21. 2. 2024

All our rings have 1 unless otherwise stated explicitly. 10

Thm Chinese Remainder thm

Let R be a comm w/ 1, $I_1, \dots I_n$ ideals in R, then the map

$$\phi : R \longrightarrow (R/I_1) \times (R/I_2) \dots \times R/I_n$$

$$r \longrightarrow (r+I_1, r+I_2, \dots, r+I_n)$$

is a ring homomorphism with kernel $I_1 \cap I_2 \dots \cap I_n$.

If for each $i \neq j$ $I_i + I_j = R$, then the map is surjective and $\bigcap_{i=1}^{n} I_i = I_1 \dots I_n$ and we have

$$R/(I_1 \dots I_n) \cong (R/I_1) \times \dots \times (R/I_n).$$

Quotient field of an integral domain

If R is a comm. ring, and $a \in R$ is not a zero divisor and $a \neq 0$ then $ab = ac \Rightarrow b = c$

Thus a non-zero divisor enjoys some of the properties of a unit without necessarily possessing an inverse

It turns out that a comm. ring R can always be made into a subring of a larger ring Q in which every non-zero elt of R which is not a zero divisor becomes a unit in Q.
In the case that R is an int. domain, Q is a field, called the field of fractions.

The construction of Q from R takes its inspiration from the construction of $\mathbb{Q}$, rationals, from $\mathbb{Z}$, integers

Let R be an integral domain.
On the set of pairs $(a, b) \in R \times (R \setminus \{0\})$ we define an equivalence relation

$$(a, b) \sim (c, d) \iff ad - bc = 0$$

let $\frac{a}{b}$ denote the equiv. class of (a, b).

$$\boxed{Q(R) := \left\{ \frac{a}{b} \mid a \in R,\ b \in R - \{0\} \right\} \quad \text{with } +, \cdot}$$

$$\boxed{\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}}$$

$Q(R)$ is called the quotient field of R.

Side remark This construction can be generalized to more general rings. But we need some restriction on the "denominators" that it should not contain zero divisors and and it should be closed under multiplication.
We then have

Thm: let R be a comm ring w/1, $D \neq \emptyset$ subset of R which does not contain 0, any zero divisors and is closed under multiplication.
Then $\exists$ a comm ring Q with 1 s.t. R is a subring of Q and every elt of D is a unit in Q.

The ring Q is denoted by $D^{-1}R$.
It is the smallest ring containing R in which elts of D become units. Every elt of $D^{-1}R$ is of the form $d^{-1}r$ with $d \in D$, $r \in R$.

eg. ① R com ring $d \neq 0$, not a zero divisor
$D = \{1, d, d^2, \ldots\}$. Then $D^{-1}R \cong R[1/d]$

② R int. dom. $D = R \setminus \{0\}$, $D^{-1}R = Q(R)$ from before.

Next we restrict ourselves to commutative rings.

For a ring R and an ideal I, one can observe that R/I can be "better" or "worse" than R.

eg ① $\mathbb{Z}$ has no zero divisors but $\mathbb{Z}/6\mathbb{Z}$ does

② On the other hand for $R = \mathbb{Z}/6\mathbb{Z}$ let $I = \{0, 3\}$ an ideal of R. Then $R/I \cong \mathbb{Z}/3\mathbb{Z}$ has no zero divisors even though R does.

Natural question: Given R, I which properties of R translate to which properties of I

with $a \notin I$

$I+a$ is a zero divisor of R/I $\iff$ $\exists$ $b+I \in R/I$ w/ $b \notin I$ s.t. $(I+a)(I+b) = I$

$\iff$ $ba \in I$

Hence ruling out zero divisors motivates the following defn.

Defn A proper ideal I of R is called a prime ideal if $\forall\, a, b \in \mathbb{R}$ with $ab \in I$ we have that either $a \in I$ or $b \in I$

Thm Let R be a comm ring with 1.
R/I is an integral domain $\iff$ I is a prime ideal

Rk This thm can also be taken as defn of a prime ideal and shown that it is equivalent to the defn we gave.

Next question is when R/I is a field.

Thm Let R be a comm ring w/ 1.
R/I is a field $\iff$ I is a maximal ideal

lemma ① R comm ring w/ 1. R is a field $\iff$ its only ideals are 0 and R.
② $I \trianglelefteq R$. $I = R \iff I$ contains a unit

$0 \neq I$ maximal ideal $\Rightarrow$ I prime ideal

(prime ideal $\not\Rightarrow$ max'l ideal

Defn Let R be a ring w/1. The characteristic of a ring is the smallest positive integer n (if it exits) such that $\underbrace{1_R + \dots + 1_R}_{n \text{ times}} = 0$

If no such n exists, the ring is said to have characteristic zero

The characteristic is the natural number n such that $n\mathbb{Z}$ is the kernel of the homomorphism
$$\mathbb{Z} \longrightarrow R$$
$$n \longrightarrow n.1_R$$

Prime ring (Primring) of a ring R is the smallest subring $S \neq 0$ of the ring R.

It is unique and is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n > 0$.

If F is a field then its characteristic is either zero or a prime number p.

The Primesubfield is the smallest subfield of F and is isomorphic either to $\mathbb{Q}$, the rationals, or $\mathbb{Z}/p\mathbb{Z}$ = field of p elements.

Important example: Polynomial rings

Let R be a comm ring w/ 1. Consider the set of sequences
$$S = \{ (a_i)_{i \in \mathbb{N}} \mid a_i \in R \ \forall i \text{ and } a_i = 0 \text{ for all but finitely many } i \}$$

let $x := (0, 1, 0 \dots 0 \dots) \in S$

We define the addition and multiplication in S of $(a_i), (b_i) \in S$ via

$$(a_i)_i + (b_i)_i := (a_i + b_i)_i$$

$$(a_i) \cdot (b_i) := (c_k)_k \qquad c_k := \sum_{i+j=k} a_i b_j$$

With these operations S becomes a ring.

The zero elt $0 = (0, \dots 0 \dots)$

$$x^n = \underbrace{x \dots x}_{n \text{ times}} = (0, \dots, \underset{\uparrow \, n\text{-th position}}{1}, 0 \dots)$$

$a \in R$ can be identified with $(a, 0 \dots 0)$.

For $a \in R$ we have $ax^n = (0 \dots 0, \underset{\uparrow \, n\text{-th position}}{a}, 0 \dots)$

and $(a_0, a_1, \dots, a_n, 0 \dots)$
$$= a_0 + a_1 x + \dots + a_n x^n$$

and we can identify the ring S with the formal expressions $\{ f(x) = \sum_{i=0}^{n} a_i x^i \mid a_i \in R, n \in \mathbb{N} \}$

and write $R[x]$ instead of S.

Elements of $R[x]$ are called polynomials

If $f \in R[X] \setminus \{0\}$, $f = \sum_{i=0}^{n} a_i x^i$ with $a_n \neq 0$, then n is called the degree of f (grad)

a_n is called the leading coefficient of f

If $a_n = 1$, f is called monic

Rmk: The ring in which the coefs are taken makes a big difference in the behaviour of polynomials

eg. ① x^2+1 is not a square in $\mathbb{Z}[x]$
but $(x^2+1) = (x+1)^2$ in $(\mathbb{Z}/2\mathbb{Z})[x]$.

②

In $\mathbb{Z}[x]$, $\deg fg = \deg f + \deg g$

but in $(\mathbb{Z}/6\mathbb{Z})[x]$ it is not true anymore

$$\underbrace{(2x+1)}_{\deg=1}\underbrace{(3x)}_{\deg=1} = \underbrace{(3x)}_{\deg=1}$$

Prop: If R is an Int. domain (ID), $p, q \in R[x]$
then ⓐ $\deg pq = \deg p + \deg q$
ⓑ $(R[x])^{\times} = R^{\times}$ (units in $R[x]$ = units in R)
ⓒ $R[x]$ is an integral domain

<u>Universal property</u>: let R, S be comm rings, $s_0 \in S$ and $\varphi : R \to S$ a ring homomorphism.
Then $\exists$ a unique ring hom
$\varphi_{s_0} : R[X] \to S$ such that $\varphi_{s_0} \circ \iota = \varphi$

where $\bar{\iota} : R \to R[X]$ is the natural embedding
$a \to (a, 0 \dots\dots)$

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr] & & S \\ & R[X] \arrow[ur, "\varphi_{s_0}"'] & \end{tikzcd}$$

$$\varphi_{s_0}(f(x)) = \varphi_{s_0}\left(\sum_{i=0}^{n} a_i x^i\right) := \varphi(a_0) + \varphi(a_1)s_0 + \dots \varphi(a_n)s_0^n$$

is the evaluation mapping (Auswertungsabbildung)

Each polynomial $f \in R[X]$ induces a polynomial function for each hom $\varphi : R \to S$, namely the function

$$S \longrightarrow S$$
$$s_0 \longmapsto \sum_{i=0}^{n} \varphi(a_i)s_0^i =: f_\varphi(s_0) \stackrel{\swarrow}{=} f(s_0)$$

by abuse of notation

<u>Rmk</u>: If R is finite, different polynomials over R can define the same polynomial function
eg. The polynoms 0, $X^2 + X \in (\mathbb{Z}/2\mathbb{Z})[X]$ define the same polynomial function

Division algorithm for polynomials

Thm 1 (1) Let F be a field, $f(x), g(x) \in F[x]$ with $b(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x) \quad \text{with } r(x) = 0 \text{ or } \deg r(x) < \deg b(x)$$

(2) Let $f \in F[x]$, $a \in F$. Then $\exists !$ poly $q \in F[x]$ s.t

$$f(x) = q(x)(x-a) + f(a).$$

Moreover $(x-a)$ divides $f(x) \iff f(a) = 0$.
In this case a is called a zero of f

Recall: For R a comm ring w/ 1 and $a, b \in R$, we say a divides b and write $a \mid b$ if $\exists\, c \in R$ s.t $ac = b$

Thm 2 If F is a field then $F[x]$ is a principal ideal domain

Thm 3 Let F be a field, $f \in F[x]$ a poly of degree $n > 0$. Then f has at most n zeroes in F.

Rk (1) Note Thm 3 is not true for general rings
$x^2 - 1 \in (\mathbb{Z}/8\mathbb{Z})[x]$ has 4 zeroes $1, 3, 5, 7$

Rmk

(2) The division alg. also holds for general comm rings w/ 1 in a generalized form

Thm (a) let $f, g \in R[x]$, $g \neq 0$ with leading coef b_m. Then $\exists\ q, r \in R[x]$ with degree $r <$ deg q and a $k \in \mathbb{N}$ s.t

$$b_m^k f = g q + r$$

(b) let $f \in R[x]$, $a \in R$. Then $\exists!$ poly $h \in R[x]$ s.t

$$f(x) = h(x)(x-a) + f(a)$$

$(x-a) \mid f \iff f(a) = 0$.

Rmk (3) if F is not a field, then in general $F[x]$ is not a PID

Eg In $\mathbb{Z}[x]$, the ideal $(2, x)$ is not principal

$$(2, x) = \{ 2p(x) + x q(x) \mid p, q \in \mathbb{Z}[x] \}$$

Assume $(2,x)$ is principal. Then $\exists\ a(x) \in \mathbb{Z}[x]$ s.t $(2,x) = (a(x))$. In particular $2 = a(x) b(x)$ for some $b \in \mathbb{Z}[x]$. Looking at the degrees both a, b must be constant. Since 2 is prime $a, b \in \{\pm 1, \pm 2\}$. But if $a = \pm 1$ then $(2,x) = \mathbb{Z}[x]$ which is not the case (Not every poly have even const term). Hence $a(x) = \pm 2$. But then $x \in (2)$ $\lightning$ Since $x = 2q(x)$ w/ $q \in \mathbb{Z}[x]$ is impossible.

Chapter 1

Euclidean Domains, Principal ideal Domains and Unique Factorization Domains

(Euclidischer Ring, Hauptidealring, Factorielle Ringe)

There are classes of rings which have more algebraic structure than generic rings.

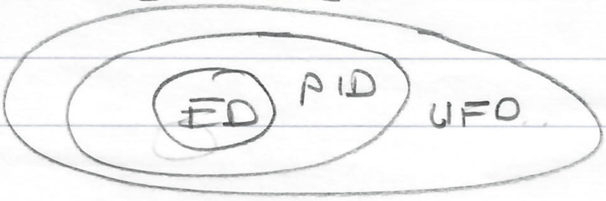
- The usual integers $\mathbb{Z}$ has a Euclidean algorithm, every ideal is principal and every $n \in \mathbb{Z}$ is a unique product of powers of primes.

Our goal is to look at these properties in general integral domains

We'll consider rings

- which have a division alg (Euclidean domains)
- in which every ideal is principal (PID)
- in which every element have factorization into "irreducible" elements (UFD)

We'll see ED $\Rightarrow$ PID $\Rightarrow$ UFD.



An important property of integers is that we can do division with remainder, ie if $a, b \in \mathbb{Z}$, then $\exists\ q, r \in \mathbb{Z}$ s.t

$$a = bq + r, \quad 0 \leq r < |b|$$

To get such an algorithm (Division w/ remainder, Euclidean alg) the remainder r should be in some sense smaller than b. In general rings R we measure this by a function

$$N : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0} = \{0, 1, 2 \dots\}$$

<u>Defn</u> An integral domain R is said to be an <u>Euclidean domain</u> if there is a function $N : R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ s.t For any 2 elements $a, b \in R \setminus \{0\}$ $\exists\ q, r \in R$ with

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

The element q is called the quotient
r " " " remainder.

<u>Examples</u> ① $\mathbb{Z}$, $N(a) := |a|$

② $F[x]$, F a field, $N(p(x)) := \deg p$.

③ <u>Exercise</u>: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a ED with $N(a+bi) := a^2 + b^2$

(4) Every field F is an E.D. Take $N(a)=0$ $\forall a$. For a, b, $b \neq 0$
$a = bq + 0$ with $q = ab^{-1}$

We have seen that the ring $F[x]$ with F a field is also a PID.
It is also true for $\mathbb{Z}$.
In general we have

Theorem 1.1 An Euclidean domain is a PID

Proof. Let R be an ED with $N: R\setminus\{0\} \to \mathbb{Z}_{\geq 0}$

w.t.s every ideal $I \trianglelefteq R$ is principal.
The zero ideal $\{0\} = \langle 0 \rangle$ is principal
Let $I \neq \{0\}$ be a non-trivial ideal.

Let $a \in I$, $a \neq 0$ be s.t. $N(a)$ is the smallest.
(Such an a exists since the set $\{N(b) \mid b \in I\}$ has a minimum by well-ordering of $\mathbb{Z}$.)

Claim: $I = \langle a \rangle$.
Clearly $\langle a \rangle \subset I$. To see the other inclusion, let $b \in I$. Then division alg in R gives $b = aq + r$, $q, r \in R$ with $r = 0$ or $N(r) < N(a)$
Since $r = b - qa \in I$ this contradicts the choice of a unless $r = 0$. In that case

$b = qa \in \langle a \rangle$. Hence $I = \langle a \rangle$ and I is principal ☒

Recall in $\mathbb{Z}$, Euclidean algorithm also produces greatest common divisors.

But we first define various notions in a general integral domain R.

Defn let R be an I.D.

1. An element $r \in R$ is called irreducible (Irreduzibel, unzerlegbar) in R if $r \neq 0$, $r \notin R^\times$ and $r = ab$ with $a, b \in R$ implies that either $a \in R^\times$ or $b \in R^\times$

2. An element $p \in R$ is called a prime element (Primelement) if $p \neq 0$, $p \notin R^\times$ and $p \mid ab$ implies that $p \mid a$ or $p \mid b$.

3. 2 elements $a, b \in R$ are called associates (assoziiert) if $\exists$ $r \in R^\times$ such that $a = r^\times b$. We write $a \sim b$.

4. Let $a, b \in R \setminus \{0\}$. Then $d \in R$ is called (gcd) a greatest common divisor of a and b (grösste gemeinsamer Teiler von a und b) if (1) $d \mid a$, $d \mid b$ and (2) if $c \mid a$ and $c \mid b$ then $c \mid d$