For pedestrians, when you cross the roads, you should as least notice there are cars on the road!

— Micheal Zieve

It's totally wrong, but I remembered I was told that Gauss had a personal computer, in the sense that there was some person who did computations for him. That does not make sense since Gauss is also the best at doing computations while being the best at everything else. But I like the idea.

— Micheal Zieve

Let R be a UFD and K be $\mathrm{Frac}(R)$.

Theorem. *Let R be a UFD and K be $\mathrm{Frac}(R)$. Then $R[x]$ is a UFD ($\implies$ $R[x,y]$ is UFD, $R[x_1,x_2,\ldots,x_n]$ is UFD.)*

Proof. First note that $K[x]^* = K^*$ and $R[x]^* = R^* \subseteq K^*$. For any nonconstant $f(x) := \sum_{i=0}^{n} a_i x^i$ in $R[x]$, define the "content" to be $c(f) := \gcd(a_0, a_1, \ldots, a_n)$. Then $f(x) = c(f) \cdot \hat{f}(x)$ where $c(\hat{f}) = 1$. (or equivalently a unit)

If $f(x) \in R[x] \setminus R$ has $c(f) = 1$, say $f(x)$ is "primitive". Note that if $f(x) \in R[x] \setminus R$ is irreducible, then $c(f) = 1$.

So the irreducibles in $R[x]$ are:

- irreducible elements in R (these are units in $K[x]$)
- nonconstant irreducible elements in $R[x]$ (these are primitive)

We'll show that the irreducible polynomials in $K[x]$ are precisely the primitive irreducible polynomials in $R[x]$ times elements of K^*. (e.g. $2x$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$, but x is irreducible in $\mathbb{Z}[x]$.)

Any nonconstant $f(x) \in K[x]$ can be written as $\frac{a}{b}\hat{f}(x)$ with $\hat{f}(x) \in R[x]$ primitive and $a, b \in R \setminus \{0\}$. We may assume that $\gcd(a,b) = 1$.

$f, g \in R[x]$ are primitive then fg is primitive, since if $c(fg) \neq 1$ then $\exists$ irreducible $p \in R$ *s.t.* $p \mid c(fg)$ $\implies$ if $\phi : R[x] \to (R/(p))[x]$ is the "reduce $\bmod p$" homomorphism then $\phi(fg) = 0$ $\implies$ $\phi(f)\phi(g) = 0$. But p is irreducible and R is UFD $\implies$ p is prime $\implies$ $R/(p)$ is an integral domain $\implies$ $(R/(p))[x]$ is an integral domain $\implies$ $\phi(f) = 0$ or $\phi(g) = 0$ $\implies$ $p \mid c(f)$ or $p \mid c(g)$ $\implies$ f or g is not primitive, a contradiction.

CLAIM: If $f \in R[x]$ is irreducible and primitive then f is irreducible in $K[x]$.

Proof of claim. Suppose $f = gh, g, h \in K[x]$ nonconstant. We may assume $g \in R[x]$, g

primitive. Then $h = \frac{a}{b}\hat{h}(x)$, $\hat{h}(x) \in R[x]$ primitive, a, b are nonzero and coprime.

Then $f = \frac{a}{b}g\hat{h} \implies g\hat{h}$ is primitive. Hence $bf = ag\hat{h}$ where f is primitive and $g\hat{h}$ is primitive. Then $a \mid b$ and $b \mid a \implies a, b \in R^*$ since $\gcd(a, b) = 1$. So f is irreducible in $R[x]$, a contradiction.

So we have shown that the irreducible polynomials in $K[x]$ are precisely the primitive irreducible polynomials in $R[x]$ times elements of K^*.

Then if $f, g \in R[x]$ are irreducible primitive then $f \in g \cdot (R[x])^*$ if and only if $f \in g \cdot (K[x])^*$, since if $f = g \cdot \frac{a}{b}, a, b \in R \setminus \{0\}$ coprime then $bf = ag \implies b \mid a, a \mid b$ so $\gcd(a, b) = 1 \implies a, b \in R^* \implies \frac{a}{b} \in R^*$.

Given any $f(x) \in R[x]$ which is not 0, if $f(x) \in R$ then the unique factorization of $f(x)$ in R is the unique factorization of $f(x)$ in $R[x]$.

If $\deg(f) > 0$ then $f(x) = c(f) \cdot \hat{f}(x)$ so there is a factorization of $f(x)$ in $R[x]$, obtained by appending factorizations of $c(f)$ and of $\hat{f}(x)$.

Conversely, any factorization of $f(x)$ must consists of (irreducibles with product $c(f)$) times some unit and (irreducible with product $\hat{f}(x)$).

The factorization of $c(f)$ is unique since R is UFD. And the factorization of $\hat{f}(x)$ is the unique factorization of $\hat{f}(x)$ in $K[x]$.

By above, the notions of uniqueness are the same, so $R[x]$ is a UFD. ■

Eisenstein's irreducibility criterion

Theorem (Eisenstein's irreducibility criterion)**.** *If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ and for some prime p,*

$$p \nmid a_n, p \mid a_{n-1}, \ldots, a_0, p^2 \nmid a_0 \text{ and } c(f) = 1.$$

Then $f(x)$ is irreducible in $\mathbb{Z}[x]$ and hence in $\mathbb{Q}[x]$.

Proof. $p : \mathbb{Z}[x] \to (\mathbb{Z}/(p))[x]$, $p(f) = a_n x^n \neq 0$. If $f = gh$ with $g, h \in \mathbb{Z}[x]$ nonconstant, then $\phi(f) = \phi(g)\phi(h)$ and $p \nmid a_n \implies \deg(\phi(g)) = \deg(g), \deg(\phi(h)) = \phi(h)$.

$\implies \phi(g) = bx^i, \phi(h) = dx^{n-i}, b, d \in (\mathbb{Z}/(p))^*, 0 < i < n \implies g \equiv bx^i \mod p, h \equiv dx^{n-i} \mod p$.

So $p \mid g(0), p \mid h(0) \implies p^2 \mid g(0), h(0) = a_0$, a contradiction. ■

Corollary. *$x^n - p$ is irreducible in $\mathbb{Q}[x]$, $\forall n > 0$ and every prime p.*

Next time: deduce that $x^{p-1} + x^{p-2} + \ldots + 1$ is irreducible in $Q[x]$ for prime p.