cdots p_r^{b_r} \in D$. Then $\ell = p_1^{\max(a_1,b_1)} \cdots p_r^{\max(a_r,b_r)}$ is an lcm of a and b, and $\ell' \in R$ is another lcm iff. ℓ' assoc. ℓ.

Example

In $\mathbb{Z}$, $\operatorname{lcm}(-6, 45) = \operatorname{lcm}\left((-1)2^1 3^1 5^0, 2^0 3^2 5^1\right) = u 2^1 3^2 5^1 = \pm 90$.

A relation between gcd and lcm

Proposition

Let D be a UFD, and let a, b in D. Then $\gcd(a,b)\operatorname{lcm}(a,b)$ is associate to ab.

Proof.

For each i, the exponent of p_i in $\gcd(a,b)\operatorname{lcm}(a,b)$ is $\min(a_i, b_i) + \max(a_i, b_i) = a_i + b_i$. $\square$

Example

In $\mathbb{Z}$, $\gcd(-6,45)\operatorname{lcm}(-6,45) = (\pm 3)(\pm 90) = \pm -6 \times 45$.

Counterexample in a non-UFD

Counter-example

Let $\gamma = 1 + i\sqrt{5} \in R = \mathbb{Z}[i\sqrt{5}] = \{x + yi\sqrt{5} \mid x, y \in \mathbb{Z}\}$.
Recall that $N(x + yi\sqrt{5}) = x^2 + 5y^2$ satisfies

$$N(\alpha\beta) = N(\alpha)N(\beta);$$

therefore, if $\alpha \mid \beta$ in R, then $N(\alpha) \mid N(\beta)$ in $\mathbb{Z}$.
Suppose $\Delta \in R$ is a gcd of $\alpha = 6 = \gamma\overline{\gamma}$ and of $\beta = 2\gamma$.
Then $\Delta \mid \alpha, \beta$, so $N(\Delta) \mid N(\alpha) = 36, N(\beta) = 24$,
so $N(\Delta) \mid \gcd_{\mathbb{Z}}(36, 24) = 12$.
Besides, for all common divisors δ of α and β in R, we must have $\delta \mid \Delta$ in R, and in particular $N(\delta) \mid N(\Delta)$ in $\mathbb{Z}$.
In particular, $2 \mid \Delta$, so $4 = N(2) \mid N(\Delta)$; similarly, $\gamma \mid \Delta$, so $6 = N(\gamma) \mid N(\Delta)$. Thus $12 = \operatorname{lcm}(4, 6) \mid N(\Delta)$.
In conclusion, necessarily $N(\Delta) = 12$; but $x^2 + 5y^2 = 12$ has no solutions, absurd. So α and β do not have a gcd in R.

The PID case

Theorem

Let D be a PID, and let $a, b \in D$. Then
$(a) + (b) = \big(\gcd(a, b)\big)$ *and* $(a) \cap (b) = \big(\operatorname{lcm}(a, b)\big)$.

Remark

Even though the elements $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are only defined up to associates, the ideals $\big(\gcd(a, b)\big)$ and $\big(\operatorname{lcm}(a, b)\big)$ are well-defined.

The PID case

Theorem

Let D be a PID, and let $a, b \in D$. Then
$(a) + (b) = \big(\gcd(a,b)\big)$ *and* $(a) \cap (b) = \big(\operatorname{lcm}(a,b)\big)$.

Proof.

Since D is a PID, we have $(a) + (b) = (g)$ for some $g \in D$. Then for all $d \in D$,

$$d \mid a, b \iff a, b \in (d) \iff (a), (b) \subseteq (d)$$
$$\iff (g) = (a) + (b) \subseteq (d) \iff d \mid g$$

so g is a gcd. $\square$

The PID case

Theorem

Let D be a PID, and let $a, b \in D$. Then $(a) + (b) = \big(\gcd(a,b)\big)$ *and* $(a) \cap (b) = \big(\operatorname{lcm}(a,b)\big)$.

Proof.

Since D is a PID, we have $(a) \cap (b) = (\ell)$ for some $\ell \in D$. Then for all $m \in D$,

$$a, b \mid m \Leftrightarrow m \in (a), (b) \Leftrightarrow m \in (a) \cap (b) = (\ell) \Leftrightarrow \ell \mid m$$

so ℓ is an lcm. $\square$

The PID case

Theorem

Let D be a PID, and let $a, b \in D$. Then $(a) + (b) = \big(\gcd(a, b)\big)$ and $(a) \cap (b) = \big(\operatorname{lcm}(a, b)\big)$.

Corollary (Bézout)

Let D be a PID, and let $a, b \in D$. There exist $c, d \in D$ such that $ac + bd = \gcd(a, b)$.

The PID case

Corollary (Bézout)

Let D be a PID, and let $a, b \in D$. There exist $c, d \in D$ such that $ac + bd = \gcd(a, b)$.

Counter-example

This is <u>false</u> if D is a UFD which is not a PID.
For example, take $D = \mathbb{Z}[x]$; we will prove later that this is a UFD, and that the elements $a(x) = x$ and $b(x) = 2$ of D are both irreducible in D.
Since $\mathbb{Z}$ is a domain, $D^\times = \mathbb{Z}^\times = \{\pm 1\}$, so $a(x)$ and $b(x)$ are not associates; therefore $\gcd(a(x), b(x)) = 1$.
However, there are no $c(x), d(x) \in D$ such that $a(x)c(x) + b(x)d(x) = 1$, since taking $x = 0$ would yield $0 + 2d(0) = 1$.
This is because $D = \mathbb{Z}[x]$ is not a PID, as $\mathbb{Z}$ is not a field.

The ED case

Lemma

Let D be a ED, let $a, b \in D$, $b \neq 0$, and let $a = bq + r$ be the Euclidean division. Then $\gcd(a, b) = \gcd(b, r)$.

Proof.

$$(a) + (b) = (a, b) = (bq + r, b) = (r, b) = (b) + (r). \qquad \square$$

The ED case

Lemma

Let D be a ED, let $a, b \in D$, $b \neq 0$, and let $a = bq + r$ be the Euclidean division. Then $\gcd(a, b) = \gcd(b, r)$.

Theorem ((Extended) Euclidean algorithm)

Divide a by b, and then b by r, ..., until $r = 0$; the last nonzero r is a gcd of a and b.
By working in reverse, we can find $c, d \in D$ such that $ac + bd = \gcd(a, b)$.

The ED case

Theorem ((Extended) Euclidean algorithm)

Divide a by b, and then b by r, $\dots$, until $r = 0$; the last nonzero r is a gcd of a and b.
By working in reverse, we can find $c, d \in D$ such that $ac + bd = \gcd(a, b)$.

Example (In $D = \mathbb{Z}$)

Take $D = \mathbb{Z}$, $a = 42$, $b = 16$. We compute

$$\begin{array}{r|l} 42 & 16 \\ \hline 10 & 2 \end{array} \qquad \begin{array}{r|l} 16 & 10 \\ \hline 6 & 1 \end{array} \qquad \begin{array}{r|l} 10 & 6 \\ \hline 4 & 1 \end{array} \qquad \begin{array}{r|l} 6 & 4 \\ \hline 2 & 1 \end{array} \qquad \begin{array}{r|l} 4 & 2 \\ \hline 0 & 2 \end{array}$$

so $\gcd(a, b) = 2$ and thus $\operatorname{lcm}(a, b) = ab/2 = 336$. Besides, $2 = 6 - 4 = 6 - (10 - 6) = 6 \times 2 - 10 = (16 - 10) \times 2 - 10 = 16 \times 2 - 10 \times 3 = 16 \times 2 - (42 - 16 \times 2) \times 3 = 16 \times 8 - 42 \times 3$, whence $\gcd(a, b) = ac + bd$ with $c = -3$, $d = 8$.

The ED case

Example (In $D = \mathbb{Q}[x]$)

Take $D = \mathbb{Q}[x]$, $a = x^3 + x$, $b = x^2 + 3$. We compute

$$\begin{array}{r|l} x^3 + x & x^2 + 3 \\ \hline -2x & x \end{array} \qquad \begin{array}{r|l} x^2 + 3 & -2x \\ \hline 3 & -\frac{1}{2}x \end{array} \qquad \begin{array}{r|l} -2x & 3 \\ \hline 0 & -\frac{2}{3}x \end{array}$$

so $\gcd(a, b) = 3 \in D^\times$, so a and b are coprime, and thus $\operatorname{lcm}(a, b) = ab$. Besides,

$$\begin{aligned} 1 = \frac{1}{3}3 = \frac{1}{3}\left((x^2+3) + \frac{1}{2}x(-2x)\right) &= \frac{1}{3}(x^2+3) + \frac{1}{6}x(-2x) \\ &= \frac{1}{3}(x^2+3) + \frac{1}{6}x\left((x^3+x) - x(x^2+3)\right) \\ &= \frac{1}{6}x(x^3+x) + \left(-\frac{1}{6}x^2 + \frac{1}{3}\right)(x^2+3) \end{aligned}$$

whence $1 = ac + bd$ with $c = \frac{1}{6}x$, $d = -\frac{1}{6}x^2 + \frac{1}{3}$.

Factorisation in polynomial rings, part 1/3: Over a field

Irreducibility in Field$[x]$

Theorem

Let F be a field, and let $P(x) \in F[x]$.

1. $F[x]^\times = F^\times = F \setminus \{0\}$.
2. *If* $\deg P = 1$, *then P is irreducible in $F[x]$.*
3. *If* $\deg P \geq 2$ *and P is irreducible in $F[x]$, then P has no roots in F.*
4. *If* $\deg P = 2$ *or* 3 *and P has no roots in F, then P is irreducible in $F[x]$.*

Proof.

1. If $PQ = 1$, then $0 = \deg PQ = \deg P + \deg Q$, so $\deg P = 0$.

$\square$

Irreducibility in Field[x]

Theorem

Let F be a field, and let $P(x) \in F[x]$.

1. $F[x]^\times = F^\times = F \setminus \{0\}$.
2. *If* $\deg P = 1$, *then P is irreducible in $F[x]$.*
3. *If* $\deg P \geq 2$ *and P is irreducible in $F[x]$, then P has no roots in F.*
4. *If* $\deg P = 2$ *or* 3 *and P has no roots in F, then P is irreducible in $F[x]$.*

Proof.

2. If $P = QR$, then $1 = \deg P = \deg Q + \deg R$, so $\deg Q = 0$ and $\deg R = 1$ or vice-versa, so $Q \in F[x]^\times$ or $R \in F[x]^\times$.

$\square$

Irreducibility in Field$[x]$

Theorem

Let F be a field, and let $P(x) \in F[x]$.

1. $F[x]^\times = F^\times = F \setminus \{0\}$.
2. *If* $\deg P = 1$, *then P is irreducible in $F[x]$.*
3. *If* $\deg P \geq 2$ *and P is irreducible in $F[x]$, then P has no roots in F.*
4. *If* $\deg P = 2$ *or* 3 *and P has no roots in F, then P is irreducible in $F[x]$.*

Proof.

3. If $\alpha \in F$ is a root of P, then $P(x) = (x - \alpha)Q(x)$, so P is reducible since $(x - \alpha), Q(x) \notin F[x]^\times$ as $\deg Q = \deg P - 1 \neq 0$.

$\square$

Irreducibility in Field$[x]$

Theorem

Let F be a field, and let $P(x) \in F[x]$.

1. $F[x]^\times = F^\times = F \setminus \{0\}$.
2. *If* $\deg P = 1$*, then* P *is irreducible in* $F[x]$.
3. *If* $\deg P \geq 2$ *and* P *is irreducible in* $F[x]$*, then* P *has no roots in* F.
4. *If* $\deg P = 2$ *or* 3 *and* P *has no roots in* F*, then* P *is irreducible in* $F[x]$.

Proof.

4. If P were reducible, one if its factors would have degree 1, whence a root. $\square$

Irreducibility in Field[x]

Theorem

Let F be a field, and let $P(x) \in F[x]$.

1. $F[x]^\times = F^\times = F \setminus \{0\}$.
2. *If* $\deg P = 1$, *then P is irreducible in $F[x]$.*
3. *If* $\deg P \geq 2$ *and P is irreducible in $F[x]$, then P has no roots in F.*
4. *If* $\deg P = 2$ *or* 3 *and P has no roots in F, then P is irreducible in $F[x]$.*

Counter-example

$(x^2+1)(x^2+2)$ is reducible in $\mathbb{R}[x]$ but has no root in $\mathbb{R}$.

Irreducibility in Field[x]

Theorem

Let F be a field, and let $P(x) \in F[x]$.

1. $F[x]^\times = F^\times = F \setminus \{0\}$.
2. *If* $\deg P = 1$, *then* P *is irreducible in* $F[x]$.
3. *If* $\deg P \geq 2$ *and* P *is irreducible in* $F[x]$, *then* P *has no roots in* F.
4. *If* $\deg P = 2$ *or* 3 *and* P *has no roots in* F, *then* P *is irreducible in* $F[x]$.

Example

$P(x) = x^2 + 1$ has no roots in $\mathbb{R}$, so it is irreducible in $\mathbb{R}[x]$.
However, $P(x) = (x - i)(x + i)$ becomes reducible in $\mathbb{C}[x]$.

Irreducibility in Field[x]

Theorem

Let F be a field, and let $P(x) \in F[x]$.

1. $F[x]^\times = F^\times = F \setminus \{0\}$.
2. *If* $\deg P = 1$, *then P is irreducible in $F[x]$.*
3. *If* $\deg P \geq 2$ *and P is irreducible in $F[x]$, then P has no roots in F.*
4. *If* $\deg P = 2$ *or* 3 *and P has no roots in F, then P is irreducible in $F[x]$.*

Example

The factorisation $\underbrace{-6}_{\in \mathbb{Q}[x]^\times} \underbrace{(2x+1)}_{\deg 1} \underbrace{(x^2+2)}_{\text{no roots}}$ is complete in $\mathbb{Q}[x]$.

Factorisation in polynomial rings, part 2/3: UFD[x] is still a UFD

Content and primitive part

Definition (Content, primitive)

Let D be a UFD, and let $F(x) \in D[x]$.
"The" content $c(F) \in D$ of $F(x)$ is "the" gcd of the coefficients of $F(x)$.
We say that $F(x)$ is primitive if $c(F) = 1$.

So for any $0 \neq F(x) \in D[x]$, we have $F(x) = c(F)pp(F)$ where $pp(F) = F/c(F) \in D[x]$ is primitive.

Example

In $\mathbb{Z}[x]$, $F(x) = 8x^3 - 6x + 12 = \underbrace{2}_{c(F) \in \mathbb{Z}} \underbrace{(4x^3 - 3x + 6)}_{pp(F) \in \mathbb{Z}[x], \text{ primitive}}$.

Remark

Every monic polynomial is primitive.

Content is multiplicative

Lemma

Let D be a UFD. For all $F(x), G(x) \in D[x]$,
$$c(FG) = c(F)c(G).$$

Proof.

Writing $F = c(F)pp(F)$, $G = c(G)pp(G)$, WLOG we assume F and G primitive. By contradiction, suppose $p \in D$ is irreducible and divides $c(FG)$. Then in $(D/pD)[x]$, $\overline{FG} = \overline{0}$, whereas $\overline{F}, \overline{G} \neq \overline{0}$ as F, G primitive.
However, p is prime as D is a UFD, so D/pD is a domain, and therefore so is $(D/pD)[x]$, absurd. □

Gauss's theorem

Theorem (Gauss)

Let D be a UFD, and let $F = \mathrm{Frac}(D)$.
Then $D[x]$ is also a UFD, whose irreducibles are exactly

1. *the constant polynomials which are irreducible in D,*
2. *the primitive polynomials which are irreducible in $F[x]$.*

Example

$\mathbb{Z}[x]$ is a UFD. The complete factorisation of
$F(x) = -6(2x+1)(x^2+2)$ in $\mathbb{Z}[x]$ is

$$\underbrace{-1}_{\in \mathbb{Z}[x]^\times} \underbrace{2}_{\text{irr}} \underbrace{3}_{\text{irr}} \underbrace{(2x+1)}_{\text{irr}} \underbrace{(x^2+2)}_{\text{irr}}.$$

Proof (1/3): They are really irreducible in $D[x]$

1. Let $p \in D$ be irreducible.
   If $p = A(x)B(x)$ with $A, B \in D[x]$, then taking degrees yields $\deg A = \deg B = 0$, so actually $A, B \in D$.
   But then A or $B \in D^\times$ since p is irreducible in D.
   WLOG $A \in D^\times$, but then $A \in D[x]^\times$.
2. Let $P(x) \in D[x]$ be primitive and irreducible in $F[x]$.
   If $P(x) = A(x)B(x)$ with $A, B \in D[x]$, then $A, B \in F[x]$, so WLOG $A \in F[x]^\times = F^\times$ as P is irreducible in $F[x]$.
   Thus A is a nonzero constant in D; but then
   $$1 = c(P) = c(AB) = c(A)c(B) = A\,c(B),$$
   so actually $A \in D^\times$.

Proof (2/3): That's all irreducibles + existence

Let $0 \neq G(x) \in D[x]$. Then $G(x) \in F[x]$, which is a PID and hence a UFD, so we can factor

$$G(x) = \lambda P_1(x) \cdots P_r(x)$$

where $\lambda \in F[x]^\times = F^\times$ and the $P_i(x)$ irreducibles in $F[x]$
Clearing denominators, we may assume that the $P_i(x)$ lie in $D[x]$ and are primitive. Write $\lambda = p/q$ with $p, q \in D$; then

$$q \mid c(q)c(G) = c(qG) = c\big(pP_1(x) \cdots P_r(x)\big) = p\, c(P_1) \cdots c(P_r) = p$$

so actually $\lambda = p/q \in D$. We factor λ in the UFD D:

$$\lambda = up_1 \cdots p_s, \quad u \in D^\times, p_j \in D \text{ irreducibles,}$$

whence $G(x) = up_1 \cdots p_s P_1(x) \cdots P_r(x)$ with $u \in D^\times = D[x]^\times$ and the p_j, P_i irreducible in $D[x]$.
In particular, if $G(x)$ is irreducible, then it must be associate to either $p \in D$ irreducible, or to $P(x) \in D[x]$ primitive and irreducible in $F[x]$.

Proof (3/3): Uniqueness

Let $P(x) \in D[x]$ irreducible. WTS $P(x)$ prime in $D[x]$, so suppose $P(x) \mid G(x)H(x)$ with $G, H \in D[x]$, so that $P(x)Q(x) = G(x)H(x)$ for some $Q(x) \in D[x]$.

1. If $P(x) = p$ irreducible in D, then $p = c(p) \mid c(p)c(Q) = c(pQ) = c(GH) = c(G)c(H)$. As $p \in D$ is prime, WLOG $p \mid c(G)$, so $p \mid G$ in $D[x]$.
2. If $P(x)$ is primitive and irreducible in $F[x]$, then $P(x)$ is prime in the UFD $F[x]$, so WLOG $P \mid G$ in $F[x]$, say $G = PR$ with $R \in F[x]$. Clear denominators: $R(x) = \frac{p}{q}S(x)$, with $p, q \in D$ and $S(x) \in D[x]$, $c(S) = 1$. Then $qG = pPS$, so

$$q = c(q) \mid c(q)c(G) = c(qG) = c(pPS) = c(p)c(P)c(S) = p$$

so $R(x) = \frac{p}{q}S(x) \in D[x]$, whence $P \mid G$ in $D[x]$. $\square$

Factorisation in polynomial rings, part 3/3: Some practical results

The rational root theorem

Theorem (Rational root theorem)

Let D be a UFD, and $A(x) = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$. If $p/q \in \operatorname{Frac}(D)$ is a root of $A(x)$ in lowest terms (meaning $\gcd(p, q) = 1$), then $p \mid a_0$ and $q \mid a_n$ in D.

Proof.

Since p/q is a root,

$$\begin{aligned} 0 = q^n A(p/q) &= q^n \left(a_n (p/q)^n + \cdots + a_1 p/q + a_0\right) \\ &= a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n. \end{aligned}$$

Thus $q \mid (-a_{n-1} p^{n-1} q - \cdots - a_1 p q^{n-2} - a_0 q^{n-1}) = -a_n p^n$.
So $a_n p^n$ contains all the irreducible factors of q; yet q and p^n have no irreducible factor in common, so all these factors come from a_n, so $q \mid a_n$.
Similarly, $p \mid a_0 q^n$, so $p \mid a_0$. □

The rational root theorem

Theorem (Rational root theorem)

Let D be a UFD, and $A(x) = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$. If $p/q \in \operatorname{Frac}(D)$ is a root of $A(x)$ in lowest terms (meaning $\gcd(p, q) = 1$), then $p \mid a_0$ and $q \mid a_n$ in D.

Example

Let $A(x) = x^3 - 6x + 2 \in \mathbb{Z}[x]$.
If $p/q \in \mathbb{Q}$ were a root of $A(x)$ in lowest terms, then $p \mid 2$ and $q \mid 1$. So the only possible rational roots are ± 1 and ± 2; as none of those is a root, $A(x)$ has no rational root.
As $\mathbb{Q}$ is a field, if $A(x)$ were reducible in $\mathbb{Q}[x]$, **since** $\deg A = 3$, it would have a root in $\mathbb{Q}$.
So $A(x)$ is irreducible in $\mathbb{Q}[x]$. Since it is also primitive, it is irreducible in $\mathbb{Z}[x]$ as well.

Eisenstein's criterion

Theorem (Eisenstein's criterion)

Let D be a UFD, and $A(x) = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$.
If $c(A) = 1$ and if there exists $p \in D$ irreducible such that

$$p \mid a_{n-1}, \cdots, a_1, a_0 \text{ , } \textit{but } p^2 \nmid a_0,$$

then $A(x)$ is irreducible in $D[x]$ and in $\mathrm{Frac}(D)[x]$.

In this case, we say that $A(x)$ is Eisenstein at p.

Example

$A(x) = x^3 - 6x + 2 \in \mathbb{Z}[x]$ is Eisenstein at $p = 2$:
Indeed, $p \mid 0, 6, 2$ and $p^2 \nmid 2$.
Therefore, $A(x)$ is irreducible in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Eisenstein's criterion

Theorem (Eisenstein's criterion)

Let D be a UFD, and $A(x) = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$. If $c(A) = 1$ and if there exists $p \in D$ irreducible such that

$$p \mid a_{n-1}, \cdots, a_1, a_0 \text{ , but } p^2 \nmid a_0,$$

then $A(x)$ is irreducible in $D[x]$ and in $\operatorname{Frac}(D)[x]$.

Counter-example

$A(x) = x^2 + 6x + 9 \in \mathbb{Z}[x]$ is not Eisenstein at $p = 3$ even though $p \mid 6, 9$, because $p^2 \mid 9$. Actually, $A(x) = (x+3)^2$ is reducible both in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

Counter-example

$A(x) = x^2 + 1 \in \mathbb{Z}[x]$ is not Eisenstein at any $p \in \mathbb{Z}$, but it is still irreducible in $\mathbb{Q}[x]$ since it has degree 2 and no roots in $\mathbb{Q}$, and therefore also irreducible in $\mathbb{Z}[x]$ since it is primitive.

Proof of Eisenstein's criterion

Suppose that $A(x) = G(x)H(x)$ with $G, H \in D[x]$.
In $(D/pD)[x]$, we have $\overline{G}(x)\overline{H}(x) = \overline{A}(x) = \overline{a_n}x^n$ with $\overline{a_n} \neq \overline{0}$ as $p \nmid a_n$ since A is primitive.
Write $\overline{G}(x) = \overline{g_R}x^R + \cdots + \overline{g_r}x^r$, $\overline{H}(x) = \overline{h_S}x^S + \cdots + \overline{h_s}x^s$ with $\overline{g_R}, \overline{g_r}, \overline{h_S}, \overline{h_s} \neq \overline{0}$. If $R > r$ or $S > s$, then

$$\overline{a_n}x^n = \overline{A}(x) = \overline{G}(x)\overline{H}(x) = \overline{g_R}\,\overline{h_S}x^{R+S} + \cdots + \overline{g_r}\,\overline{h_s}x^{r+s},$$

absurd since $\overline{g_R}\,\overline{h_S}, \overline{g_r}\,\overline{h_s} \neq \overline{0}$ as D/pD is a domain as p prime.
So $R = r$, and $S = s$; besides $R + S = n$, so $\deg G = \deg \overline{G} = R$ and $\deg H = \deg \overline{H} = S$, whence $G(x) = g_R x^R + pG_1(x)$ with $G_1(x) \in D[x]$, $\deg G_1 < \deg G$, and similarly $H(x) = h_S x^S + pH_1(x)$.
If $R, S > 0$, then $p^2 \mid p^2 G_1(0)H_1(0) = G(0)H(0) = a_0$, absurd.
WLOG, $R = 0$, so $G \in D$ is constant, but then $G = c(G) \mid c(G)c(H) = c(A) = 1$ so $G \in D^\times = D[x]^\times$.
Thus A is irreducible in $D[x]$, and hence in $\mathrm{Frac}(D)[x]$. $\square$