Math 122 Wednesday, November 30

Last time we constructed a field of p^2 elements $p>2$

$\mathbb{Z}/p\mathbb{Z}[x]/(x^2-a) \simeq \mathbb{Z}/p + \mathbb{Z}/p\cdot X$ is a ring with p^2 elements
This is a field if x^2-a is irreducible over $\mathbb{Z}/p\mathbb{Z}$ $\Leftrightarrow$ if there are no roots in $\mathbb{Z}/p\mathbb{Z}$ $\Leftrightarrow$ a is not a square in $\mathbb{Z}/p\mathbb{Z}$. But using the homomorphism $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ $b \mapsto b^2$ with kernel $= \{b \mid b^2 \equiv 1 \bmod p\} = \{b \mid p \mid (b-1)(b+1)\} = \langle \pm 1 \rangle$. So image has order $\frac{p-1}{2}$ so there are $\frac{p-1}{2}$ choices for a which are not a square.

What about $p=2$? x^2-a is always reducible but x^2+x+1 is not as it has no roots.
$F = \mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$ is a field with 4 elements.
$F = \{0, 1, x, 1+x\}$ $x(1+x) = x+x^2 \equiv 1$ so $1+x = x^{-1}$. $x^2 = 1+x$, $x^3 = 1$, $(1+x)^3 = 1$

Why can we always adjoin square roots for $p>2$? Because you can complete the square $x^2+bx+c = (x+\frac{b}{2})^2 + c - \frac{b^2}{4} = X^2 - a$ (note for $p>2$, 2^{-1} exists). But you can't divide by 2 over $\mathbb{Z}/2\mathbb{Z}$. Exercise: Why do you get the same field when you adjoin x to $\mathbb{Z}/p\mathbb{Z}$ satisfying x^2+bx+c as you do when you adjoin X satisfying $X^2 - (\frac{b^2}{4} - c)$.

Claim Let F be a finite field. Then there is a prime number p and an integer $n \geq 1$ such that $\#F = p^n$.
Pf: Let R be any ring. There is a natural homomorphism $f: \mathbb{Z} \to R$ given by $0 \mapsto 0_R$, $1 \mapsto 1_R$, $2 \mapsto 1_R + 1_R$, $n \mapsto 1_R + \cdots + 1_R$ (n times), $-1 \mapsto -1_R$ = additive inverse of 1_R, $-n \mapsto -1_R + \cdots + -1_R$ (n times) etc. $\ker f \subset \mathbb{Z}$ is an ideal so there are two possibilities.
Case 1: $\ker f = (0) \Rightarrow f: \mathbb{Z} \hookrightarrow R$ (ex $R = \mathbb{R}, \mathbb{C}, \mathbb{Q}$)
Case 2: $\ker f \neq (0) \Rightarrow \ker f = n\mathbb{Z}$ for some $n \geq 1$ ($\ker f = \mathbb{Z}$ iff $R = (0)$)
Here the image of f is a finite subring of R isomorphic to $\mathbb{Z}/n\mathbb{Z}$
If R is a field the $\ker f$ is either (0) or $p\mathbb{Z}$ for some prime p. If kernel is $n\mathbb{Z}$ and $n = a \cdot b$ $(a, b \neq n)$ then $f(a)\cdot f(b) = f(ab) = f(n) = 0$ but $f(a), f(b) \neq 0$. This can't happen in a field (so note at the end of this). If F is finite, we can't have $\ker f = (0)$ because the image is finite. So $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$. Since F is an abelian group with scalar multiplication from $\mathbb{Z}/p\mathbb{Z}$ it is a vector space over $\mathbb{Z}/p\mathbb{Z}$. Since F is finite it has a finite spanning set over $\mathbb{Z}/p\mathbb{Z}$. So $\dim_{\mathbb{Z}/p\mathbb{Z}}(F) = n \geq 1$. Hence $F \simeq (\mathbb{Z}/p\mathbb{Z})^n$ by choosing a basis so $\#F = p^n$.

$\mathbb{Z} \xrightarrow{f} F$
$\searrow \quad \nearrow$
$\mathbb{Z}/p\mathbb{Z}$

Thm (Galois) For every p and $n \geq 1$ there is a finite field of order p^n. Any two finite fields F and F' of the same order are isomorphic.

Note $F = \mathbb{Z}/p\mathbb{Z}[x]/(f(x))$ ($\leftarrow$ degree n, monic) = a finite ring with p^n elements $= \mathbb{Z}/p\mathbb{Z} + \cdots + \mathbb{Z}/p\mathbb{Z}\,x^{n-1}$
Can one find f of degree n irreducible over $\mathbb{Z}/p\mathbb{Z}$?

Not at all obvious. Note for $F = \mathbb{R}$ can not find any irreducible polys of degree ≥ 3.
for $F = \mathbb{C}$ can't find any of degree ≥ 2.

defn A zero divisor in R is an element $a \in R$, $a \neq 0$, such that $\exists\ b \in R, b \neq 0$, with $a \cdot b = 0_R$.

Note if $a \neq 0$ in a field then $a \cdot b = 0 \Rightarrow a^{-1} \cdot a \cdot b = 0 \Rightarrow b = 0$, so there are no zero divisors. Some rings have zero divisors and some do not.

defn A ring is called a domain (sometimes an integral domain) if it has no zero divisors.

ex. $F[x]$, $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ are domains (the last of course is a field)
non-ex. $\mathbb{Z}/ab\mathbb{Z}$ is not as we saw before $a \cdot b \equiv 0 \pmod n$
neither is $\mathbb{C}[x]/(x^n)$ for x is a zero divisor. In fact $x^n = 0$ so we say x is nilpotent.

Every integral domain is naturally a subring of a field (called the field of fractions of R)

$R \hookrightarrow F = \{ a/b : a, b \in R, b \neq 0 \}/\sim$ (set of symbols) Say $a/b \equiv a'/b'$ iff $ab' = a'b$ in R.

To check that this is an equivalence relation you need a cancelation property that is unique to a domain (need it for transitivity)

Claim In a domain if $ax = bx$ and $x \neq 0$ then $a = b$.
Pf: $ax = bx \Rightarrow (a-b)x = 0$. As $x \neq 0$, $a - b = 0$ as there are no zero divisors $\Rightarrow a = b$.

Remains to show that the set of equivalence classes of fractions a/b has the structure of a field with $R \hookrightarrow F$ an injective homomorphism $a \mapsto a/1$.
e.g. define $a/b + c/d = \frac{ad+bc}{bd}$ → nonzero because R a domain.
$a/b \cdot c/d = \frac{ac}{bd}$ Define $1 = \frac{b}{b}$, $0 = \frac{0}{a}$. Check $a/b = 0$ iff $a = 0$.
Also must show that these are well defined.

One field of fractions you may not have thought of as such: $\mathbb{C}(x)$ = rational functions in x over $\mathbb{C} = \{ \frac{p(x)}{q(x)} \mid p, q \in \mathbb{C}[x], q \neq 0 \}$ the field of fractions of $\mathbb{C}[x]$.