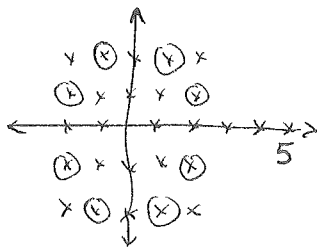
② In $\mathbb{Z}[i] = R$ which is a Euclidean domain hence PID hence UFD,
the units $R^\times = \{\pm 1, \pm i\}$ e.g. $5 = (2+i)(2-i)$
$= (-2-i)(-2+i)$
$= (-1+2i)(1-2i)$
$= (1+2i)(1-2i)$



§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 $\mathbb{Z}[x] \subset \mathbb{Q}[x]$ ...

1/28/2019 > DEFN: Call $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ primitive if $\gcd(a_0, \dots, a_n) = 1$ and $a_n > 0$.

EXAMPLES: ① $f(x) = 8x^2 + 12x - 16$ is not primitive
$= 4(2x^2 + 3x - 4)$
↑ this is primitive

② $f(x) = 2 - x$ is not primitive
$= -(-2 + x)$
↑ 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.

proof: (a) If a prime $p \in \mathbb{Z}$ has $p \mid f(x)g(x)$

then reduce coefficients $\mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x] = \mathbb{F}_p[x]$

to get $\bar{0} = \bar{f}(x)\bar{g}(x)$ in $\mathbb{F}_p[x]$

$\Rightarrow$ either $\bar{0} = \bar{f}(x)$ in $\mathbb{F}_p[x]$ since $\mathbb{F}_p[x]$ is a domain
or $\bar{0} = \bar{g}(x)$

$\Rightarrow$ $p \mid f(x)$ or $p \mid g(x)$ in $\mathbb{Z}[x]$.

(b) If $f(x), g(x)$ are both primitive then $\forall$ primes $p \in \mathbb{Z}$,

$p \nmid f(x)$ in $\mathbb{Z}[x]$
$p \nmid g(x)$ in $\mathbb{Z}[x]$
$\Rightarrow$ (part(a)) $p \nmid f(x)g(x)$ in $\mathbb{Z}[x]$ $\Rightarrow$ $f(x)g(x)$ has no primes p dividing GCD of its coefficients, so it is primitive (also its leading coefficient is > 0) ∎

DEF'N-LEMMA (12.3.5) Nonconstant polynomials $f(x) \in \mathbb{Q}[x]$ have a unique expression $f(x) = c \cdot f_0(x)$ with $f_0(x) \in \mathbb{Z}[x]$ primitive and $c \in \mathbb{Q}$ (called the content $\text{cont}(f)$ of f)

e.g. $f(x) = \frac{-x^2}{5} - \frac{3}{10}x + \frac{2}{5} = \frac{-1}{10}(2x^2 - 3x - 4)$

Furthermore $\text{cont}(f) \in \mathbb{Z} \Leftrightarrow f \in \mathbb{Z}[x]$,

in which case $\text{cont}(f) = \text{GCD}(a_0, \ldots, a_n)$ where $f = a_0 + a_1 x + \ldots + a_n x^n$

proof: Existence is easy: if $f(x) \in \mathbb{Z}[x]$, $\sum_{i=0}^{n} a_i x^i$

then let $c = \pm \text{GCD}(a_0, \ldots, a_n)$ and write $f(x) = c \underbrace{f_0(x)}_{\text{primitive}}$

↑ choose this so f_0 has top coeff > 0

If $f(x) \in \mathbb{Q}[x]$, first clear denominators to get $df(x) \in \mathbb{Z}[x]$

then write $df(x) = c \cdot f_0(x)$ as above

and $f(x) = \frac{c}{d} \cdot f_0(x)$

But why is it unique? Given $cf_0 = c'f_0'$ with $f_0, f_0' \in \mathbb{Z}[x]$ primitive, $c, c' \in \mathbb{Q}$

we'll show why $f_0 = f_0'$ (which then forces $c = c'$).

By clearing denominators in c, c', can assume $c, c' \in \mathbb{Z}$.

If $c \neq \pm 1$, pick a prime p dividing c, so $cf_0 = c'f_0'$ shows p divides $c'f_0'$, and hence p divides c' by primeness of p in $\mathbb{Z}[x]$ or p divides f_0', false, since f_0' primitive.

Hence p divides c'. Now cancel p from both c, c' and induct on number of prime factors in c, c' ∎

This shows there are no surprises about relating factorization in $\mathbb{Z}[x]$ vs. $\mathbb{Q}[x]$...

THEOREM (12.3.6): (a) For $f_0, g \in \mathbb{Z}[x]$ with f_0 primitive

$$f_0 \mid g \text{ in } \mathbb{Z}[x] \iff f_0 \mid g \text{ in } \mathbb{Q}[x]$$

(b) $f, g \in \mathbb{Z}[x]$ have a nonconstant common factor in $\mathbb{Z}[x]$ $\iff$ they have one in $\mathbb{Q}[x]$

proof: (a) Given $g(x) = f_0(x)\, q(x)$ with $q(x) \in \mathbb{Q}[x]$

we want to show $q(x) \in \mathbb{Z}[x]$

Write $g(x) = c \cdot g_0(x)$ with $g_0, q_0 \in \mathbb{Z}[x]$ primitive

$q(x) = d \cdot q_0(x)$ $c, d \in \mathbb{Q}$

Then $c\, g_0(x) = d\, f_0(x) q_0(x)$ $\Longrightarrow$ $c = d$ (uniqueness)

($f_0(x) q_0(x)$ primitive by Gauss's Lemma)

But $g(x) \in \mathbb{Z}[x]$ forces $c \in \mathbb{Z}$, so $q(x) = d\, q_0(x) = c\, q_0(x) \in \mathbb{Z}[x]$ also.

(b) If $f, g \in \mathbb{Z}[x]$ have $h \in \mathbb{Q}[x]$ with $h \mid f, g$

then writing $h = c \cdot h_0$ with $h_0 \in \mathbb{Z}[x]$ primitive, $c \in \mathbb{Q}$

$h_0 \mid f, g$ in $\mathbb{Q}[x]$, so $h_0 \mid f, g$ in $\mathbb{Z}[x]$ by part (a) ∎

COROLLARY (PROP 12.3.7. THM 12.3.8)

(a) The irreducibles in $\mathbb{Z}[x]$ are the primes p in $\mathbb{Z}$ and the primitive polynomials in $\mathbb{Z}[x]$ that are irreducible in $\mathbb{Q}[x]$

(b) Both kinds are also prime elements of $\mathbb{Z}[x]$

(c) Consequently, $\mathbb{Z}[x]$ is a U.F.D.

proof: Note (c) follows from (a) & (b), since factorizations exist in $\mathbb{Z}[x]$.

For (a) & (b), note that for constant polynomials $f(x)=a_0 \in \mathbb{Z}$ part (a) is pretty clear and (b) we already proved earlier.

For a nonconstant polynomial $f(x) \in \mathbb{Z}[x]$,

to see (a), note that if f is irreducible in $\mathbb{Z}[x]$ it better have $\text{cont}(f) = \pm 1$, so WLOG f is primitive.

If it had a proper factorization $f=gh$ in $\mathbb{Q}[x]$

write $g = cg_0$ with $c,d \in \mathbb{Q}$
$h = dh_0$ g_0, h_0 primitive in $\mathbb{Z}[x]$

and then $f = cd\, g_0 h_0$ forces $cd=1$ and $f=g_0h_0$,
(f primitive; g_0h_0 primitive, by Gauss's lemma)

a factorization in $\mathbb{Z}[x]$.

2/25/2019 >

To see (b), i.e. $f(x) \in \mathbb{Z}[x]$ primitive, irreducible in $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$ $\Rightarrow f(x)$ prime in $\mathbb{Z}[x]$,

note that if $f(x)$ divides $g(x)h(x)$ in $\mathbb{Z}[x]$
then since f is irred. in $\mathbb{Q}[x]$, it is prime in $\mathbb{Q}[x]$ (a PID & UFD)
hence f divides $g \cdot h$ in $\mathbb{Q}[x]$,
but then f divides $g \cdot h$ in $\mathbb{Z}[x]$ by previous THM part (a).

REMARK: Same proofs show THM: R a UFD $\Rightarrow$ $R[x]$ a UFD ($\Rightarrow R[x,y]=R[x][y]$ a UFD, $R[x_1,\dots,x_n]$ a UFD)

replacing $\mathbb{Z} \rightsquigarrow R$
$\mathbb{Q} \rightsquigarrow F = \text{Frac}(R)$
$\mathbb{Z}[x] \rightsquigarrow R[x]$
$\mathbb{Q}[x] \rightsquigarrow F[x] = \text{Frac}(R)[x]$