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 $\mathbb{Q}[x]$

e.g. $2x+2 = 2(x+1)$ is not prime in $\mathbb{Z}[x]$, although irred. 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 primitive; $g_0 h_0$ primitive, by Gauss's lemma)
$f = g_0 h_0$, 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, so 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).

REMARKS (1) Same proofs show THM: R a UFD $\Rightarrow R[x]$ a UFD (so $R[x,y] = R[x][y]$ a UFD, and $R[x_1, \ldots, x_n]$ a UFD)

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

(2) In a UFD, GCD's exist, since if $a = u p_1^{e_1} \cdots p_N^{e_N}$ p_i irred., $b = u' p_1^{e_1'} \cdots p_N^{e_N'}$ $u, u' \in R^\times$
then $\text{GCD}(a,b) = p_1^{\min(e_1, e_1')} \cdots p_N^{\min(e_N, e_N')}$

§12.4 Factoring in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$

When arguing irreducibility for $f(x) \in \mathbb{Q}[x]$, it's often easier to clear denominators and work in $\mathbb{Z}[x]$ instead, where one can use divisibility of coefficients, and reductions $\mathbb{Z}[x] \to \mathbb{F}_p[x]$.

Linear factors are easy to deal with...

LEMMA (12.4.2) (Rational root test) Given $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$,

(a) if $b_1 x + b_0$ divides f in $\mathbb{Z}[x]$, then $b_1 \mid a_n$ in $\mathbb{Z}$, $b_0 \mid a_0$

(since $f(x) = (b_1 x + b_0)\sum_{i=0}^{n-1} c_i x^i = \frac{b_0 c_0}{a_0} + (\dots)x^1 + \dots + \frac{b_1 c_{n-1}}{a_n} x^n$)

(b) if $\gcd(b_0, b_1) = 1$ then $b_1 x + b_0$ divides f in $\mathbb{Z}[x] \iff f\left(\frac{-b_0}{b_1}\right) = 0$

(c) if $a_n = 1$ so f is monic in $\mathbb{Z}[x]$, then any root $f(r) = 0$ with $r \in \mathbb{Q}$ actually has $r \in \mathbb{Z}$. (Write $r = \frac{-b_0}{b_1}$ with $\gcd(b_1, b_0) = 1$, and then b_1 divides $a_n = 1$ so $b_1 = \pm 1$)

EXAMPLE: $f(x) = x^3 - 3x - 1$ is irreducible in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$

because as a cubic, reducibility would require a linear factor $b_1 x + b_0$, so

(and a root $r = \frac{-b_0}{b_1}$)

$$\left.\begin{array}{l} b_1 \mid 1 \implies b_1 = \pm 1 \\ b_0 \mid (-1) \implies b_0 = \pm 1 \end{array}\right\} \implies r = \frac{-b_0}{b_1} = \pm 1$$

but $f(+1) = 1^3 - 3 - 1 = -3 \neq 0$

$f(-1) = (-1)^3 - 3 - 1 = -5 \neq 0$

How can reduction $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ help?

PROPOSITION (12.4.3): If $f(x) \in \mathbb{Z}[x]$ has its reduction $\bar{f}(x) \in \mathbb{F}_p[x]$ irreducible, and of the same degree, then f is irreducible in $\mathbb{Q}[x]$.

EXAMPLE: $f(x) = x^3 - 3x - 1$ is irreducible in $\mathbb{Z}[x]$, since applying $\mathbb{Z}[x] \to \mathbb{F}_2[x]$

$\bar{f}(x) = x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$ (cubic, no roots in $\mathbb{F}_2$)

and of same degree

NON-EXAMPLE: $f(x) = 1+3x+2x^2 \in \mathbb{Z}[x]$ has reduction to $\mathbb{F}_2[x]$ given by $\bar{f}(x) = 1+x$, which is irreducible, but of lower degree

And in fact, $f(x) = (1+x)(1+2x)$ is not irreducible in $\mathbb{Q}[x]$.

proof of PROP: Given $f(x) \in \mathbb{Z}[x]$ reducible,

say $f(x) = g(x)h(x)$ with $\deg(g), \deg(h) > 0$ and $\deg(f) = \deg(g)+\deg(h)$

then applying $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ gives

$\bar{f}(x) = \bar{g}(h)\,\bar{h}(x)$ with $\deg(\bar{g})+\deg(\bar{h}) = \deg(\bar{f}) = \deg(f)$ (by hypothesis)

$\deg(g) = \deg(\bar{g})$, $\deg(h) = \deg(\bar{h})$, $\deg(\bar{h}) > 0$

i.e. it is a proper factorization in $\mathbb{F}_p[x]$. ∎

REMARK: Unlike factoring in $\mathbb{Z}$, there is a fast algorithm for factoring in $\mathbb{F}_p[x]$, called Berlekamp's algorithm, from 1967.

2/27/2019 Another useful reduction trick:

Eisenstein's Criterion: If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ (PROP 12.4.6) has some prime p in $\mathbb{Z}$ with

$p \nmid a_n$,

$p \mid a_0, a_1, \dots, a_{n-1}$,

but $p^2 \nmid a_0$,

then f is irreducible in $\mathbb{Q}[x]$.

EXAMPLE: $x^5 - 24x^3 + 70x^2 - 10x + 6$ is irreducible in $\mathbb{Q}[x]$ using Eisenstein's criterion at $p=2$:

$p \nmid 1 = a_5$

$p \mid 6, -10, 70, -24, 0$
$\quad\;\; a_0 \;\; a_1 \;\; a_2 \;\; a_3 \;\; a_4$

$p^2 \mid 6$
$\quad\; a_0$

Proof of Eisenstein: If $f(x)=g(x)h(x)$ in $\mathbb{Q}[x]$, then this is also true in $\mathbb{Z}[x]$, so reduce $\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$

to give $\bar{f}(x) = \bar{g}(x)\,\bar{h}(x) \Rightarrow \bar{g}(x)=\bar{g}_r x^r$, $\bar{h}(x)=\bar{h}_s x^s$ for some r,s with $r+s=n$

$\bar{f}(x) = \bar{a}_n x^n$

(unique factorization in $\mathbb{F}_p[x]$, for example)

$$\Rightarrow g(x)=g_r x^r+\ldots+g_1 x+g_0$$
$$h(x)=h_s x^s+\ldots+h_1 x+h_0$$

where $g_0, g_1, \ldots, g_{r-1}$ and $h_0, h_1, \ldots, h_{s-1}$ $\Big\} \in p\mathbb{Z}$

$\Rightarrow a_0 = g_0 h_0 \in p^2\mathbb{Z}$. Contradiction ∎

---

§12.5 Primes in $\mathbb{Z}[i]$ and solving $x^2+y^2=n$

It turns out that understanding the primes in $\mathbb{Z}[i]$ (= irreducibles) comes down to knowing primes p in $\mathbb{Z}$ and which ones stay prime in $\mathbb{Z}[i]$, versus factoring further $p=\pi\cdot\bar{\pi}$ in $\mathbb{Z}[i]$

e.g. $2=(1+i)(1-i)$ $(=(i-1)(-i-1))$ not prime in $\mathbb{Z}[i]$

3 is prime in $\mathbb{Z}[i]$

$5=(2+i)(2-i)$ not prime in $\mathbb{Z}[i]$

7 is prime in $\mathbb{Z}[i]$

⋮