(37) Now we can define what unique factorization means and see why PID's have it.

DEF'N: (12.2.12) A domain R is a <u>unique factorization domain</u> (U.F.D.)

if for every $r \in R - \{0\}$ which is <u>not a unit</u>,

(a) there <u>exists</u> a factorization $r = p_1 p_2 \cdots p_n$ with p_i <u>irreducible</u> in R

(b) it is <u>unique</u> in the sense that if $r = p_1 \cdots p_n = q_1 \cdots q_m$ with p_i, q_j irreducibles

then in fact $n = m$ and one can re-index so that p_i, q_i are <u>associates</u> ($p_i = u_i q_i$ with $u_i \in R^\times$) for $i = 1, 2, \ldots, n$

EXAMPLE: In $\mathbb{Z}$, this is usual <u>uniqueness of prime factorization</u>

e.g. $40 = 2 \cdot 2 \cdot 5 \cdot 5$
$= (-2) \cdot 5 \cdot (-2) \cdot 5$
$= (-5) \cdot 2 \cdot (-2) \cdot 5$
$= \cdots$

2/20/2019 >

Parts (a) & (b) in the UFD definition are really separate issues, and PID's avoid the problem for both.

PROPOSITION: (12.2.13) (i) A domain R has existence of factorizations $r = p_1 p_2 \cdots p_n$ into irreducibles p_i $\forall r \in R$ if
$\nexists$ an infinite (strictly) ascending chain of principal ideals
$$(a_1) \subsetneqq (a_2) \subsetneqq (a_3) \subsetneqq \cdots \text{ in } R$$

(ii) In particular, P.I.D.'s have no such chains of principal ideals, so they <u>do</u> have irred. factorizations.

NON-EXAMPLE: $R = \mathbb{R}[t, t^{1/2}, t^{1/4}, t^{1/8}, \ldots]$

contains elements like $7t + 20t^{5/16} - 109t^{\frac{43}{256}}$

and t has <u>no</u> <u>irreducible factorization</u>, e.g. $t = t^{1/2} \cdot t^{1/2}$
$= (t^{1/4} \cdot t^{1/4})(t^{1/4} \cdot t^{1/4})$
$= (t^{1/8} \cdot t^{1/8})(t^{1/8} \cdot t^{1/8})(t^{1/8} \cdot t^{1/8})(t^{1/8} \cdot t^{1/8})$
$= \cdots$

also $(t) \subsetneqq (t^{1/2}) \subsetneqq (t^{1/4}) \subsetneqq (t^{1/8}) \subsetneqq \cdots$

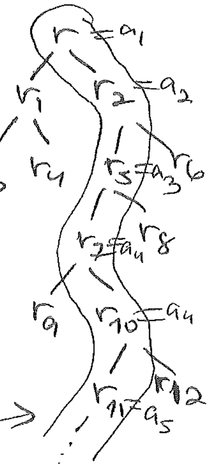
(38) proof: (i) If $\nexists$ ∞ chains $(a_1) \subsetneq (a_2) \subsetneq \dots$ in R

then given any $r \in R$, try to factor it. If it's irreducible, done

If not $r = r_1 r_2$ is a proper factorization

If r_1, r_2 irreducible, done.

Else one or both has a proper factorization.



Repeat, and if the process never terminates, one obtains an ∞ chain

$(a_1) \subsetneq (a_2) \subsetneq \dots$

by following an infinite branch $\boxed{\text{here}}$

(ii) In a P.I.D., given $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$

consider $I = (a_1) \cup (a_2) \cup (a_3) \cup \dots \subset R$

which we claim is an ideal of R:

given $a, b \in I$ say $a \in (a_i)$, $b \in (a_j)$ then $a + b \in (a_{\max(i,j)}) \subset I$

and $r \in R$ and $ra \in (a_i) \subset I$

Since R is a PID, $I = (a_0)$ for some $a_0 \in R$

But then $a_0 \in (a_i)$ for some i

and hence $(a_i) = (a_{i+1}) = (a_{i+2}) = \dots = I = (a_0)$ ∎

THEOREM: PROP (12.2.14) In a domain R ~~that~~ has ~~factorizations~~ $r = p_1 \cdots p_n$ into irreducibles for all $r \in R$, the factorizations are unique (i.e. R is a UFD)

$\iff$ irreducibles are all prime

In particular, P.I.D.'s are U.F.D.'s.

proof: ($\Leftarrow$): Assuming irreducibles are prime, given two factorizations $r = p_1 \cdots p_n = q_1 \cdots q_m$ say with $m \le n$, want $m = n$ and reindexing so p_i, q_i are associates.

Induct on n, with base case $n=1$ easy since $r = p_1 = q_1$

In the inductive step $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$

$\Longrightarrow$ p_1 divides $q_1 \cdot (q_2 \cdots q_m)$, and p_1 irreducible is also prime

so either $\underbrace{p_1 \text{ divides } q_1}$ or $\underbrace{p_1 \text{ divides } q_2 \cdots q_m}$

$\Rightarrow p_1 = u_1 q_1$, $u_1 \in R^\times$

$\Rightarrow$ continue by induction on m until p_1 divides some q_j and re-index $j=1$

Thus $p_1 p_2 \cdots p_n = u_1 p_1 \cdot q_2 \cdots q_m$

$= p_1 \cdot u_1 q_2 \cdots q_m$

R a domain

So $p_1 (p_2 \cdots p_n - u_1 q_2 \cdots q_m) = 0 \Rightarrow p_2 \cdots p_n = \underbrace{u_1 q_2}_{\text{call this } q_2'} \cdots q_m$

$= q_2' \cdots q_m'$

Apply induction on n to say $m=n$ and p_i, q_i' are associates for $i = 2, \ldots, n$. ∎

$(\Longrightarrow)$: If some irreducible p is not prime, so

$p \mid ab =: r$ but $p \nmid a$, $p \nmid b$, then factor $r = ab$

$\vdots$

$= a_1 \cdots a_n b_1 \cdots b_m$

a_i, b_j irreducibles

but also factor $r = pc$

$\vdots$

$= p\, q_1 \cdots q_\ell$, q_i irreducibles

and p is not associate to any of a_i, b_j since $p \nmid a$, $p \nmid b$ ∎

EXAMPLES:

① In $R = \mathbb{F}[x]$, $\mathbb{F}$ a field, which is a P.I.D and hence UFD, the units $R^\times = \mathbb{F}^\times = \mathbb{F} - \{0\}$ (Why? Think about degrees in $u(x) \cdot v(x) = 1$)

so associates are scalar multiples

e.g. $x^2 - 3x + 2 = (x-1)(x-2)$ in $\mathbb{Q}[x]$

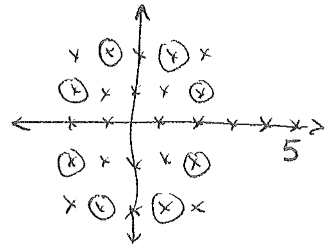
$= (\tfrac{1}{2}x - 2)(2x-4)$ in $\mathbb{Q}[x]$

$x^2 - \bar{3}x + \bar{2} = (x - \bar{1})(x - \bar{2})$ in $\mathbb{F}_5[x]$

$= (\bar{3}x - \bar{3})(\bar{2}x - \bar{4})$ in $\mathbb{F}_5[x]$

② In $\mathbb{Z}[i]=R$ which is a Euclidean domain hence PID hence UFD, the units $R^\times=\{\pm1,\pm i\}$ e.g.

$$\begin{aligned}5&=(2+i)(2-i)\\&=(-2-i)(-2+i)\\&=(-1+2i)(-1-2i)\\&=(1+2i)(1-2i)\end{aligned}$$



§12.3 Gauss's lemma

Is $\mathbb{Z}[x]$ a UFD? It's not a P.I.D., e.g. $(2,x)$ is not principal.

There is no problem with the existence of irred. factorizations,

e.g. $4x^2-12x+8=4(x^2-3x+2)$ ← factor out the GCD of the coefficients

$=4(x-1)(x-2)$ ← use induction on degree to reach irreducibles

We'll show $\mathbb{Z}[x]$ is a UFD by using its inclusion $\mathbb{Z}[x]\subset\mathbb{Q}[x]$ ...

2/22/2019 > DEFIN: Call $f(x)\in\mathbb{Z}[x]$ **primitive** if $GCD(a_0,\ldots,a_n)=1$ and $a_n>0$.

$f(x) = a_0+a_1x+\ldots+a_nx^n$

EXAMPLES: ① $f(x)=8x^2+12x-16$ is not primitive

$=4\underbrace{(2x^2+3x-4)}$ ← this is primitive

② $f(x)=2-x$ is not primitive

$=-\underbrace{(-2+x)}$ ← this is primitive

PROPOSITION (Gauss's lemma) (12.3.4)

(a) Primes $p\in\mathbb{Z}$ are also prime elements of $\mathbb{Z}[x]$,

i.e. if $p\mid f(x)g(x)$ for $f,g\in\mathbb{Z}[x]$ then $p\mid f(x)$ or $p\mid g(x)$

(b) $f(x),g(x)$ primitive $\Rightarrow$ $f(x)g(x)$ primitive.