Chapter 9: Domains

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 8510, Visual Algebra

Divisibility and factorization

Previously, we saw how to extend a familiar construction (fractions) from $\mathbb{Z}$ to other commutative rings.

Now, we'll do the same for other basic features of the integers.

Blanket assumption

Unless otherwise stated, R is an integral domain, and $R^* := R \setminus \{0\}$.

The integers have several basic properties that we usually take for granted:

- every nonzero number can be factored uniquely into primes;
- any two numbers have a unique greatest common divisor and least common multiple;
- for a and $b \neq 0$ the division algorithm gives us

$$a = qb + r, \qquad \text{where } |r| < |b|.$$

- the Euclidean algorithm uses the divison algorithm to find GCDs.

These need not hold in integrals domains! We would like to understand this better.

Divisibility

Definition

If $a, b \in R$, then a divides b, or b is a multiple of a if $b = ac$ for some $c \in R$. Write $a \mid b$.

If $a \mid b$ and $b \mid a$, then a and b are associates, written $a \sim b$.

Examples

- In $\mathbb{Z}$: n and $-n$ are associates.
- In $\mathbb{R}[x]$: $f(x)$ and $c \cdot f(x)$ are associates for any $c \neq 0$.

This defines an equivalence relation on R^*, and partitions it into equivalence classes.

- The unique maximal class is $\{0\}$ (because $r \mid 0$, $\forall r \in R$).
- The unique minimal class is $U(R)$ (because $u \mid r$, $\forall u \in U(R)$, $r \in R$).
- Elements in the minimal classes of $R - U(R)$ are called irreducible.

Exercise

The following are equivalent for $a, b \in R$:

(i) $a \sim b$, (ii) $a = bu$ for some $u \in U(R)$, (iii) $(a) = (b)$.

Divisibility via ideals

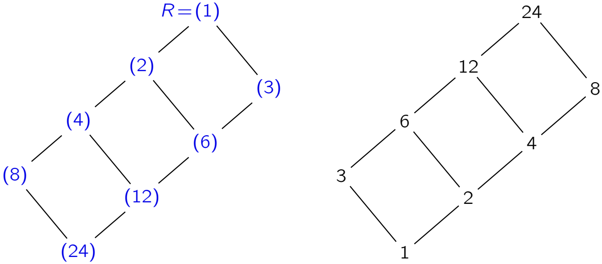
Remark

For nonzero $a, b \in R$,

$$a \mid b \quad \Leftrightarrow \quad (b) \subseteq (a).$$

Key idea

Questions about divisibility are cleaner when translated into the language of ideals.



subring lattice; $\langle d \rangle = (d)$ *divisor lattice*

Divisibility is well-behaved in rings where every ideal is generated by a single element.

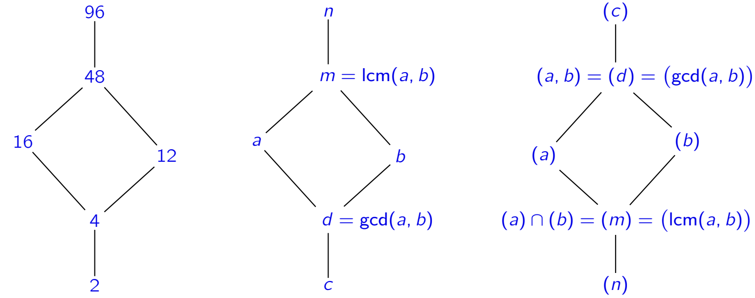
Divisibility via ideals

Remark

Divisors and multiples of $a \in R$ are easily identified in the ideal lattice:

1. (nonzero) multiples are "above" (a),
2. divisors are "below" (a).

The GCD and LCM have nice interpretations in the divisor and ideal lattices.



Key idea

Everything behaves nicely if all ideals have the form $I = (a)$, for some $a \in R$.

Divisibility, factorization, and principal ideals

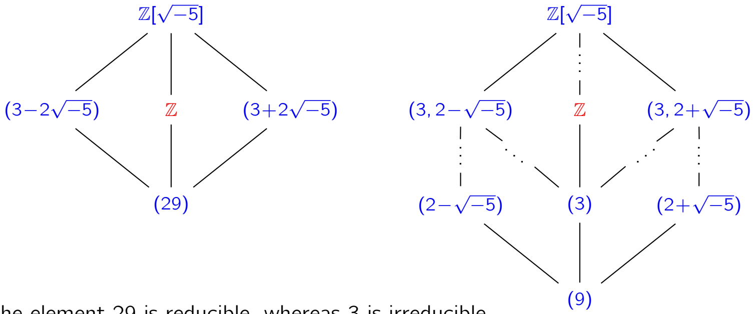
Definition

An ideal generated by a single element $a \in R$, denoted $I = (a)$, is called a principal ideal.

If non-principal ideals lurk, we can lose nice properties like unique factorization.

Consider the following examples in $\mathbb{Z}[\sqrt{-5}]$:

$$29 = (3 - 2\sqrt{-5})(3 + 2\sqrt{-5}), \qquad 3 \cdot 3 = 9 = (2 - \sqrt{-5})(2 + \sqrt{-5}).$$



- The element 29 is reducible, whereas 3 is irreducible.
- Neither of the ideals (3) and (29) are prime in $\mathbb{Z}[\sqrt{-5}]$.

Principal ideal domains

Definition

If every ideal of R is principal, then R is a principal ideal domain (PID).

Divisibility via ideals: a summary

Let R be an integral domain.

1. u is a unit iff $(u) = R$,
2. $a \mid b$ iff $(b) \subseteq (a)$,
3. a and b are associates iff $(a) = (b)$.
4. a is irreducible iff there is no $(b) \supsetneq (a)$, i.e., if (a) *is a maximal principal ideal*.

The following are all PIDs (stated without proof):

- the integers $\mathbb{Z}$,
- any field F,
- the ring $F[x]$.

The ring $R = \mathbb{Z}[x]$ is *not* a PID: x is irreducible but $(x) \subsetneq (x, 2) \subsetneq R$.

Key idea

Divisibility and factorization are well-behaved in PIDs.

Prime ideals, prime elements, and irreducibles

Euclid's lemma (300 B.C.)

If a prime p divides ab, then it must divide a or b.

In the language of ideals:

If (a non-unit) p is prime, then $(ab) \subseteq (p)$ implies either $(a) \subseteq (p)$ or $(b) \subseteq (p)$.

Definition

An element $p \in R$ is prime if it is not a unit, and one of the equivalent conditions holds:

- $p \mid ab$ implies $p \mid a$ or $p \mid b$
- $(ab) \subseteq (p)$ implies $(a) \subseteq (p)$ or $(b) \subseteq (p)$.

Compare this to what it means for p to be irreducible: $a \mid p \Rightarrow a \sim p$ $(a \notin U(R))$.

These concepts coincide in PIDs (like $\mathbb{Z}$), but not in all integral domains.

Irreducibles and primes

Recall that a nonzero $p \notin U(R)$ is:

- irreducible if $\underbrace{p = ab}_{(ab)=(p)} \;\Rightarrow\; \underbrace{b \in U(R)}_{(a)=(p)}$ or $\underbrace{a \in U(R)}_{(b)=(p)}$.
- prime if $\underbrace{p \mid ab}_{(ab)\subseteq(p)} \;\Rightarrow\; \underbrace{p \mid a}_{(a)\subseteq(p)}$ or $\underbrace{p \mid b}_{(b)\subseteq(p)}$.

Proposition

In an integral domain R, if $p \neq 0$ is prime, then p is irreducible.

Proof (elementwise)

Suppose p is prime, but (for sake of contradiction) reducible. Then $p = ab$; $a, b \notin U(R)$.

Then (wlog) $p \mid a$, so $a = pc$ for some $c \in R$. Now,

$$p = ab = (pc)b = p(cb)\,.$$

This means that $cb = 1$, and thus $b \in U(R)$. Therefore, p is prime. □

Irreducibles and primes

Recall that a nonzero $p \notin U(R)$ is:

- irreducible if $\underbrace{p = ab}_{(ab)=(p)} \;\Rightarrow\; \underbrace{b \in U(R)}_{(a)=(p)}$ or $\underbrace{a \in U(R)}_{(b)=(p)}$.
- prime if $\underbrace{p \mid ab}_{(ab)\subseteq(p)} \;\Rightarrow\; \underbrace{p \mid a}_{(a)\subseteq(p)}$ or $\underbrace{p \mid b}_{(b)\subseteq(p)}$.

Proposition

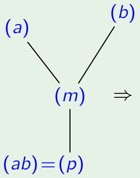
In an integral domain R, if $p \neq 0$ is prime, then p is irreducible.

Proof (idealwise; contrapositive)

If p is reducible, $\underbrace{(p) = (ab)}_{p=ab}$ for $(p) \subsetneq (a)$ and $(p) \subsetneq (b)$.

Then, we have $\underbrace{(ab) \subseteq (p)}_{p \mid ab}$ but $\underbrace{(a) \not\subseteq (p)}_{p \nmid a}$ and $\underbrace{(b) \not\subseteq (p)}_{p \nmid b}$.

Therefore, p is not prime.



$\Rightarrow$ $(a) \not\subseteq (p)$ and $(b) \not\subseteq (p)$

Prime ideals in a PID

Proposition

In a PID, every irreducible is prime.

Proof

m is irreducible	$\Longleftrightarrow$	(m) is a max'l principal ideal	*always*
	$\Longleftrightarrow$	(m) is maximal	*in a PID*
	$\Longrightarrow$	(m) is prime	*always*
	$\Longleftrightarrow$	m is prime	*always*

Corollary

In a PID, every nonzero prime ideal is maximal.

Proof

In any intergral domain, (nonzero) prime $\Rightarrow$ irreducible. □

For $m \neq 0$ in a general integral domain:

$$\begin{array}{ccccc} (m) \text{ is maximal} & \Longrightarrow & (m) \text{ is prime} & \Longleftrightarrow & m \text{ is prime} \\ & \Longrightarrow & m \text{ is irreducible} & \Longleftrightarrow & (m) \text{ is max'l principal} \end{array}$$

Non-prime irreducibles, and non-unique factorization

Caveat: Irreducible $\not\Rightarrow$ prime

In the ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$,

$$2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3, \quad \text{but} \quad 2 \nmid (1 \pm \sqrt{-5}).$$

Thus, 2 (and 3) are irreducible but not prime.

When irreducibles fail to be prime, we can lose nice properties like unique factorization.

Things can get really bad: not even the factorization *lengths* need be the same!

For example:

- $30 = 2 \cdot 3 \cdot 5 = -\sqrt{-30} \cdot \sqrt{-30} \in \mathbb{Z}[\sqrt{-30}]$,
- $81 = 3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}) \in \mathbb{Z}[\sqrt{-14}]$.

For another example, in the ring $R = \mathbb{Z}[x^2, x^3] = \{a_0 + a_2x^2 + a_3x^3 + \cdots + a_nx_n \mid a_i \in \mathbb{Z}\}$,

$$x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3.$$

The element $x^2 \in R$ is not prime because $x^2 \mid x^3 \cdot x^3$ yet $x^2 \nmid x^3$ in R.

Greatest common divisors & least common multiples

Proposition

If $I \subseteq \mathbb{Z}$ is an ideal, and $a \in I$ is its smallest positive element, then $I = (a)$.

Proof

Pick any positive $b \in I$. Write $b = aq + r$, for $q, r \in \mathbb{Z}$ and $0 \leq r < a$.

Then $r = b - aq \in I$, so $r = 0$. Therefore, $b = qa \in (a)$. □

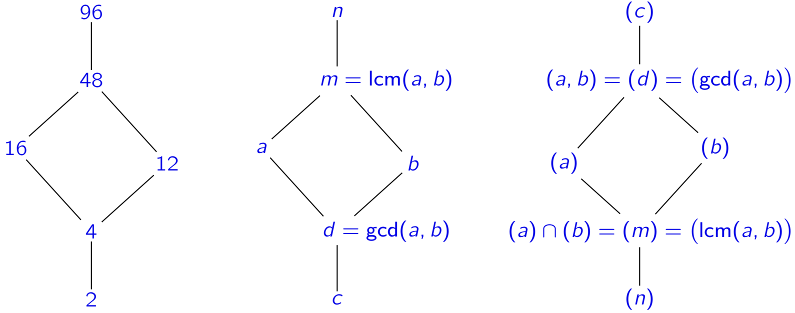
Definition

Given $a, b \in R$ in an integral domain,

- $d \in R$ is a common divisor if $d \mid a$ and $d \mid b$.
- d is a greatest common divisor (GCD) if $c \mid d$ for every common divisor c.
- $m \in R$ is a common multiple if $a \mid m$ and $b \mid m$.
- $m \in R$ is a least common multiple (LCM) if $m \mid n$ for every common multiple n.

Greatest common divisors & least common multiples

The GCD and LCM have nice interpretations in the divisor and ideal lattices.



This is how we'll prove their existence and uniqueness in a PID.

Note that ab is a common multiple of a and b, so $(ab) \subseteq (a) \cap (b)$.

Nice properties of PIDs

Proposition

If R is a PID, then any $a, b \in R^*$ have a GCD, $d = \mathbf{gcd}(a, b)$.

It is *unique up to associates*, and can be written as $d = xa + yb$ for some $x, y \in R$.

Proof

Existence. The ideal generated by a and b is

$$I = (a, b) = \{ua + vb \mid u, v \in R\}.$$

Since R is a PID, we can write $I = (d)$ for some $d \in I$, and so $d = xa + yb$.

Since $a, b \in (d)$, both $d \mid a$ and $d \mid b$ hold.

If c is a divisor of a & b, then $c \mid xa + yb = d$, so d is a GCD for a and b. ✓

Uniqueness. If d' is another GCD, then $d \mid d'$ and $d' \mid d$, so $d \sim d'$. ✓ □

The second statement above is called Bézout's identity.

Noetherian rings (weaker than being a PID)

A ring is Noetherian if it satisfies any of the three equivalent conditions.

Proposition

Let R be a ring. The following are equivalent:

(i) Every ideal of R is finitely generated.

(ii) Every ascending chain of ideals stabilizes. (*"ascending chain condition"*)

(iii) Every nonempty family of ideals has a maximal element. (*"maximal condition"*)

Proof (sketch)

$(1 \Rightarrow 2)$: Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain with $I = \bigcup_{j=1}^{\infty} I_j = (a_1, \ldots, a_n)$.

$(2 \Rightarrow 3)$: Let S be a nonempty family of ideals.

Take $I_1 \in S$. If it isn't maximal, take some $I_2 \supsetneq I_1$ in S. Repeat; this process must stop.

$(3 \Rightarrow 1)$: Given I, let $S = \{\text{f.g. } J \trianglelefteq I\}$, with max'l element $M \subseteq I$. Suppose $a \in I - M$.

Then $M \subsetneq (M, a) \subseteq I \;\Rightarrow\; (M, a) = I$. $\square$

We can define left-Noetherian and right-Noetherian rings analogously.

Unique factorization domains

Definition

An integral domain is a unique factorization domain (UFD) if:

(i) It is atomic: every nonzero nonunit is a product of irreducibles;

(ii) Every irreducible is prime.

Examples

1. $\mathbb{Z}$ is a UFD: Every $n \in \mathbb{Z}$ can be uniquely factored as a product of irreducibles (primes):

$$n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$

   This is the *fundamental theorem of arithmetic*.

2. The ring $\mathbb{Z}[x]$ is a UFD, because every polynomial can be factored into irreducibles. It is not a PID because the following ideal is not principal:

$$(2, x) = \{ f(x) \mid \text{ the constant term is even} \}.$$

3. The ring $\mathbb{Q}[x, x^{1/2}, x^{1/4}, \dots]$ has no irreducibles.

4. The ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

5. We've shown that (ii) holds for PIDs. Next, we will see that (i) holds as well.

Unique factorization domains

Theorem

If R is a PID, then R is a UFD.

Proof

We need to show Condition (i) holds: every element is a product of irreducibles.

We'll show that if this fails, we can construct

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots ,$$

which is impossible in a PID. (They are Noetherian.)

Define

$$X = \big\{ a \in R^* \setminus U(R) \mid a \text{ can't be written as a product of irreducibles} \big\}.$$

If $X \neq \emptyset$, then pick $a_1 \in X$. Factor this as $a_1 = a_2 b$, where $a_2 \in X$ and $b \notin U(R)$. Then $(a_1) \subsetneq (a_2) \subsetneq R$, and repeat this process. We get an ascending chain

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

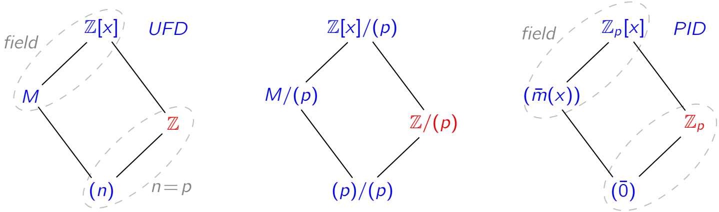
that does not stabilize. Since this is impossible in a PID, $X = \emptyset$. □

Maximal ideals of $\mathbb{Z}[x]$

Let $M \trianglelefteq \mathbb{Z}[x]$ be a maximal ideal.

The intersection $M \cap \mathbb{Z} = (n)$, and by the diamond theorem, $\underbrace{\mathbb{Z}[x]/M}_{\text{field}} \cong \underbrace{\mathbb{Z}/(n)}_{\text{field}}$, so $n = p$.

Reducing mod p gives a PID, $\mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$, and so $M/(p) = (\bar{m}(x))$ is principal.



The original ideal in $\mathbb{Z}[x]$ must have the form

$$M = \big(m(x),\, p\cdot f_1(x), \dots, p\cdot f_m(x)\big) = \big(p,\, m(x)\big),$$

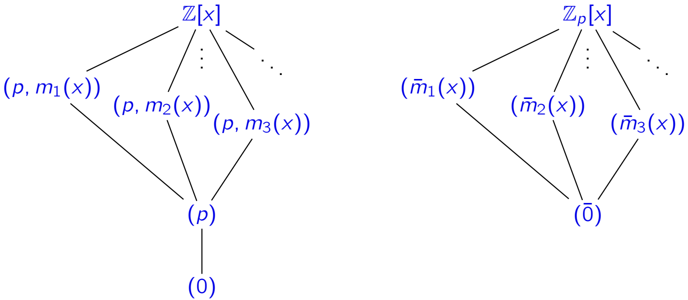
where $m(x)$ modulo p is irreducible in $\mathbb{Z}_p[x]$.

Maximal ideals of $\mathbb{Z}[x]$

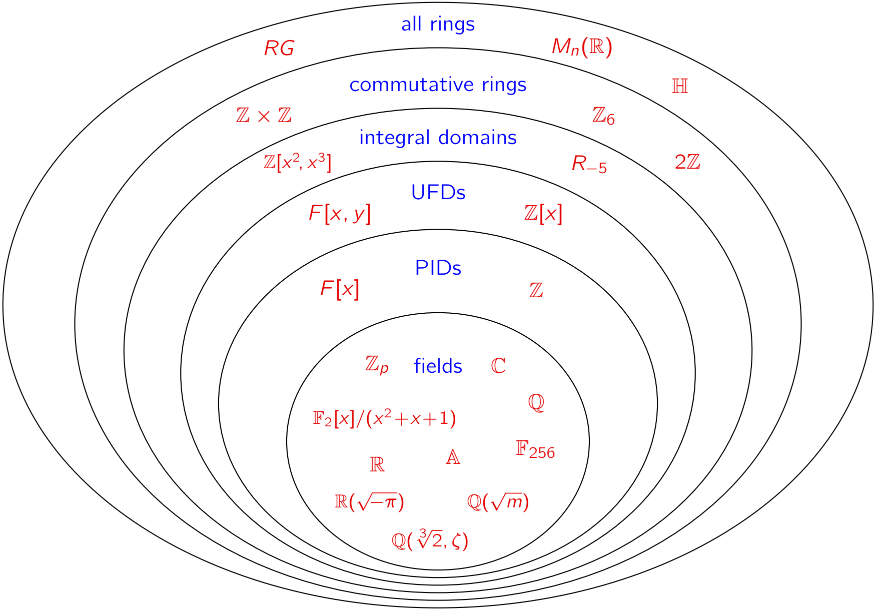
Proposition

There is a biijection between:

- maximal ideals of $\mathbb{Z}_p[x]$, and
- polynomials $m(x) \in \mathbb{Z}[x]$ that remain irreducible modulo p.



Summary of ring types



The Euclidean algorithm

Around 300 B.C., Euclid wrote his famous book, the *Elements*, in which he described what is now known as the Euclidean algorithm:

Proposition VII.2 (Euclid's *Elements*)

Given two numbers not prime to one another, to find their greatest common measure.

The algorithm works due to two key observations:

- If $a \mid b$, then $\gcd(a,b) = a$;
- If $a = bq + r$, then $\gcd(a,b) = \gcd(b,r)$.

This is best seen by an example: Let $a = 654$ and $b = 360$.

$$\begin{aligned} 654 &= 360 \cdot 1 + 294 \qquad & \gcd(654,360) &= \gcd(360,294) \\ 360 &= 294 \cdot 1 + 66 & \gcd(360,294) &= \gcd(294,66) \\ 294 &= 66 \cdot 4 + 30 & \gcd(294,66) &= \gcd(66,30) \\ 66 &= 30 \cdot 2 + 6 & \gcd(66,30) &= \gcd(30,6) \\ 30 &= 6 \cdot 5 & \gcd(30,6) &= 6. \end{aligned}$$

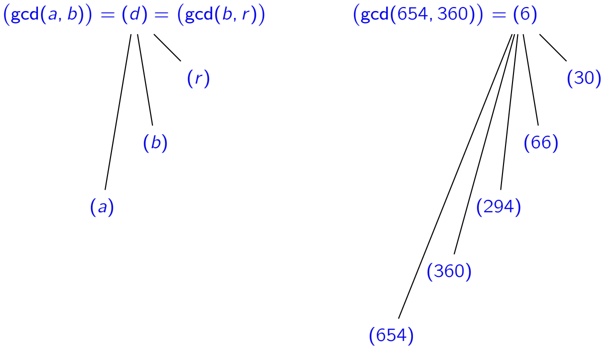
We conclude that $\gcd(654,360) = 6$.

The Euclidean algorithm in terms of ideals

Let's see that example again: Let $a = 654$ and $b = 360$.

$$\begin{aligned} 654 &= 360 \cdot 1 + 294 & \gcd(654, 360) &= \gcd(360, 294) \\ 360 &= 294 \cdot 1 + 66 & \gcd(360, 294) &= \gcd(294, 66) \\ 294 &= 66 \cdot 4 + 30 & \gcd(294, 66) &= \gcd(66, 30) \\ 66 &= 30 \cdot 2 + 6 & \gcd(66, 30) &= \gcd(30, 6) \\ 30 &= 6 \cdot 5 & \gcd(30, 6) &= 6. \end{aligned}$$

We conclude that $\gcd(654, 360) = 6$.



Euclidean domains

Loosely speaking, a Euclidean domain is a ring for which the Euclidean algorithm works.

Definition

An integral domain R is Euclidean if it has a degree function $d\colon R^* \to \mathbb{Z}$ satisfying:

(i) non-negativity: $d(r) \geq 0 \quad \forall r \in R^*$.

(ii) monotonicity: if $a \mid b$, then $d(a) \leq d(b)$,

(iii) division-with-remainder property: For all $a, b \in R$, $b \neq 0$, there are $q, r \in R$ such that

$$a = bq + r \qquad \text{with} \qquad r = 0 \quad \text{or} \quad d(r) < d(b)\,.$$

Note that Property (ii) could be restated to say: $d(a) \leq d(ab)$ *for all* $a, b \in R^*$.

Since 1 divides every $x \in R$,

$$d(1) \leq d(x), \qquad \text{for all } x \in R.$$

Similarly, if x divides 1, then $d(x) \leq d(1)$. Elements that divide 1 are the units of R.

Proposition

If u is a unit, then $d(u) = d(1)$. □

The division algorithm in $R = \mathbb{Z}$

The integers are a Euclidean domain with degree function

$$d\colon \mathbb{Z}^* \longrightarrow \mathbb{Z}, \qquad d(n) = |n|.$$

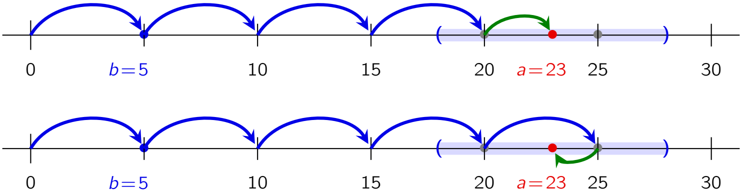
The division algorithm takes $a, b \in R$, $b \neq 0$, and finds $q, r \in R$ such that

$$a = bq + r \qquad \text{with} \qquad r = 0 \quad \text{or} \quad d(r) < d(b)\,.$$

Note that q and r are not unique!

There are two possibilities for q and r when dividing $b = 5$ into $a = 23$:

$$23 = 4 \cdot 5 + 3, \qquad\qquad 23 = 5 \cdot 5 + (-2).$$



Euclidean domains

Examples

- $R = \mathbb{Z}$ is Euclidean, with $d(r) = |r|$.
- $R = F[x]$ is Euclidean if F is a field. Define $d(f(x)) = \deg f(x)$.
- The Gaussian integers
$$\mathbb{Z}[\sqrt{-1}] = \{a + bi \mid a, b \in \mathbb{Z}\}$$
is Euclidean with degree function $d(a + bi) = a^2 + b^2$.

Proposition

If R is Euclidean, then $U(R) = \{x \in R^* \mid d(x) = d(1)\}$.

Proof

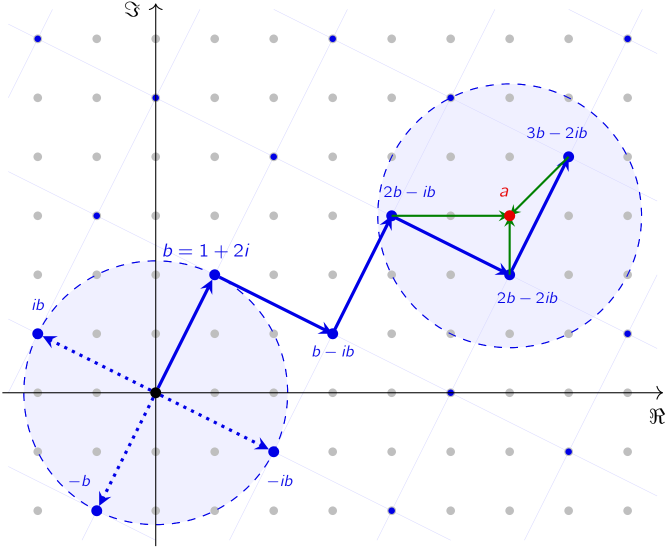
We've already established "$\subseteq$". For "$\supseteq$", Suppose $x \in R^*$ and $d(x) = d(1)$.

Write $1 = qx + r$ for some $q \in R$, and $r = 0$ or $d(r) < d(x) = d(1)$.

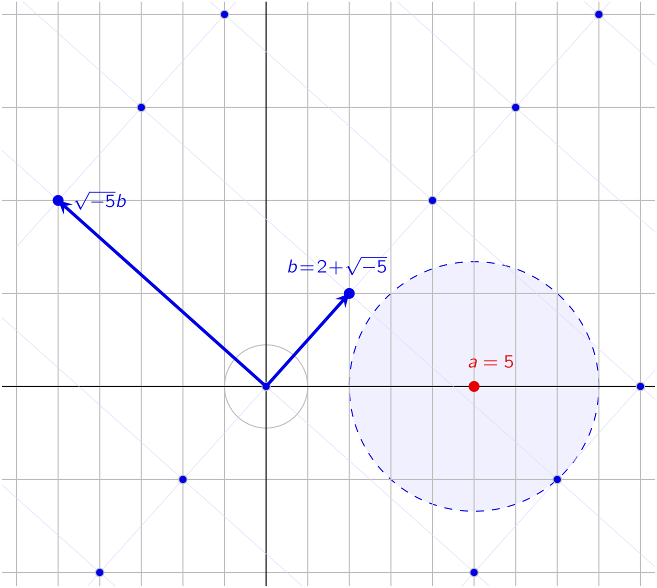
But $d(r) < d(1)$ is impossible, and so $r = 0$, which means $qx = 1$ and hence $x \in U(R)$. $\square$

The division algorithm in the Gaussian integers

$$6+3i = a = (2-i)b+2 = (2-2i)b+i = (3-2i)b+(-1-i)$$

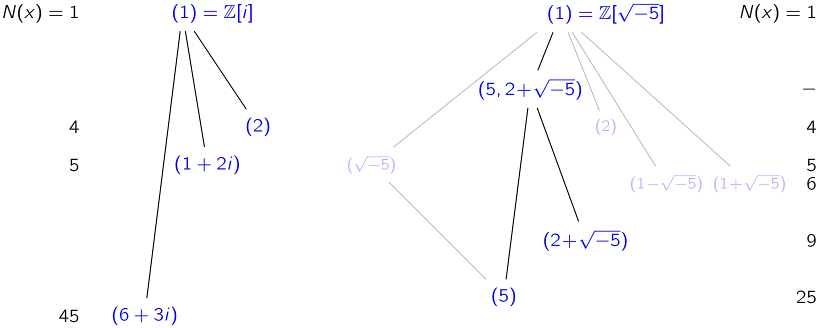


Failure of the division algorithm in $R_{-5} = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$



The Euclidean algorithm in terms of principal ideals and lattices

- $\gcd(6+3i, 1+2i)=1$ in $\mathbb{Z}[i]$: (1) is the min'l princ. ideal containing $(6+3i)$ & $(1+2i)$.
- $\gcd(5, 2+\sqrt{-5})=1$ in $\mathbb{Z}[\sqrt{-5}]$: (1) is the min'l princ. ideal containing (5) & $(2+\sqrt{-5})$.



$$\underbrace{6+3i}_{=a} = \underbrace{(1+2i)}_{=b}(2-i)\underbrace{+2}_{=r}$$

$$5 \neq (2+\sqrt{-5})q + r, \quad N(r) < N(b) = 9$$

Note that there are only four principal ideals of $\mathbb{Z}[\sqrt{-5}]$ of norm less than $N(2+\sqrt{-5}) = 9$!

Euclidean domains and PIDs

Proposition

Every Euclidean domain is a PID.

Proof

Let $I \neq 0$ be an ideal of R and pick some $b \in I$ with $d(b)$ minimal.

Pick $a \in I$, and write

$$a = bq + r, \qquad \text{where } r = 0 \text{ or } \underbrace{0 < d(r) < d(b)}_{\text{impossible by minimality}}.$$

Therefore, $r = 0$, which means $a = bq \in (b)$.

Since a was arbitrary, $I = (b)$. □

Therefore, non-PIDs like the following cannot be Euclidean:

(i) $\mathbb{Z}[\sqrt{-5}]$, (ii) $\mathbb{Z}[x]$, (iii) $F[x, y]$.

Quadradic fields

The quadratic field for a square-free $m \in \mathbb{Z}$ is

$$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{Q}\}.$$

Proposition (exercise)

In $\mathbb{Q}[x]$, since $x^2 - m$ is irreducible, it generates a maximal ideal, and there's an isomorphism

$$\mathbb{Q}[x]/(x^2 - m) \longrightarrow \mathbb{Q}(\sqrt{m}), \qquad f(x) + I \longmapsto f(\sqrt{m}).$$

Definition

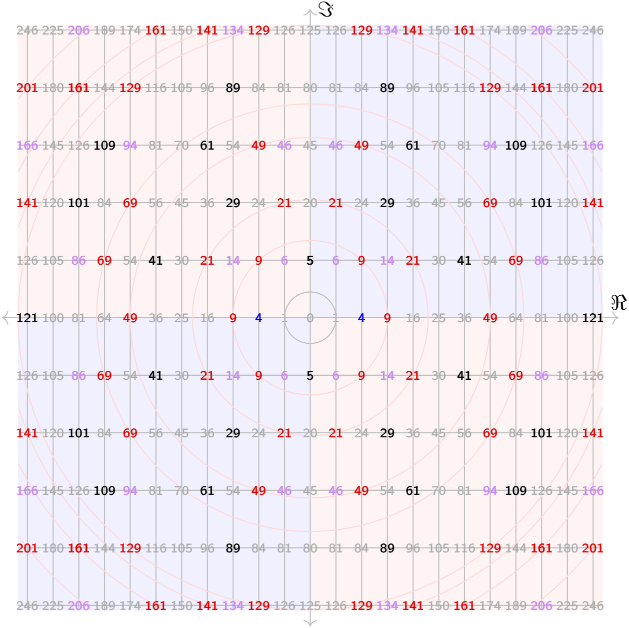
The field norm of $\mathbb{Q}(\sqrt{m})$ is

$$N\colon \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}, \qquad N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2$$

Remarks (exercises)

- The field norm is multiplicative: $N(xy) = N(x)N(y)$.
- If $m < 0$ and $z = a + b\sqrt{m} \in \mathbb{C}$, then $N(a + b\sqrt{m}) = z\bar{z} = |z|^2$.
- If $m > 0$, then $N(x)$ isn't a classic "norm" – it can take negative values.

Norms of elements in $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{-5})$



Quadradic integers

Every number in $\mathbb{Z}[\sqrt{m}]$ is a root of a monic degree-2 polynomial:

$$a + b\sqrt{m} \qquad \text{is a root of} \qquad f(x) = x^2 - 2ax + (a^2 - b^2 m) \in \mathbb{Z}[x].$$

If $m \equiv 1 \bmod 4$, then

$$\mathbb{Z}\left[\tfrac{1+\sqrt{m}}{2}\right] = \left\{a + b\tfrac{1+\sqrt{m}}{2} \mid a, b \in \mathbb{Z}\right\} = \left\{\tfrac{c}{2} + \tfrac{d\sqrt{m}}{2} \mid c \equiv d \pmod 2\right\}$$

also contains roots of monic polynomials:

$$\tfrac{a+b\sqrt{m}}{2} \qquad \text{is a root of} \qquad f(x) = x^2 - ax + \tfrac{a^2-b^2m}{4} \in \mathbb{Z}[x].$$

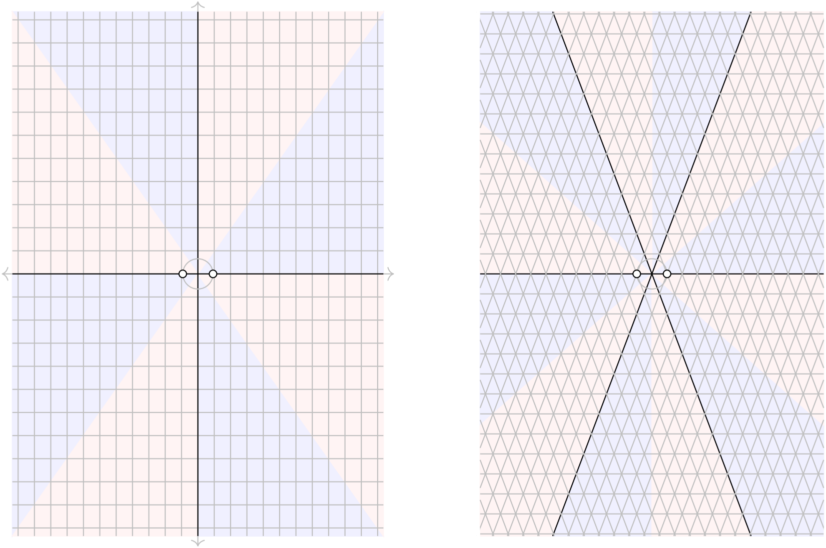
Definition

For a square-free $m \in \mathbb{Z}$, the ring R_m of quadratic integers is the subring of $\mathbb{Q}(\sqrt{m})$ consisting of roots of monic quadratic polynomials in $\mathbb{Z}[x]$:

$$R_m = \begin{cases} \mathbb{Z}[\sqrt{m}] & m \equiv 2 \text{ or } 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & m \equiv 1 \pmod 4 \end{cases}$$

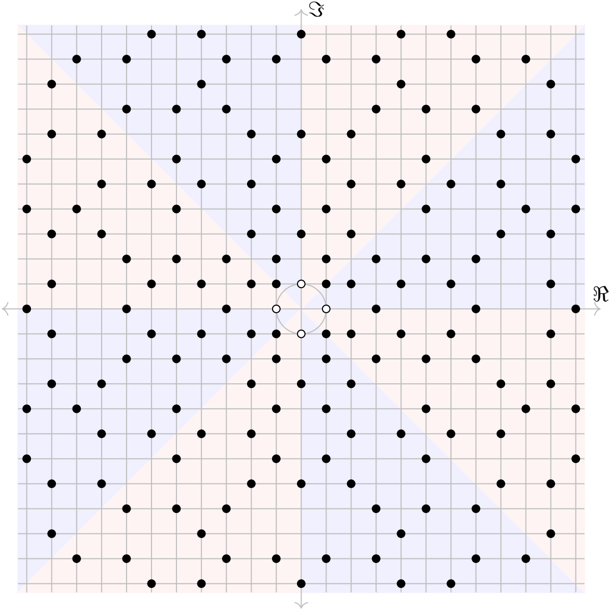
These are subrings of the algebraic integers, the roots of polynomials, and the algebraic numbers, the roots of all polynomials in $\mathbb{Z}[x]$.

Examples: $R_{-2} = \mathbb{Z}[\sqrt{-2}]$ and $R_{-7} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right] \subseteq \mathbb{C}$

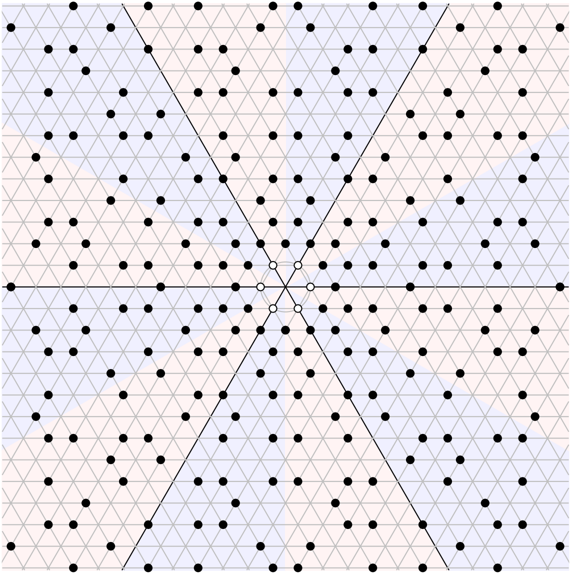


"*rectangular*" "*triangular*"

Primes in the Gaussian integers: $R_{-1} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$

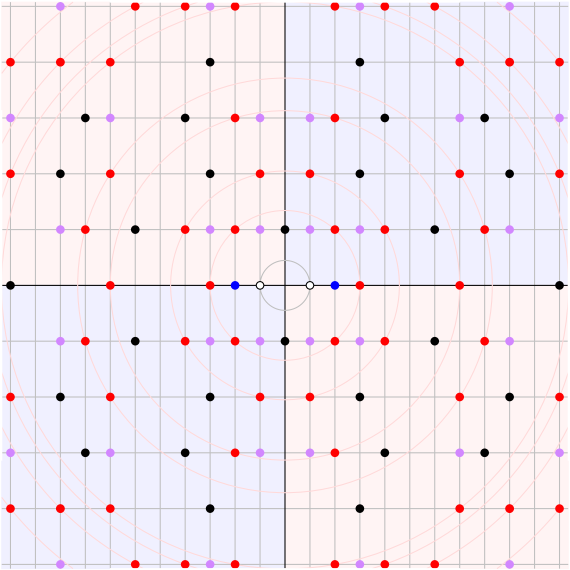


Primes in the Eisenstein integers: $R_{-3} = \left\{ a + \omega b \mid a, b \in \mathbb{Z} \right\}$, $\omega = \frac{1+\sqrt{-3}}{2}$



Primes in $R_{-5} = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

Units are white, primes are **black**, non-prime irreducibles are **blue**, **red** and **purple**.



Units, primes, and irreducibles in algebraic integer rings

The field norm of $z \in R_m$ is an integer, even in $\mathbb{Z}\big[\frac{1+\sqrt{m}}{2}\big]$:

$$N\big(a + b\tfrac{1+\sqrt{m}}{2}\big) = a^2 + ab + \tfrac{1-m}{4}b^2 \in \mathbb{Z}, \qquad \text{if } m \equiv 1 \bmod 4.$$

This, with $N(xy) = N(x)N(y)$, means that $u \in U(R_m)$ iff $N(u) = \pm 1$.

Units in R_m

- R_{-1} has 4 units: ± 1 and $\pm i$ (solutions to $N(a + bi) = a^2 + b^2 = 1$).
- R_{-3} has 6 units: ± 1, and $\pm\frac{1\pm\sqrt{-3}}{2}$ (solutions to $N(a + b\sqrt{-3}) = a^2 + 3b^2 = 1$).
- $U(R_m) = \{\pm 1\}$ for all other $m < 0$.
- If $m \geq 0$, then R_m has infinitely many units – solutions to Pell's equation:

$$N(a + b\sqrt{m}) = a^2 - b^2 m = \pm 1.$$

The norm is useful for determining the primes and irreducibles in R_m.

Non-prime irreducibles lead to multiple elements with the same norm. In R_{-5}:

$$3 \cdot 3 = 9 = (2 + \sqrt{-5})(2 - \sqrt{-5}) \quad \Rightarrow \quad N(3) = N(2 + \sqrt{-5}) = 9.$$

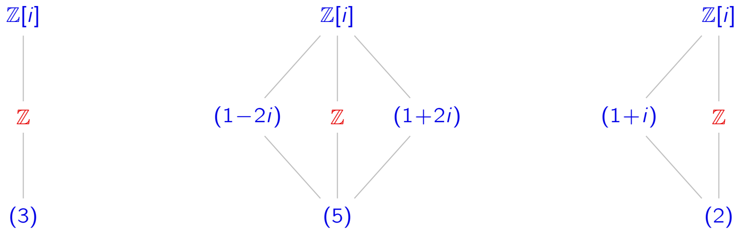
If $N(x)$ is prime, then x is prime in R_m, but not conversely.

Primes in R_m

Consider a prime $p \in \mathbb{Z}$ but in the larger ring R_m. There are three possible behaviors:

- p **splits** if $(p) = \mathfrak{p}\mathfrak{q}$ for distinct prime ideals.
- p is **inert** if (p) remains prime in R_m.
- p is **ramified** if $(p) = \mathfrak{p}^2$, for a prime ideal $\mathfrak{p}$.

Here's what this looks like in the subring lattice, for the Gaussian integers.



"3 *is inert*" "5 *splits; is reducible*" "2 *is ramified; irreducible*"

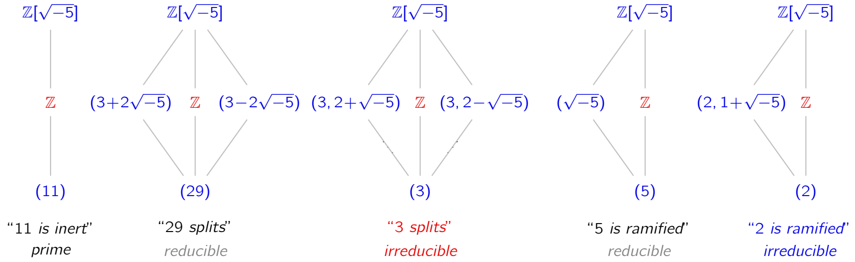
Notice that if a prime splits in $\mathbb{Z}[i]$, then it is reducible, and must factor.

Primes in R_m that aren't PIDs

Consider a prime $p \in \mathbb{Z}$ but in the larger ring R_m. There are three possible behaviors:

- p **splits** if $(p) = \mathfrak{p}\mathfrak{q}$ for distinct prime ideals.
- p is **inert** if (p) remains prime in R_m.
- p is **ramified** if $(p) = \mathfrak{p}^2$, for a prime ideal $\mathfrak{p}$.

Here's what this looks like in the subring lattice of $R_{-5} = \mathbb{Z}[\sqrt{-5}]$.



Remark

In a non-PID, a split prime p may or may not factor, but its ideal (p) will.

Primes in R_m

If p is split or ramified, then (p) isn't a prime ideal because it factors.

The following characterizes *when* and *how* it factors.

Proposition (HW)

Consider the ring R_m of quadratic integers and a odd prime $p \in \mathbb{Z}$.

- If $p \nmid m$ and m is a *quadratic residue* mod p (i.e., $m \equiv n^2 \pmod{p}$), then p **splits**:

$$(p) = \big(p, n + \sqrt{m}\big)\big(p, n - \sqrt{m}\big),$$

- If $p \nmid m$ and m is not a quadratic residue mod p, then p is **inert**.
- If $p \mid m$, then p is **ramified**, and

$$(p) = \big(p, \sqrt{m}\big)^2.$$

Remark

This extends to all primes by replacing $p \mid m$ with $p \mid \Delta$, the **discriminant** of $\mathbb{Q}(\sqrt{-m})$:

$$\Delta = \begin{cases} m & m \equiv 1 \pmod{4} \\ 4m & m \equiv 2, 3 \pmod{4} \end{cases}$$

Primes in R_m

The behavior of a prime $p \in \mathbb{Z}$ in R_m is completely characterized by *quadratic residues*.

The *discriminant* Δ of R_m is $\Delta = m$ (triangular) or $\Delta = 4m$ (rectangular).

A prime $p \neq 2$ in $\mathbb{Z}$, when passed to R_m, becomes:

- **ramified** iff $\Delta \equiv 0 \pmod{p}$.
- **split** iff $\Delta \equiv a^2 \pmod{p}$, for some $a \not\equiv 0$,
- **inert** iff $\Delta \not\equiv a^2 \pmod{p}$, for all a.

The prime $p = 2$ in $\mathbb{Z}$, when passed to R_m, becomes:

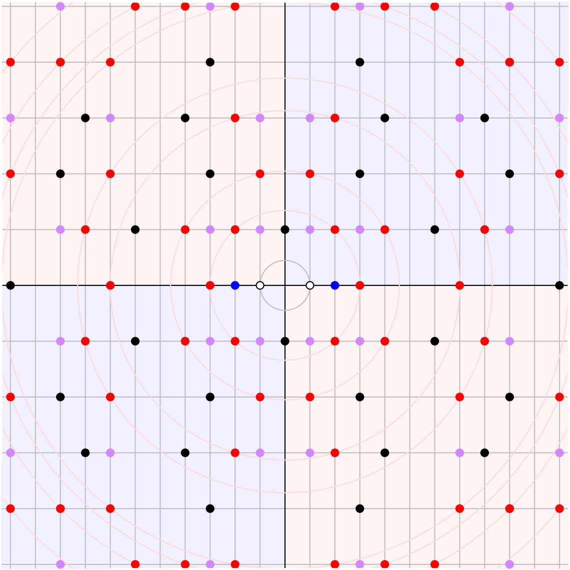
- **ramified** iff $\Delta \equiv 0, 4 \pmod{8}$.
- **split** iff $\Delta \equiv 1 \pmod{8}$.
- **inert** iff $\Delta \not\equiv 5 \pmod{8}$.

Remark

- If R_m is a PID and p splits, then it is reducible.
- If R_m is not a PID and p splits, then
  - p might be **reducible**, or
  - p could be a **non-prime irreducible**.

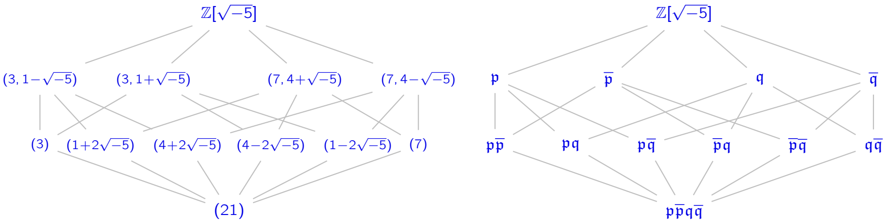
Primes in $R_{-5} = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

Units are **white**, primes are **black**, non-prime irreducibles are **blue**, **red** and **purple**.



The ideal class group

The degree to which unique factorization fails in R is measured by the class group, $\mathrm{Cl}(R)$.



Formally, two ideals I and J are equivalent if $\alpha I = \beta J$ for some $\alpha, \beta \in R$.

The equivalence classes form a group, under $[I] \cdot [J] := [IJ]$.

The identity element is the class of principal ideals, $[(1)]$.

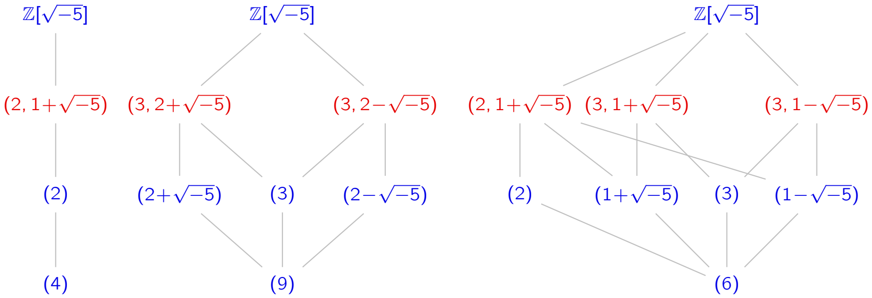
In the example above, $\mathrm{Cl}(R_{-5}) = \Big\{ \big[(1)\big],\ \big[\mathfrak{p}\big] \Big\} \cong C_2$.

Key point

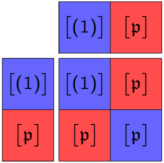
The class group is trivial iff R_m is a PID (equivalently, UFD).

The ideal class group

The degree to which unique factorization fails in R is measured by the class group, $\mathrm{Cl}(R)$.



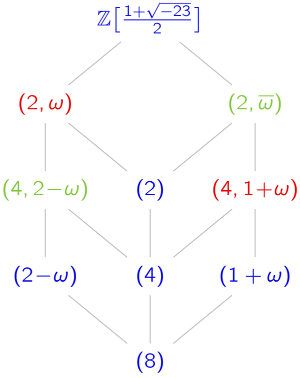
The class group is $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) \cong C_2$.

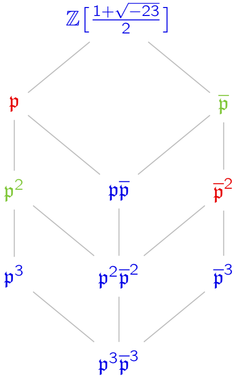


The ideal class group

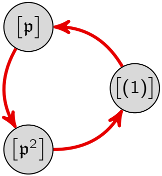
Unique factorization fails in $R_{-23} = \mathbb{Z}[\omega]$, for $\omega = \frac{1+\sqrt{-23}}{2}$, in a different way:

$$(2-\omega)(1+\omega) = \left(\tfrac{3-\sqrt{-23}}{2}\right)\left(\tfrac{3+\sqrt{-23}}{2}\right) = \left(\tfrac{3}{2}\right)^2 - \left(\tfrac{\sqrt{-23}}{2}\right)^2 = \tfrac{9}{4} + \tfrac{23}{4} = 8 = 2^3.$$





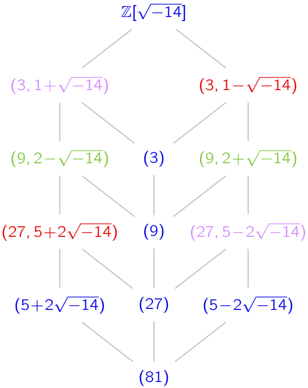
	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$
$[(1)]$	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$
$[\mathfrak{p}]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$	$[(1)]$
$[\mathfrak{p}^2]$	$[\mathfrak{p}^2]$	$[(1)]$	$[\mathfrak{p}]$

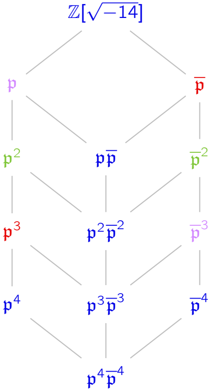


The class group is $\text{Cl}\left(\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]\right) \cong C_3$.

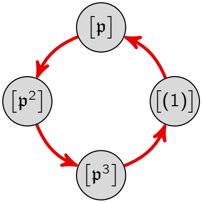
The ideal class group

Unique factorization fails in $R_{-14} = \mathbb{Z}[\sqrt{-14}]$ because $3^4 = 81 = (5 + \sqrt{-14})(5 + \sqrt{-14})$.





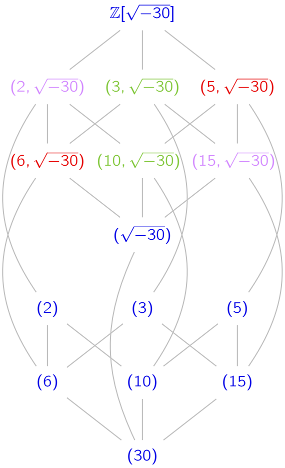
	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$
$[(1)]$	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$
$[\mathfrak{p}]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$	$[(1)]$
$[\mathfrak{p}^2]$	$[\mathfrak{p}^2]$	$[\mathfrak{p}^3]$	$[(1)]$	$[\mathfrak{p}]$
$[\mathfrak{p}^3]$	$[\mathfrak{p}^3]$	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{p}^2]$

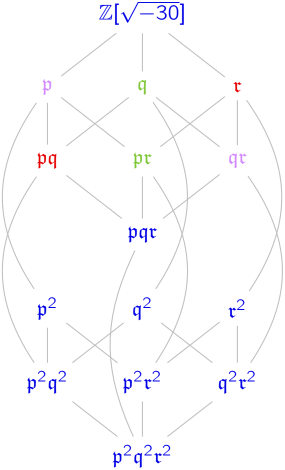


The class group is $\mathrm{Cl}(\mathbb{Z}[\sqrt{-14}]) \cong C_4$.

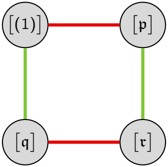
The ideal class group

Unique factorization fails in $R_{-30} = \mathbb{Z}[\sqrt{-30}]$ because $2 \cdot 3 \cdot 5 = 30 = -(\sqrt{-30})^2$.





	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{q}]$	$[\mathfrak{r}]$
$[(1)]$	$[(1)]$	$[\mathfrak{p}]$	$[\mathfrak{q}]$	$[\mathfrak{r}]$
$[\mathfrak{p}]$	$[\mathfrak{p}]$	$[(1)]$	$[\mathfrak{r}]$	$[\mathfrak{q}]$
$[\mathfrak{q}]$	$[\mathfrak{q}]$	$[\mathfrak{r}]$	$[(1)]$	$[\mathfrak{p}]$
$[\mathfrak{r}]$	$[\mathfrak{r}]$	$[\mathfrak{q}]$	$[\mathfrak{p}]$	$[(1)]$



The class group is $\mathrm{Cl}(\mathbb{Z}[\sqrt{-30}]) \cong V_4$.

The ideal class group

Theorem

For squarefree $m < 0$, the class group $\mathrm{Cl}(R_m)$ is trivial if and only if

$$m \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Conjecture (Cohen/Lenstra, 1984)

There are infinitely many $m > 0$ for which $\mathrm{Cl}(R_m)$ is trivial.

Here is the list of squarefree $m > 0$ for which the class group of R_m is trivial:

2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97, 101, 103, 107, 109, 113, 118, 127, 129, 131, 133, 134, 137, 139, 141, 149, 151, 157, 158, 161, 163, 166, 167, 173, 177, 179, 181, 191, 193, 197, 199, 201, 206, 209, 211, 213, 214, 217, 227, 233, 237, 239, 241, 249, 251, 253, 262, 263, 269, 271, 277, 278, 281, 283, 293, 301, 302, 307, 309, 311, 313, 317, 329, 331, 334, 337, 341, 347, 349, 353, 358, 367, 373, 379, 381, 382, 383, 389, 393, 397, 398, 409, 413, 417, 419, 421, 422, 431, 433, 437, 446, 449, 453, 454, 457, 461, 463, 467, 478, 479, 487, 489, 491, 497, 501, 502, 503, 509, 517, 521, 523, 526, 537, 541, 542, 547, 553, 557, 563, 566, 569, 571, 573, 581, 587, 589, 593, 597, 599, 601, 607, 613, 614, 617, 619, 622, 631, 633, 641, 643, 647, 649, 653, 661, 662, 669, 673, 677, 681, 683, 691, 694, 701, 709, 713, 717, 718, 719, 721, 734, 737, 739, 743, 749, 751, 753, 757, 758, 766, 769, 773, 781, 787, 789, 797, 809, 811, 813, 821, 823, 827, 829, 838, 849, 853, 857, 859, 862, 863, 869, 877, 878, 881, 883, 886, 887, 889, 893, 907, 911, 913, 917, 919, 921, 926, 929, 933, 937, 941, 947, 953, 958, 967, 971, 973, 974, 977, 983, 989, 991, 997, 998.

Quadratic integers and norm-Euclidean domains

Proposition

If $m = -2, -1, 2, 3$, then R_m is Euclidean with $d(x) = |N(x)|$; ("norm-Euclidean").

Proof

Take $a, b \in R_m = \mathbb{Z}[\sqrt{m}]$, with $b \neq 0$. Let $a/b = s + t\sqrt{m} \in \mathbb{Q}(\sqrt{m})$.

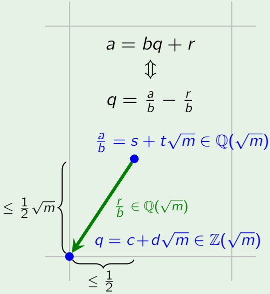
Pick $q = c + d\sqrt{m} \in R_m$, the nearest element to a/b.

Since $N(b) = N(r)N(b/r)$, we have

$$|N(r)| < |N(b)| \quad \Leftrightarrow \quad |N(r/b)| < |N(1)|$$

For each $m = -2, -1, 2, 3$:

$$-1 < N(\tfrac{r}{b}) = \underbrace{(c-s)^2}_{\leq \frac{1}{4}} - m \underbrace{(d-t)^2}_{\leq \frac{1}{4}} < 1.$$



Proposition (HW)

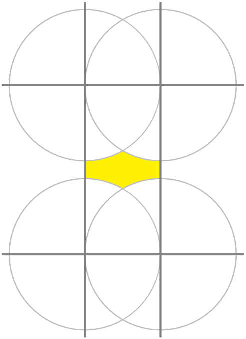
If $m = -3, -7, -11$, then $R_m = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$ is norm-Euclidean.

Quadratic integers and norm-Euclidean domains

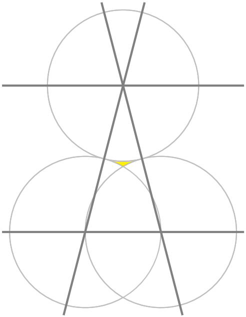
Alternate characterization

For $m < 0$, the ring R_m is norm-Euclidean iff the unit balls centered at points in R_m cover the complex plane.

$R_{-5} = \mathbb{Z}[\sqrt{-5}]$



$R_{-15} = \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$



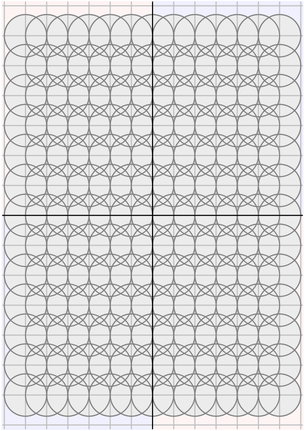
If $a/b \in \mathbb{Q}(\sqrt{m})$ (see previous proof) lies in the yellow region, then $N(r/b) > 1$.

Quadratic integers and norm-Euclidean domains

Alternate characterization

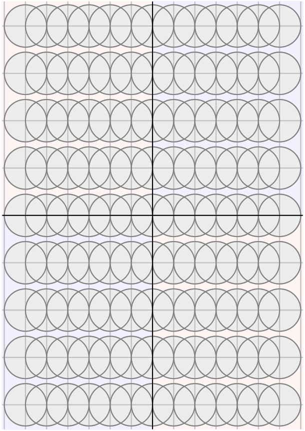
For $m < 0$, the ring R_m is norm-Euclidean iff the unit balls centered at points in R_m cover the complex plane.

$R_{-2} = \mathbb{Z}[\sqrt{-2}]$



Euclidean, PID

$R_{-5} = \mathbb{Z}[\sqrt{-5}]$



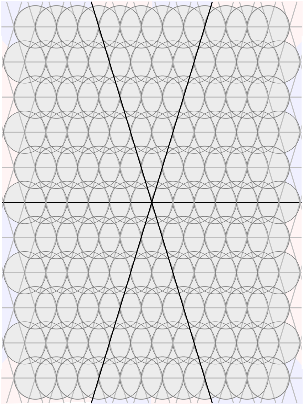
non-Euclidean, non-PID

Quadratic integers and norm-Euclidean domains

Alternate characterization

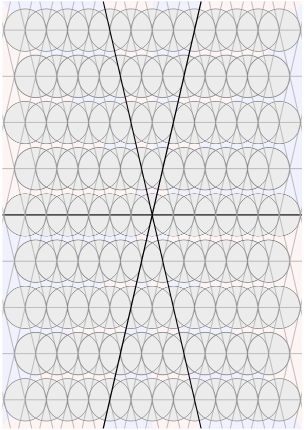
For $m < 0$, the ring R_m is norm-Euclidean iff the unit balls centered at points in R_m cover the complex plane.

$R_{-11} = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$



Euclidean, PID

$R_{-19} = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$



non-Euclidean, PID

PIDs that are not Euclidean

Theorem

The ring R_m is norm-Euclidean iff

$$m \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Theorem (D.A. Clark, 1994)

The rings R_{69} and R_{14} are Euclidean domains that are *not* norm-Euclidean.

The following degree function works for R_{69}, defined on the primes

$$d(p) = \begin{cases} |N(p)| & \text{if } p \neq 10 + 3\alpha \\ c & \text{if } p = 10 + 3\alpha \end{cases} \qquad \alpha = \frac{1+\sqrt{69}}{2}, \quad c > 25 \text{ an integer.}$$

Theorem

If $m < 0$, then R_m is Euclidean iff $m \in \{-11, -7, -3, -2, -1\}$.

Theorem

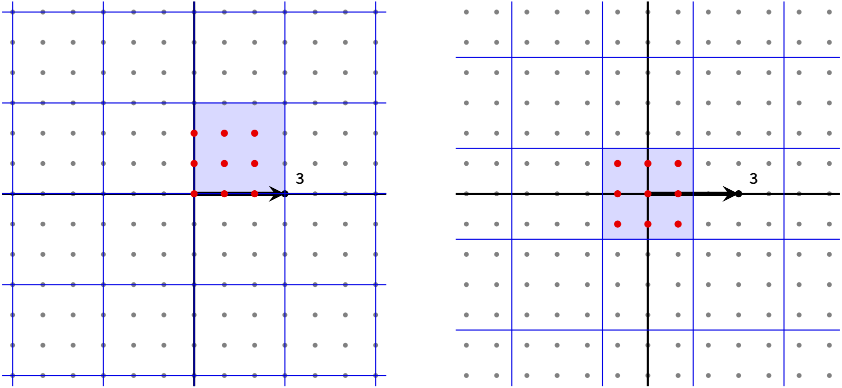
If $m < 0$, then R_m is a PID iff $m \in \{\underbrace{-163, -67, -43, -19}_{\text{non-Euclidean}}, \underbrace{-11, -7, -3, -2, -1}_{\text{Euclidean}}\}$.

Quotients of the Gaussian integers

Since $\mathbb{Z}[i]$ is PID, every quotient ring has the form $\mathbb{Z}[i]/(z_0)$, for some $z_0 \in \mathbb{Z}[i]$.

This ring is finite, and there are several canonical ways to describe the residue classes.

Here are two ways to visualize $\mathbb{Z}[i]/(3)$.

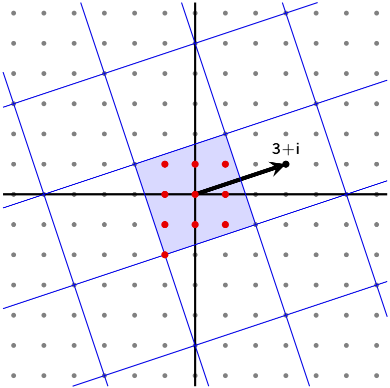


Since 3 is prime in $\mathbb{Z}[i]$, the ideal (3) is maximal, so $\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$.

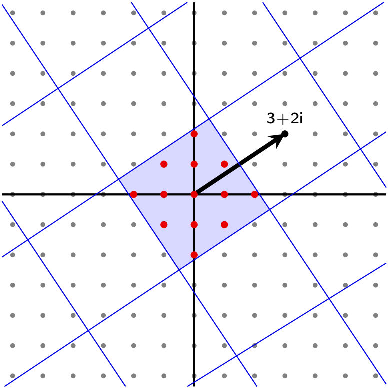
Quotients of the Gaussian integers

Since $3+i=(1+2i)(1-i)$, the quotient $\mathbb{Z}[i]/(3+i)$ is not a field; it has order 10.

The element $3+2i$ is irreducible ($N(3+2i)=13$ is prime), so $\mathbb{Z}[i]/(3+2i)$ is a field.



$\mathbb{Z}[i]/(3+i)\cong\mathbb{Z}_{10}$



$\mathbb{Z}[i]/(3+2i)\cong\mathbb{Z}_{13}$

Algebraic integers (roots of monic polynomials)

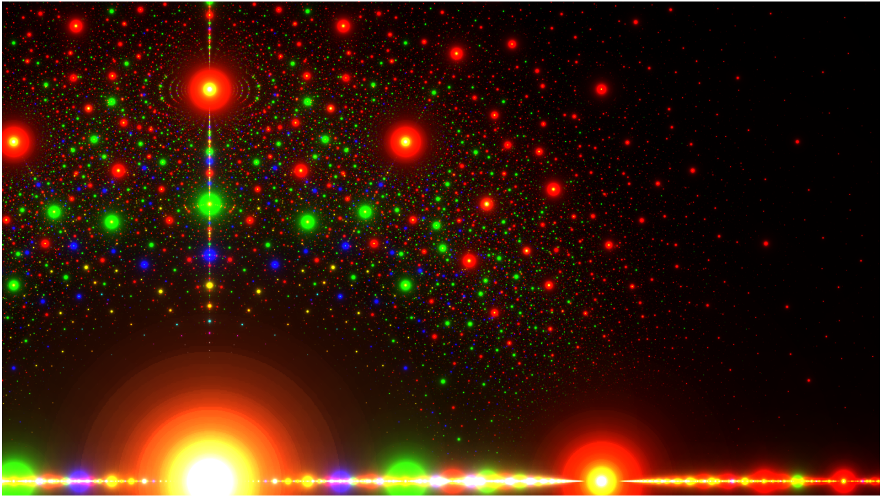


Figure: Algebraic numbers in $\mathbb{C}$. Colors indicate the coefficient of the leading term: red $= 1$ (algebraic integer), green $= 2$, blue $= 3$, yellow $= 4$. Large dots mean fewer terms and smaller coefficients. Image from Wikipedia (made by Stephen J. Brooks).

Algebraic integers (roots of monic polynomials)

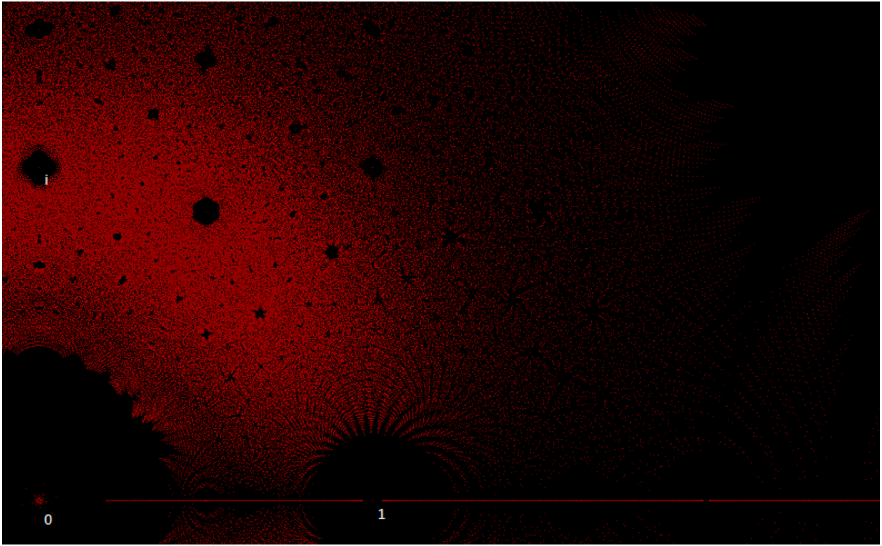
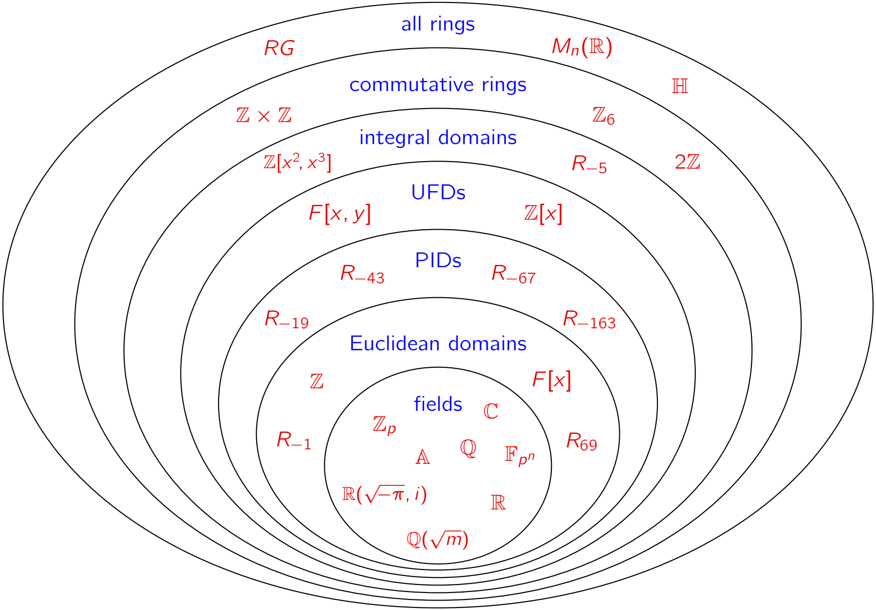


Figure: Algebraic integers in $\mathbb{C}$. Each red dot is the root of a monic polynomial of degree ≤ 7 with coefficients from $\{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$. From Wikipedia.

Summary of ring types



A problem from *Master Sun's mathematical manual* (3rd century A.D.)

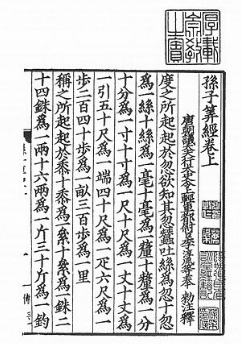
Problem 26, Volume 3 from the *Sunzi Suanjing*:

> *"There are certain things whose number is unknown. A number is repeatedly divided by* 3*, the remainder is* 2*; divided by* 5*, the remainder is* 3*; and by* 7*, the remainder is* 2*. What will the number be?"*

This is describing solution(s) to

$$x \equiv 2 \pmod 3) \equiv 3 \pmod 5) \equiv 2 \pmod 7).$$

This problem was also studied by Aryabhata (476–550 A.D.), Brahmagupta (598–668 A.D.), Ibn al-Haytham (965–1040 A.D.), and Fibonacci (1170–1250 A.D.).


孫子算經卷上
唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋
度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

During the Song dynasty, Qin Jiushau (1202–1261) published this in his famous *Shùshū Jiǔzhāng*: "*A Mathematical Treatise in Nine Sections*."

It appears today in algorithms for RSA cryptography and the FFT.

The Sunzi remainder theorem in $\mathbb{Z}$

A solution to $x \equiv 2 \pmod 3 \equiv 3 \pmod 5 \equiv 2 \pmod 7$ satisfies

$$x \in (2+3\mathbb{Z}) \cap (3+5\mathbb{Z}) \cap (2+7\mathbb{Z}).$$

Every solution has the form $23+105k$, i.e., elements of the coset $23+105\mathbb{Z}$.

Formally, there is a ring isomorphism

$$\mathbb{Z}/105\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \qquad x \bmod 105 \longmapsto \big(x \bmod 3,\, x \bmod 5,\, x \bmod 7\big).$$

Sunzi remainder theorem in $\mathbb{Z}$

Let $n_1, \dots, n_k$ be pairwise co-prime integers. For any $a_1, \dots, a_k \in \mathbb{Z}$, the system

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad\vdots \\ x \equiv a_k \pmod{n_k}. \end{cases}$$

has a solution. Moreoever, any two solutions are equivalent modulo $n := n_1 n_2 \cdots n_k$. Equivalentally, there is an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}, \qquad x \bmod n \longmapsto (x \bmod n_1, \dots, x \bmod n_k).$$

The Sunzi remainder theorem in a PID

Elements $n_1, \dots, n_k$ in a PID are pairwise co-prime if any of the three equivalent conditions hold, for every $i \neq j$:

(a) $\gcd(n_i, n_j) = 1$,

(b) $an_i + bn_j = 1$, for some $a, b \in R$,

(c) $(n_i) + (n_j) = R$.

Sunzi remainder theorem for PIDs

Let $n = n_1, \dots, n_k \in R$ be pairwise co-prime elements in a PID, with $n = n_1 n_2 \dots n_k$. Then there is an isomorphism

$$R/(n) \longrightarrow R/(n_1) \times \cdots \times R/(n_k), \qquad x \bmod n \longmapsto (x \bmod n_1, \dots, x \bmod n_k).$$

Corollary

Let $R = \mathbb{Z}$ and $I_j = (n_j)$, for $j = 1, \dots, k$ with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then

$$I_1 \cap \cdots \cap I_k = (n_1 n_2 \cdots n_k), \qquad \text{and} \qquad \mathbb{Z}_{n_1 n_2 \cdots n_n} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}.$$

The Sunzi remainder theorem in a commutative ring

In a ring R, say that $I, J \trianglelefteq R$ are co-maximal ideals if $I + J = R$.

Equivalently, neither contain a maximal ideal. We can define co-prime analogously.

If R is commutative, then product of ideals I with J is

$$IJ := \{a_1 b_1 + \cdots + a_m b_m \mid a_m \in I,\ b_m \in J,\ m \in \mathbb{N}\}.$$

This is the smallest ideal that contains all elements of the form ab, for $a \in I$ and $b \in J$.

It is straightforward to define this for more than two ideals.

Sunzi remainder theorem for commutative rings

Let R be a commutative ring with 1, and $I_1, \ldots, I_n$ pairwise co-maximal ideals with $I = I_1 I_2 \cdots I_n$. Then there is an isomorphism

$$R/I \longrightarrow R/I_1 \times \cdots \times R/I_n, \qquad x + I \longmapsto (x + I_1, \ldots, x + I_n).$$

Do you see how to extend this to general rings?

The key is to find a suitable replacement for $I_1 I_2 \cdots I_n$.

The Sunzi remainder theorem in a general ring

Lemma

In a commutative ring R with pairwise co-maximal ideals $I_1, \dots, I_n$,

$$I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n.$$

Proof

The "$\subseteq$" direction always holds. (Why?) ✓

"$\supseteq$:" Use induction.

Base case ($n = 2$): suppose $I + J = R$, and write $a + b = 1$, for $a \in I$ and $b \in J$.

Multiply by $r \in I \cap J$ to get $r = \underbrace{ra}_{\in IJ} + \underbrace{rb}_{\in IJ}$.

Thus, $r = ra + rb \in IJ$, hence $I \cap J \subseteq IJ$. ✓

Suppose the result holds for n ideals; we'll show it holds for $n + 1$. Let

$$I := I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n, \quad \text{and} \quad J = I_{n+1}.$$

The Sunzi remainder theorem in a general ring

Lemma

In a commutative ring R with pairwise co-maximal ideals $I_1, \dots, I_n$,

$$I_1 I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n.$$

Proof (contin.)

We need to show equailty in the following, and *it suffices to show that that* $I + J = R$:

$$\underbrace{I_1 I_2 \cdots I_n}_{=I} \underbrace{I_{n+1}}_{=J} \subseteq (I_1 \cap I_2 \cap \cdots \cap I_n) \cap (I_{n+1}).$$

For each $j = 1, \dots n$, since $I_j + I_{n+1} = R$, write $1 = a_j + b_j$, with $a_j \in I_j$ and $b_j \in I_{n+1}$.

$$\begin{array}{ccccccccc}
1 & = & a_1 & & & & + & b_1 & \in I_1 + I_{n+1} \\
1 & = & & a_2 & & & + & b_2 & \in I_2 + I_{n+1} \\
1 & = & & & a_3 & & + & b_3 & \in I_3 + I_{n+1} \\
& \vdots & & & & \ddots & \vdots & & \\
1 & = & & & & a_n & + & b_{n+1} & \in I_n + I_{n+1}
\end{array}$$

Note that $\underbrace{a_1 a_2 \cdots a_n}_{\in I} = (1 - b_1)(1 - b_2) \cdots (1 - b_n) = 1 + \Big[\underbrace{\sum \text{lots of terms in } J}_{\in J}\Big].$ □

The most general version

Sunzi remainder theorem, general rings

Let R be a ring with 1, and $I_1, \dots, I_n$ pairwise co-maximal ideals with $I = I_1 \cap \cdots \cap I_n$. Then there is an isomorphism

$$R/I \longrightarrow R/I_1 \times \cdots \times R/I_n, \qquad x + I \longmapsto (x + I_1, \dots, x + I_n).$$

Proof

The following defines a ring homomorphism with $\text{Ker}(\phi) = I$ (exercise):

$$\phi\colon R \longrightarrow R/I_1 \times \cdots \times R/I_n, \qquad \phi\colon x \longmapsto (x + I_1, \dots, x + I_n).$$

The result follows from the FHT once we show that ϕ is onto.

An element $(r_1 + I, \dots, r_n + I)$ in the co-domain has a preimage iff there is a solution to:

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad\vdots \\ x \equiv r_n \pmod{I_n}. \end{cases}$$

SRT: Establishing surjectivity

Proposition

Let $I_1, \dots, I_n$ be pairwise co-maximal ideals of R. For any $r_1, \dots, r_n \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I_1} \\ \quad \vdots \\ x \equiv r_n \pmod{I_n} \end{cases}$$

has a solution $r \in R$.

Proof (all we need to show)

Any element of the following form must be a solution:

$$x = r_1 s_1 + \cdots + r_n s_n, \qquad \text{where } s_k \equiv \begin{cases} 1 \pmod{I_k} \\ 0 \pmod{I_j}, \quad j \neq k \end{cases}$$

We'll replace $s_k \equiv 0 \pmod{I_j}, \forall j \neq k$ with the equivalent $s_k \equiv 0 \pmod{\bigcap_{j \neq k} I_j}$.

All we have to do is construct $s_1 \dots, s_n$!

We'll show how to construct s_1. Then, constructing $s_2, \dots, s_n$ is analogous.

SRT: Establishing surjectivity

Proposition (special case of $n = 2$)

Let I, J be co-maximal ideals of R. For any $r_1, r_2 \in R$, the system

$$\begin{cases} x \equiv r_1 \pmod{I} \\ x \equiv r_2 \pmod{J} \end{cases}$$

has a solution $r \in R$.

Proof

Write $1 = a + b$, with $a \in I$ and $b \in J$, and set $r = r_2 a + r_1 b$. This works:

$$r - r_1 = (r - r_1 b) + (r_1 b - r_1) = r_2 a + r_1(b - 1) = r_2 a - r_1 a = (r_2 - r_1)a \in I$$

implies that $r \equiv r_1 \pmod{I}$, and

$$r - r_2 = (r - r_2 a) + (r_2 a - 1) = r_1 b + r_2(a - 1) = r_1 b - r_2 b = (r_1 - r_2)b \in J$$

means that $r \equiv r_2 \pmod{J}$. ✓

SRT: Establishing surjectivity

Proposition (all that's left to show)

The ideals I_1 and $I_2 \cap \cdots \cap I_n$ are co-maximal, and thus the system

$$\begin{cases} x \equiv 1 \pmod{I_1} \\ x \equiv 0 \pmod{\bigcap_{j \neq 1} I_j} \end{cases}$$

has a solution $s_1 \in R$.

Proof (contin.)

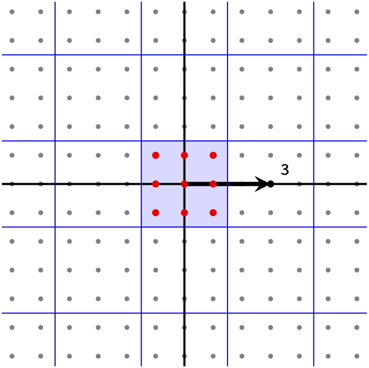
For each $j = 2, \dots n$, since $I_1 + I_j = R$, write $1 = a_j + b_j$, with $a_j \in I_1$ and $b_j \in I_j$.

$$\begin{array}{rclcl}
1 & = & a_2 + b_2 & & \in I_1 + I_2 \\
1 & = & a_3 \qquad + b_3 & & \in I_1 + I_3 \\
1 & = & a_4 \qquad\qquad + b_4 & & \in I_1 + I_4 \\
 & \vdots & & & \vdots \\
1 & = & a_n \qquad\qquad \ddots \quad + b_n & & \in I_1 + I_n
\end{array}$$

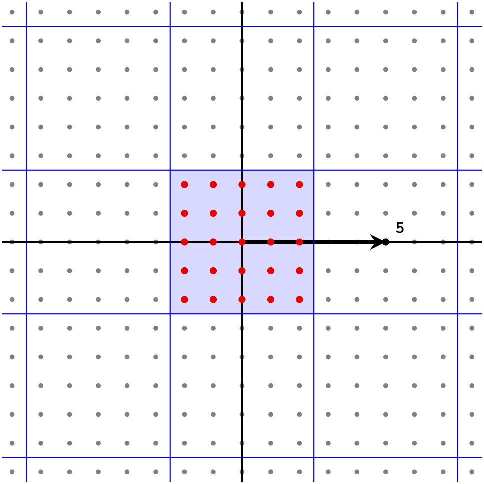
Note that $1 = (a_2 + b_2)(a_3 + b_3) \cdots (a_n + b_n) = \underbrace{\left[\sum \text{terms in } I_1\right]}_{\in I_1} + \underbrace{b_2 b_3 \cdots b_n}_{\in I_2 \cap I_3 \cap \cdots \cap I_n}$. □

An example of the Sunzi remainder theorem

Note that $(3) \subseteq \mathbb{Z}[i]$ is prime (and hence maximal), but $(5) = (1 + 2i)(1 - 2i)$.



$\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$



$\mathbb{Z}[i]/(5) \cong \mathbb{Z}[i]/(1+2i) \times \mathbb{Z}[i]/(1-2i) \cong \mathbb{Z}_5 \times \mathbb{Z}_5$

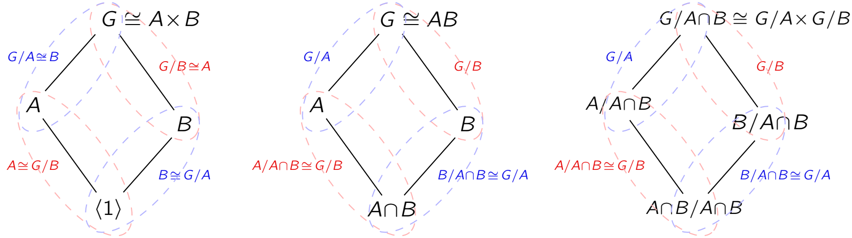
A group-theoretic analogue of the Sunzi remainder theorem

We encountered the following after proving the FHT for groups.

Theorem (HW)

Let A, B be normal subgroups satisfying $G = AB$. Then

$$G/(A \cap B) \cong G/A \times G/B.$$



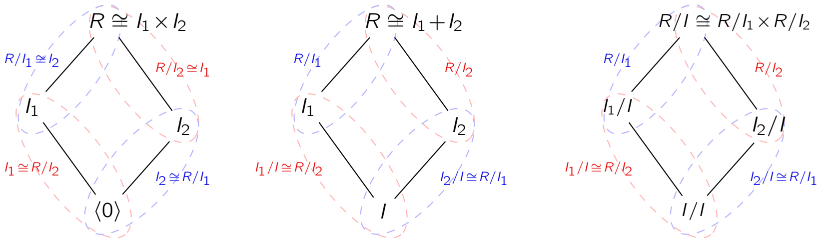
A lattice interpretation of the Sunzi remainder theorem

Let's compare to the actual Sunzi remainder theorem.

Sunzi remainder theorem (2 factors)

Let I, J be ideal of a ring R satisfying $R = I + J$. Then

$$R/(I \cap J) \cong R/I \times R/J.$$



Idempotents

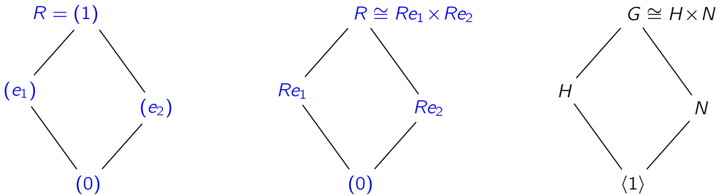
Definition

An element e in an integral domain R is an idempotent if $e^2 = e$. An orthogonal pair of idempotents are $e_1, e_2 \in R$ such that

$$e_1 + e_2 = 1 \qquad \text{and} \qquad e_1 e_2 = 0.$$

Every idempotent $e \in R$ forms an orthogonal pair with $1 - e$.

The Sunzi remainder theorem says that $R \cong Re \times R(1-e)$. Compare this to normal subgroups that are lattice complements.



If $R \cong R/I_1 \times \cdots \times R/I_n$, then the elements

$$e_1 = (1, 0, \dots, 0),\ e_2 = (0, 1, 0, \dots, 0), \dots,\ e_n = (0, 0, \dots, 0, 1),$$

are central idempotents, and are pairwise orthogonal.

Polynomials rings

Let's continue to assume that R is an integral domain with 1, and F a field.

Proposition (exercise)

Let $f(x), g(x) \in R[x]$ be nonzero. Then

1. $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.
2. $U(R[x]) = U(R)$,
3. $R[x]$ is an integral domain.

Let $f(x) \in \mathbb{Z}[x]$ be irreducible. Let's explore how $f(x)$ factors over larger rings.

For example, $f(x) = x^4 - 2 \in \mathbb{Z}[x]$ factors as

- $(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2}) \in \mathbb{R}[x]$
- $(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}) \in \mathbb{C}[x]$.

But it remains irreducible in $\mathbb{Q}[x]$.

Key idea

Remaining inside the field of fractions will never cause an irreducible polynomial to factor.

Reduction of coefficients mod I

Let I be an ideal of a commutative ring R with 1. The canonical quotient map

$$R \longrightarrow \bar{R} := R/I, \qquad r \longmapsto \bar{r} := r + I$$

defines a homomorphism called the reduction of coefficients modulo I:

$$\pi_I \colon R[x] \longrightarrow \bar{R}[x], \qquad \pi_I : \sum_{i=0}^{n} a_n x^n \longmapsto \sum_{i=0}^{n} \bar{a}_n x^n,$$

Proposition

For an integral domain R,

(i) $R[x]/(I) \cong (R/I)[x]$

(ii) $I \trianglelefteq R$ is prime iff $(I) \trianglelefteq R[x]$ is prime.

Proof

Part (i): immediate from the FHT because $\mathrm{Ker}(\phi) = (I)$. ✓

For Part (ii):

$$\begin{aligned} I \text{ prime } \Leftrightarrow R/I \text{ an integral domain } &\Leftrightarrow (R/I)[x] \text{ an integral domain} \\ &\Leftrightarrow R[x]/(I) \text{ an integral domain} \\ &\Leftrightarrow (I) \text{ prime.} \end{aligned}$$

Primitive elements and Gauss' lemma

Definition

If R is a UFD, the content of $f(x) \in R[x]$ is the GCD of its coefficients (up to associates).

If the content is 1, then $f(x)$ is primitive.

Gauss' lemma

Let R be a UFD. If $f(x), g(x) \in R[x]$ are primitive, then so is $f(x)g(x)$.

Proof (contrapositive)

$$
\begin{aligned}
f(x)g(x) \text{ not primitive} \quad &\Longleftrightarrow \quad \text{some } p \mid f(x)g(x) \in R[x] \\
&\Longleftrightarrow \quad \bar{f}(x)\bar{g}(x) = \bar{0} \in R/(p)[x] \\
&\Longrightarrow \quad \bar{f}(x) = \bar{0} \text{ or } \bar{g}(x) = 0 \\
&\Longleftrightarrow \quad p \mid f(x) \text{ or } p \mid g(x) \text{ in } R[x] \\
&\Longleftrightarrow \quad f(x) \text{ not prim., or } g(x) \text{ not prim.}
\end{aligned}
$$

Primitive elements

Lemma

Suppose R is a UFD with field of fractions F. Suppose $f(x)$ and $g(x)$ are primitive in $R[x]$, but associates in $F[x]$. Then they are associates in $R[x]$.

Proof

Since $f(x) \sim g(x)$ we have $f(x) = ag(x)$ for some $a \in F$. If $a = b/c$ for $a, b \in R$,

$$f(x) = ag(x) = \frac{b}{c} g(x) \quad \Longrightarrow \quad cf(x) = bg(x).$$

Since $f(x)$ and $g(x)$ are primitive, the content of $cf(x)$ and $bg(x)$ is $c \sim b$. Now,

$$b \sim c \text{ in } R \quad \Longrightarrow \quad b = cu \text{ for some } u \in U(R) \quad \Longrightarrow \quad a = b/c = u \in U(R).$$

This means that $f(x) \sim g(x)$ in $R[x]$. □

Primitive elements

Proposition

Let R be a UFD and F its field of fractions. If $f(x)$ is irreducible in $R[x]$, then it is irreducible in $F[x]$.

Proof

Since $f(x)$ is irreducible in $R[x]$, it is primitive. For sake of contradiction, suppose

$$\begin{aligned} f(x) &= f_1(x)f_2(x) \in F[x] & \quad \mathbf{deg}(f_i(x)) > 0 \\ &= a_1 g_1(x) \cdot a_2 g_2(x) \in F[x] & \quad a_i \in F,\ \ g_i(x) \text{ primitive in } R[x]. \end{aligned}$$

We can now conclude that:

(i) $f(x) \sim g_1(x)g_2(x)$ in $F[x]$, (*because* $a_1a_2 \in F[x]$ *is a unit*).

(ii) $g_1(x)g_2(x)$ is primitive in $R[x]$ (*by Gauss' lemma*).

(iii) $f(x) \sim g_1(x)g_2(x)$ in $R[x]$, (*by Lemma;* $f(x) \sim g_1(x)g_2(x)$ *in* $F[x]$).

Therefore, $f(x) = ug_1(x)g_2(x)$ for some $u \in U(R)$, contradicting irreducibility. □

Polynomials rings over a UFD

Theorem

If R is a UFD, then $R[x]$ is as well.

Proof

We need to show:

(i) Each nonzero nonunit $f(x) \in R[x]$ is a product of irreducibles. (simple induction)

(ii) Every irreducible is prime.

(ii): Suppose $f(x)$ is irreducible (and thus primitive), and $f(x) \mid g(x)h(x)$ in $R[x]$.

Since $f(x)$ remains irreducible in $F[x]$, a Euclidean domain, it is prime in $F[x]$.

WLOG, say $f(x) \mid g(x)$ in $F[x]$, with $g(x) = f(x)k(x) \in F[x]$ and $k(x) \in F[x]$. Write

$$g(x) = a \underbrace{g_1(x)}_{\in R[x]} = (b/c) f(x) \underbrace{k_1(x)}_{\in R[x]}, \qquad g_1(x), k_1(x) \textit{ primitive.}$$

Now,

$$g_1(x) \sim f(x)k_1(x) \text{ in } F[x] \quad \overset{\text{Gauss}}{\Longrightarrow} \quad f(x)k_1(x) \text{ prim.} \quad \overset{\text{Lemma}}{\Longrightarrow} \quad g_1(x) \sim f(x)k_1(x) \text{ in } R[x].$$

Writing $g_1(x) = uf(x)k_1(x)$ for some $u \in U(R)$ shows $f(x) \mid g_1(x) \mid g(x) \in R[x]$. $\square$

An irreducibility test

Eisenstein's criterion

Consider a polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x].$$

over a PID. If there is a prime $p \in R$ such that:

1. $p \mid a_i$ for all $i < n$
2. $p \nmid a_n$,
3. $p^2 \nmid a_0$,

then $f(x)$ is irreducible.

Proof

Assume $f(x)$ is primitive and suppose it factors as $f(x) = g(x)h(x)$:

$$f(x) = \big(b_0 + b_1 x + \cdots + b_k x^k\big)\big(c_0 + c_1 x + \cdots + c_\ell x^\ell\big) \in R[x], \quad k, \ell > 0.$$

Reduce coefficients modulo $I = (p)$ to get

$$\bar{f}(x) = \bar{a}_n x^n = \bar{b}_k \bar{c}_\ell x^n = \bar{g}(x)\bar{h}(x) \in \bar{R}[x].$$

From this we can reach a contradiction:

$$x \mid \bar{g}(x)\bar{h}(x) \quad \Rightarrow \quad \bar{b}_0 = \bar{c}_0 = 0 \quad \Rightarrow \quad p \mid b_0 \text{ and } p \mid c_0 \quad \Rightarrow \quad p^2 \mid b_0 c_0 = a_0.$$

An irreducibility test

Eisenstein's criterion (equivalent formulation)

Consider a polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x].$$

over a PID. If there is a prime ideal $P \trianglelefteq R$ such that:

1. $a_i \in P$ for all $i < n$
2. $a_n \notin P$,
3. $a_0 \notin P^2$.

then $f(x)$ is irreducible.

Eisenstein's criterion holds, more generally, over a UFD.

To prove this, assume

$$f(x) = \left(b_0 + b_1 x + \cdots + b_k x^k\right)\left(c_0 + c_1 x + \cdots + c_\ell x^\ell\right) \in R[x], \quad k, \ell > 0,$$

and $p \mid b_0$.

Now, consider the smallest k for which $p \nmid b_k \ldots$

The remainder will be left as an exercise.

Polynomial rings over a field

Proposition

A polynomial $f(x) \in F[x]$ has a factor of degree 1 iff it has a root in F.

Proof

"$\Rightarrow$:" If $f(x)$ has a degree-1 factor, then $f(x) = g(x)(x - \alpha)$. ✓

"$\Leftarrow$:" If $f(\alpha) = 0$, use the division algorithm to write

$$f(x) = g(x)(x - \alpha) + r, \qquad r \text{ is constant.}$$

But then $f(\alpha) = r = 0$. □

Corollary

A polynomial $f(x) \in F[x]$ of degree ≤ 3 is reducible iff it has a root in F. □

Polynomial rings over a field

Remarks

Let F be a field. Then $F[x]$ is Euclidean (and hence a PID).

1. The following are equivalent:
   (i) $f(x)$ is irreducible,
   (ii) $I = \big(f(x)\big)$ is a maximal ideal of $F[x]$,
   (iii) $F[x]/(f(x))$ is a field.
2. If a polynonomial factors as

$$f(x) = f_1(x)^{d_1} f_2(x)^{d_2} \cdots f_k(x)^{d_k}, \qquad f_i(x) \text{ distinct irreducibles,}$$

   then $\mathbf{gcd}\left(f_i(x)^{d_i}, f_j(x)^{d_j}\right) = 1$ for $i \neq j$.

   By the Sunzi remainder theorem,

$$F[x]/(f(x)) \cong F[x]/\left(f_1(x)^{d_1}\right) \times \cdots \times F[x]/\left(f_k(x)^{d_k}\right).$$

Multivariate polynomial rings

We can define multivariate polynomial rings inductively.

Definition

The polynomial ring in variables $x_1, \ldots, x_n$ over R is

$$R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n].$$

Note that

$$R[x_1] \subseteq R[x_1, x_2] \subseteq R[x_1, x_2, x_3] \subseteq \cdots, \qquad R[x_1, x_2, x_3, \ldots] = \bigcup_{k=1}^{\infty} R[x_1, \ldots, x_k].$$

Not surprisingly, this last ring has non-finitely generated ideals, e.g., $I = (x_1, x_2, \ldots)$.

Perhaps surprisingly, this is *not* the case in $R[x_1, \ldots, x_n]$.

Hilbert's basis theorem

If R is a Noetherian ring, then $R[x_1, \ldots, x_n]$ is Noetherian as well.

It suffices to prove this for $n = 1$.

Proof of Hilbert's basis theorem

Given $I \trianglelefteq R[x]$ and $m \geq 0$, the ideal of leading coefficients of degree-m polynomials is:

$$I(m) := \{a_m \mid f(x) = a_m x^m + \cdots + a_1 x + a_0 \in I\} \cup \{0\} \trianglelefteq R.$$

Let $I_r(s)$ be a maximal element of $\{I_n(m) \mid n, m \geq 0\}$.

$$\begin{array}{ccccccccccccc}
 & & & & & & & & \vdots & & \vdots & & \\
 & & & & & & & & \| & & \| & & \\
 & & & & & & & \cdots & \mathbf{I_r(s)} & = & \mathbf{I_r(s+1)} & = & \cdots \\
\vdots & \vdots & & \vdots & & & & \vdots & \vdots & & & & \\
\cup\!\mid & \cup\!\mid & & \cup\!\mid & & & & \cup\!\mid & \cup\!\mid & & & & \\
\mathbf{I_2} & \mathbf{I_2(0)} & \subseteq & \mathbf{I_2(1)} & \subseteq & \cdots & \subseteq & \mathbf{I_2(s-1)} & \subseteq \; \mathbf{I_2(s)} & \subseteq & \cdots & & \\
\cup\!\mid & \cup\!\mid & & \cup\!\mid & & & & \cup\!\mid & \cup\!\mid & & & & \\
\mathbf{I_1} & \mathbf{I_1(0)} & \subseteq & \mathbf{I_1(1)} & \subseteq & \cdots & \subseteq & \mathbf{I_1(s-1)} & \subseteq \; \mathbf{I_1(s)} & \subseteq & \cdots & & \\
\cup\!\mid & \cup\!\mid & & \cup\!\mid & & & & \cup\!\mid & \cup\!\mid & & & & \\
\mathbf{I_0} & \mathbf{I_0(0)} & \subseteq & \mathbf{I_0(1)} & \subseteq & \cdots & \subseteq & \mathbf{I_0(s-1)} & \subseteq \; \mathbf{I_0(s)} & \subseteq & \cdots & &
\end{array}$$

Proof of Hilbert's basis theorem

Lemma

Let $I \subseteq J$ be ideals of $R[x]$. If $I(m) = J(m)$ for all m, then $I = J$.

$$\begin{array}{ccccccccccc}
\mathbf{J(0)} & \subseteq & \mathbf{J(1)} & \subseteq & \cdots & \subseteq & \mathbf{J(s-1)} & \subseteq & \mathbf{J(s)} & \subseteq & \cdots \\
\| & & \| & & & & \| & & \| & & \\
\mathbf{I(0)} & \subseteq & \mathbf{I(1)} & \subseteq & \cdots & \subseteq & \mathbf{I(s-1)} & \subseteq & \mathbf{I(s)} & \subseteq & \cdots
\end{array}$$

Proof

If not, then pick $f(x) \in J - I$ of minimal degree $m > 0$.

Since $I(m) = J(m)$, there is some $g(x) \in I$ of degree m with

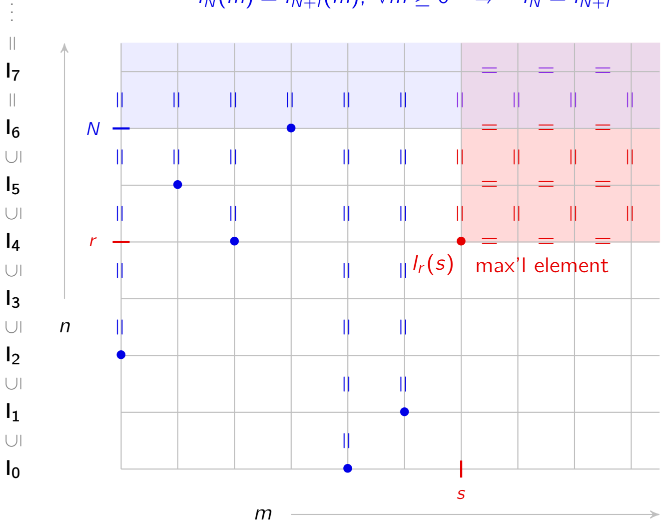
$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0, \qquad g(x) = a_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Then $f(x) - g(x)$ is in $J - I$ with smaller degree. □

Proof of Hilbert's basis theorem

Let $n_m =$ where the sequence $I_n(m) \subseteq I_{n+1}(m) \subseteq \cdots$ stabilizes, and $N = \max\limits_{0 \le m < s} \{n_m\}$.

$$I_N(m) = I_{N+i}(m), \ \forall m \geq 0 \quad \Rightarrow \quad I_N = I_{N+i}$$



An counterexample to Hilbert's basis theorem?

The ring $R = 2\mathbb{Z}$ is Noetherian because every ideal is finitely generated (actually, principal).

Consider the polynomial ring

$$\begin{aligned} R[x] = 2\mathbb{Z}[x] &= \big\{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in 2\mathbb{Z},\ n \in \mathbb{N} \big\} \\ &= \big\{ 2c_0 + 2c_1 x + \cdots + 2c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \big\}, \end{aligned}$$

with the following ideals:

$$(2) = \big\{ 2c_0 + 4c_1 x + \cdots + 4c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \big\},$$

$$(2, 2x) = \big\{ 2c_0 + 2c_1 x + 4c_2 x^2 + \cdots + 4c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \big\},$$

$$(2, 2x, 2x^2) = \big\{ 2c_0 + 2c_1 x + 2c_2 x^2 + 4c_3 x^3 + \cdots + 4c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \big\}.$$

$$(2, 2x, 2x^2, 2x^3) = \big\{ 2c_0 + 2c_1 x + 2c_2 x^2 + 2c_3 x^3 + 4c_4 x^4 + \cdots + 4c_n x^n \mid c_i \in \mathbb{Z},\ n \in \mathbb{N} \big\}.$$

We now have an ascending sequence of ideals that does not terminate:

$$(2) \subsetneq (2, 2x) \subsetneq (2, 2x, 2x^2) \subsetneq (2, 2x, 2x^2, 2x^3) \subsetneq \cdots.$$

Therefore, $R[x]$ is not Noetherian.