Theorem (F[x] is a UFD) If F is a field then the integral domain F[x] of polynomials with coeffs in F is a UFD (unique factorization domain).

But, of course, we have to define UFDs first. Let R be an i. domain. Recall that $a \in R$ is irreducible if $a \neq 0_R$, a is not a unit in R, and $a = bc$ for some $b, c \in R \Rightarrow$ b or c is a unit — a cannot be written as a product of two non-units. For example, in the i. domain of integers $\mathbb{Z}$ the irr. elements are exactly $\pm p$ where $p \in \mathbb{N}$ is a prime number.

Definition Two elements $a, b \in R$ in an i. domain are associated if $\exists \varepsilon \in R^*$ (i.e. ε is a unit of R): $a = b\varepsilon$.

Problem 18.1. Prove that this relation is an equivalence relation on R. When are two elements of $\mathbb{Z}$ associated?

Definition (of UFD) We say that an integral domain R is a UFD (unique factorization domain) if

1) Every $\neq 0_R$ and non-unit element $a \in R$ has an expression $a = \pi_1 \pi_2 \cdots \pi_k$ where $k \in \mathbb{N}$ and every π_i is irreducible (in R).

2) If $\pi_1 \pi_2 \cdots \pi_k = q_1 q_2 \cdots q_\ell$ where $k, \ell \in \mathbb{N}_0$ (for $k=0$ or $\ell=0$ we define the product as 1_R) and each element π_i and q_j is irreducible, then $k=\ell$ and there exists a permutation $f: [k] \to [k]$ ($[k] = \{1, 2, \ldots, k\}$) s.t. for every $i \in [k]$ the elements π_i and $q_{f(i)}$ are associated.

---

1) is the existence of factorizations in irr. elements and 2) is their uniqueness. This definition is a generalization of the basic fact of number theory that the i. domain of integers $\mathbb{Z}$ is a UFD. For example, $12 = 2 \cdot 3 \cdot 2 = (-3)(-2)2 = (-2) \cdot 3 \cdot (-2) = \cdots$ is the essentially (unique) factorization of the number 12 into primes.

Proof. (of the theorem that $F[x]$ is a UFD). I leave the first step as an exercise for you:

Problem 18.2. Prove that if F is a field then the i. domain $F[x]$ is a PID, i.e. every ideal in $F[x]$ is generated by a single element. ~~It suffices to prove more generally the~~ The next problem for you is an important tool in the i. domain $F[x]$.

Problem 18.3. Prove the division algorithm for $F[x]$: If $a, b \in F[x]$ and $b \neq 0_{F[x]}$ then there are polynomials $c, d \in F[x]$ s.t. $a = bc + d$ and $d = 0_{F[x]}$ or $\deg(d) < \deg(b)$.

If $0_{F[x]} \neq a = bc$ in $F[x]$ then $\deg(a) = \deg(b) + \deg(c)$.

From this we see: $a \in F[x] \setminus \{0_{F[x]}\}$ is a unit $\iff$ $\deg(a) = 0$, a is a constant polynomial. It follows by induction on degrees that every $\neq 0_{F[x]}$ and non-unit element in $F[x]$ is a product of irr. elements: take an $a \in F[x]$ s.t. $\deg(a) > 0$ and $\deg(a)$ is minimum so that a cannot be written as a product of irr. elements. Thus a is not irr., $a = bc$ for some $b, c \in F[x]$ s.t. $0 < \deg(b), \deg(c) < \deg(a)$.

But then both b and c are products of irr. elements and so is a, which is a $\lightning$. Thus we have proved condition 1) from the above definition. To prove condition 2) it suffices to prove: if $a,b,c \in F[x]$, a is irr. and a divides bc (i.e. $bc = ad$ for some $d \in F[x]$) then a divides b or a divides c. Indeed, then if $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_\ell$ for irr. elements a_i and b_i, then a_1 has to divide some b_{j_1}, $j_1 \in [\ell]$. But since a_1 and b_{j_1} are irr., it follows that a_1 and b_{j_1} are associated, $b_{j_1} = \varepsilon a_1$ for a unit ε. We cancel a_1:

$$\rightsquigarrow a_2 a_3 \cdots a_k = b_1 b_2 \cdots (\varepsilon b_{j_1}) \cdots b_\ell$$

(b_{j_1} - irr. element)

We continue cancelling elements in this way and see that $F[x]$ satisfies condition 2).

But it remains to prove ⌊ ⌋, i.e. If $a,b,c \in F[x]$, $a \mid bc$ and a is irr. then $a \mid b$ or $a \mid c$. So suppose that a is irr., a divides bc but a does not divide b. Consider

the ideal I generated by $\{a, b\}$, $I = \{ra + sb \mid r, s \in F[x]\}$. By problem 18.2, $I = (d) = \{rd \mid r \in F[x]\}$. As $a, b \in I$, d divides both a and b. Since a is irr. and $a \nmid b$, it follows that d is a unit, or $d = 1_{F[x]}$ and $I = F[x]$. Thus $1_{F[x]} \in I$ and $\boxed{1_{F[x]} = ra + sb}$ for some $r, s \in F[x]$. We multiply $\boxed{\cdots}$ by c and get that $c = rac + sbc$. But a divides both terms on the right side, hence a divides c.

$\boxtimes$

So now I am finally ~~done~~ to prove the prepared

Theorem (on finite fields) $\forall$ prime p and $\forall n \in \mathbb{N} \exists$ field F s.t. F has $|F| = p^n$ elements.

Proof: It is clear that if $\mathbb{Z}_p$ denotes the finite field with p elements, then it suffices to prove: $\forall n \in \mathbb{N} \exists$ irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ with $\deg(f) = n$. Indeed,

— continuation next time . . .