4/4/11

Recall:
F a field, a field E is called an <u>extension field</u> of F if F is a subfield of E.

Example from last time...
$F = \mathbb{Z}_3$
$E = \mathbb{Z}_3[i] = \{a+bi : a,b \in \mathbb{Z}_3\}$
operations
$$(a+bi)(c+di) = (ac-bd) \bmod 3 + i((ad+bc) \bmod 3) \in \mathbb{Z}_3[i]$$
$$(a+bi)+(c+di) = (a+c) \bmod 3 + i(b+d) \bmod 3$$
Check that every nonzero element is invertible:
$x = a+bi$, either a or b is nonzero
$$x^{-1} = \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi}$$
$$= \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + i\left(\frac{-b}{a^2+b^2}\right)$$ reduce coefficients mod 3
$$x^{-1} = \underbrace{(a(a^2+b^2)^{-1})}_{\text{mod } 3} + i\underbrace{((-b)(a^2+b^2)^{-1})}_{\text{mod } 3}$$
why is x^{-1} nonzero or even well-defined?
If $a^2+b^2 = 0 \bmod 3$, we have the following:
1. If $a=0$, then since $x \neq 0$, $b \neq 0$. Then $b = 1$ or 2. $1^2 = 1$ and $2^2 = 4 = 1 \bmod 3$, so $b^2 \neq 0$
2. If $a=1$, then b could be 0, 1 or 2.
$b=0$, $a^2+b^2 = 1$. $b=1$, $a^2+b^2 = 1+1 = 2$.
$b=2$, $a^2+b^2 = 1+4 = 2 \bmod 3$
3. If $a=2$, b could be 0, 1, or 2
$b=0$, $a^2+b^2 = 4 = 1 \bmod 3$
$b=1$, $a^2+b^2 = 4+1 = 5 = 2 \bmod 3$
$b=2$, $a^2+b^2 = 4+4 = 8 = 2 \bmod 3$

Hence $a^2+b^2 \neq 0$ $\forall$ choices of a and b with at least one of a or b nonzero →

Ex cont: So x^{-1} is well-defined. Is it possible for x^{-1} to ever be zero if $x \neq 0$?

If $b=0$, then $x \neq 0 \Rightarrow a \neq 0$, since $a^2+b^2 \neq 0$ and $\mathbb{Z}_3$ is a field, $a \cdot (a^2+b^2)^{-1} \neq 0$

Similarly, if $a=0$, $b \cdot (a^2+b^2)^{-1} \neq 0$

Hence every nonzero element of $\mathbb{Z}_3[i]$ has a multiplicative inverse.

Another Example:

$F = \mathbb{Q}$

$E = \mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$

Since $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$, we know

$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

and

$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a-c)+(b-d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$\forall\, a, b, c, d \in \mathbb{Q}$

Then $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$

Check that this is a field:

$$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

Note: $a^2-2b^2 = 0 \Rightarrow \frac{a}{b} = \sqrt{2}$ where $a, b \in \mathbb{Z}$, which is false since $\sqrt{2}$ is irrational.

Def: The characteristic of a field F is the smallest natural number n such that $nx := \underbrace{x + x + \cdots + x}_{n \text{ times}} = 0 \quad \forall\, x$ in F

If no such number exists, say F is characteristic 0.

Examples:

1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all characteristic 0
2) $\mathbb{Z}_p$ is characteristic p
3) $\mathbb{Z}_3[i]$ is characteristic 3
4) Field with 4 elements is characteristic 2

Thm: If F is a field with nonzero characteristic n, then n is prime.

Pf: Suppose F is characteristic n and that $k < n$, $k \neq 1$, k divides n ($k \in \mathbb{N}$). Take $x \in F$, suppose $kx \neq 0$. Then

$$nx = k \cdot mx = m(kx) = \underbrace{kx + kx + \cdots + kx}_{m \text{ times}}.$$

But $nx = 0$ $\forall x \in F$ since n is the characteristic of F. Hence

$$0 = \underbrace{kx + kx + \cdots + kx}_{m \text{ times}}$$

Since $kx \neq 0$ and F is a field, kx has a multiplicative inverse $(kx)^{-1}$. Take $0 = \underbrace{kx + kx + \cdots + kx}_{m \text{ times}}$ and multiply both sides by $(kx)^{-1}$. Then

$$0 = (kx)^{-1}(\underbrace{kx + kx + \cdots + kx}_{m \text{ times}})$$

$$= \underbrace{(kx)^{-1}(kx) + \cdots + (kx)^{-1}(kx)}_{m \text{ times}}$$

$$= 1 + 1 + \cdots + 1 = m \cdot 1$$

Then $\forall y \in F$, $my = (m \cdot 1)y = 0 \cdot y = 0$

This implies the characteristic of F is m.

But $n = mk$ and $k > 1$, so $m < n$, contradiction since n is the minimal number satisfying $ny = 0$ $\forall y \in F$. Then we must have n admits no proper nontrivial divisors, so n is prime $\blacksquare$

Corollary: let F be a field of characteristic $p \neq 0$. Then F has a subfield isomorphic (as a field) to $\mathbb{Z}_p$.

Pf: Consider $\{n 1_F : n \in \mathbb{N}\}$ Then this set is the desired subfield.

Isomorphism:

$\varphi_p : \mathbb{Z}_p \to F$

$\varphi_p(1) = 1_F$ ∎

$(\varphi_p(n) = n 1_F)$

Prop: Any characteristic 0, field F has a subfield isomorphic to $\mathbb{Q}$.

Pf: consider $\{(n 1_F) \cdot (m 1_F)^{-1} : n, m \in \mathbb{Z}, m \neq 0\}$

Define: $\varphi : \mathbb{Q} \to F$

$\varphi(\frac{n}{m}) = (n 1_F)(m 1_F)^{-1}$ ∎

NOTE the following field axiom:

$0 \neq 1$