

Two notions for rings:

p is **irreducible** provided $p \neq 0$, p is not a unit, and
 $p = ab \Rightarrow a$ or b is a prime

p is **prime** provided $p|ab \Rightarrow p|a$ or $p|b$.

These two notions coincide for \mathbb{Z} or $\mathbb{Z}[i]$.

In general prime \Rightarrow irreducible:

Suppose p is prime and $p = ab$. Then $p|a$ or $p|b$. WLOG, $p|a$.
So $a = pk$, and $p(1 - kb) = 0$. So $1 - kb = 0$, and b is a unit.

In general, prime and irreducible are different.

Consider $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{5}bi : a, b \in \mathbb{Z}\}$

Have a norm: $N(a + \sqrt{5}bi) = a^2 + 5b^2$; with the properties as before.

Units just ± 1 .

$6 = 2 \cdot 3$; 2 and 3 irreducible

since $a^2 + 5b^2 = 2$ and $c^2 + 5d^2 = 3$ has no integer solutions.

$6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$; and $1 + \sqrt{5}i$ and $1 - \sqrt{5}i$ are both irreducible. (Since their norms are 6).

In $\mathbb{Z}[\sqrt{-5}]$: there is not unique factorization!

So there is no division algorithm.

Euclid's Lemma fails!: 2 divides $6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$; but 2 does not divide either of the factors.

Let's show there are no positive integer solutions to $x^2 + 1 = y^3$.

Suppose there were. Note $x^2 + 1 = (x + i)(x - i) = y^3$ in the Gaussian integers.

By Euclid's Lemma, both $x + i$ and $x - i$ divide y .

Thus $x^2 + 1$ divides y , say $(x^2 + 1)k = y$.

Substitution gives $x^2 + 1 = k^3(x^2 + 1)^3$.

so $(x^2 + 1)(k^3(x^2 + 1)^2 - 1) = 0$.

Integral domain implies $k^3(x^2 + 1) = 1$.

Taking norms implies that $x^2 + 1$ must be 1.

But then $x = 0$.

Now the integral domain $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{5}bi : a, b \in \mathbb{Z}\}$ behaves quite differently.

Still have a norm: $N(a + \sqrt{5}bi) = a^2 + 5b^2$; with the properties as before.

Units just ± 1 .

Polynomials

Let R be any commutative ring, and let x be a variable.

A *monomial* is something of the form ax^n where $a \in R$ and n is a nonnegative integer.

A *polynomial* is a sum of a finite number of monomials:

$$a_{i_1}x^{n_1} + a_{i_2}x^{n_2} + \cdots + a_{i_k}x^{n_k}.$$

We call a_{i_j} the coefficient of x^{i_j} .

The *degree* of a polynomial is the largest n such that the polynomial has a term a_nx^n with $a_n \neq 0$.

Given a polynomial of degree n , we can write it as

$a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$ (be including some additional terms with 0 coefficients).

or for any $m > n$, we can write it as

$$a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n + 0x^{n+1} + \cdots + 0x^m$$

Addition: Add like terms

$$(a_0 + a_1x^1 + \cdots + a_nx^n) + (b_0 + b_1x^1 + \cdots + b_nx^n) \\ = (a_0 + b_0) + (a_1 + b_1)x^1 + \cdots + (a_n + b_n)x^n.$$

Multiplication: Use distributivity and $x^m \cdot x^n = x^{m+n}$.

$$\left(\sum_{k=0}^n a_k x^k\right) \left(\sum_{\ell=0}^m b_\ell x^\ell\right) = \sum_{p=0}^{m+n} (a_0 b_p + a_1 b_p + \cdots + a_p b_0) x^p$$

These operations make $R[x]$ into a commutative ring.

Zero is the polynomial 0 (i.e. all coefficients 0).

Multiplicative identity is 1

If R is an integral domain, then the degree of a product is the sum of the degrees

R an integral domain $\Rightarrow R[x]$ is an integral domain

Have to be careful with notion of zero polynomial!

Consider $p(x) = x^3 - x \in \mathbb{Z}_3[x]$.

$p(0) = 0$, $p(1) = 1^3 - 1 = 0$, and $p(2) = 2^3 - 2 = 0$ (in \mathbb{Z})

So $p(x)$ is identically zero as a function, but it is not the zero polynomial!

I.e $p(x)$ and the polynomial 0 have the same graph, but they are different polynomials.

We'll see this doesn't happen over characteristic 0 fields.

For a field \mathbb{F} we have:

The Division Algorithm

Let $a(x)$, and $b(x)$ be polynomials in \mathbb{F} with $b(x)$ nonzero.

Then there exist unique polynomials $q(x)$ and $r(x)$ such that

$$a(x) = b(x)q(x) + r(x) \text{ and } r(x) = 0 \text{ or } \deg(r(x)) < \deg(b(x)) .$$

Proof idea: Reduce! Let a have degree m and b have degree n

If $a(x)$ small (i.e. $m < n$), can use $q(x) = 0$ and $r(x) = a(x)$.

Otherwise, $a(x) - cx^{m-n}b(x)$ has degree less than a for some c .

Find quotient and remainder for this:

$$a(x) - cx^{m-n}b(x) = b(x)q(x) + r(x).$$

So $a(x) = b(x)[q(x) + cx^{m-n}] + r(x)$, and we're done.

A root of $p(x) \in \mathbb{F}[x]$ is an element $a \in \mathbb{F}$ such that $p(a) = 0$.

Root-Factor Theorem

a is a root of $p(x)$ if and only if $(x - a)$ divides $p(x)$.

Proof.

Suppose $p(a) = 0$. Divide $(x - a)$ into $p(x)$ to get

$p(x) = (x - a)q(x) + r(x)$, where $r(x) = 0$ or has degree 0.

Plugging in a , gives $r(a) = 0$. So r is the zero polynomial, and $(x - a)$ divides $p(x)$.

Conversely, suppose $p(x) = (x - a)m(x)$ for some $m(x)$. Then clearly, $p(a) = 0$.

Consequence:

If $p(x)$ is a nonzero polynomial in $\mathbb{F}[x]$ of degree k , then $p(x)$ has at most k roots.

Proof:

$p(x)$ has roots $a_1, \dots, a_\ell \Rightarrow$

$p(x) = (x - a_1)(x - a_2) \cdots (x - a_\ell)m(x)$ for some nonzero polynomial $m(x)$.

Thus, $\deg(p(x)) \geq \ell$.