<u>Last time</u> reviewed the notion of a vector space, bases, dimensions

<u>Proved</u> If F is a field, $f \in F[x]$ and $\deg f = n \geq 1$ then $F[x]/\langle f \rangle$ is a vector space over F with a basis

$$\mathcal{B} = \{ 1+\langle f \rangle, x+\langle f \rangle, \dots x^{n-1}+\langle f \rangle \}.$$

<u>Note</u> Let $\alpha = x+\langle f \rangle \in F[x]/\langle f \rangle$. For $\lambda \in F$ abbreviate $\lambda + \langle f \rangle \in F[x]/\langle f \rangle$ as λ. Then

$$\mathcal{B} = \{ 1, \alpha, \alpha^2, \dots \alpha^{n-1} \}.$$

<u>Recall</u> A map $T: V \to W$ between two vector spaces over F is <u>linear</u> if $\forall\, v_1, v_2 \in V$, $\lambda_1, \lambda_2 \in F$

$$T(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 T(v_1) + \lambda_2 T(v_2).$$

A linear map $T: V \to W$ is an <u>isomorphism</u> of vector spaces if $\exists$ linear map $S: W \to V$ which is the inverse of T:

$$S \circ T = \mathrm{id}_V, \quad T \circ S = \mathrm{id}_W.$$

<u>Exercise 1</u> A linear map $T: V \to W$ is an isomorphism $\iff$ T is a bijection

<u>Exercise 2</u> $\{v_1, \dots v_n\} \in V$ is a basis $\iff$ $T: F^n \to V$ $\quad T(c_1, \dots c_n) = \sum c_i v_i$ is an isomorphism.

<u>Application</u> Suppose F is a finite field, $f \in F[x]$, $\deg f = n$. Then $\{1, \alpha, \dots \alpha^{n-1}\}$ is a basis of $F[x]/\langle f \rangle$

$\Rightarrow T: F^n \to F[x]/\langle f \rangle \quad T(c_0, \dots c_{n-1}) = \sum_{i=0}^{n-1} c_i \alpha^i$ is an isomorphism $\Rightarrow$ $|F[x]/\langle f \rangle| = |F^n| = |F|^n$

<u>Aside</u> Characteristic of a ring.

Let R be a ring (with 1). Then $(R, +, 0)$ is an abelian group

$1_R \in R$ generates a subgroup $\langle 1 \rangle = \{ n 1_R \mid n \in \mathbb{Z} \}$ and
$\varphi : \mathbb{Z} \to R$, $\varphi(n) = n 1_R$ is a group homomorphism.

Definition If $\ker \varphi = \{0\}$ (ie. $\varphi : \mathbb{Z} \to \langle 1_R \rangle$ is an iso)
we say that R has characteristic 0 : $\operatorname{char} R = 0$
if $\ker \varphi = n\mathbb{Z}$ (and consequently $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \langle 1_R \rangle$ is
an isomorphism) we say that R has characteristic n
we write $\operatorname{char} R = n$.

Ex $R = \mathbb{Z}_6[x]$. $\langle [1] \rangle = \langle [0], [1], \ldots [5] \rangle \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$
$\operatorname{char}(\mathbb{Z}_6[x]) = 6$

Ex $\operatorname{char} \mathbb{Z} = 0$, $\operatorname{char} \mathbb{Q} = 0$, $\operatorname{char} \mathbb{R} = 0$.

Lemma 35.1 If R is an integral domain and $\operatorname{char} R \neq 0$
then $\operatorname{char} R$ is a prime.

Proof Note first that $\varphi : \mathbb{Z} \to \langle 1_R \rangle$, $\varphi(n) = n 1_R$
is a ring homomorphism. This is because
$\forall n, m \in \mathbb{N}$ $\varphi(n)\varphi(m) = (\underbrace{1_R + \cdots + 1_R}_{n})(\underbrace{1_R + \cdots + 1_R}_{m})$

$$= \underbrace{1 \cdot 1 + \cdots + 1 \cdot 1}_{n \cdot m} = \varphi(n \cdot m)$$

$\Rightarrow \bar{\varphi} : \mathbb{Z}/\ker\varphi \to \langle 1_R \rangle$ is an iso of rings.

Since $\langle 1_R \rangle \subseteq R$ is a subring and R has no
zero divisors, $\langle 1_R \rangle$ has no zero divisors.
$\Rightarrow$ $\mathbb{Z}/\ker\varphi$ has no zero divisors
$\Rightarrow$ $\mathbb{Z}/\ker\varphi = \mathbb{Z}_p$ where $p = \operatorname{char} R$ is prime.

$\square$

Corollary Let E be a finite field, $p = \text{char } E$ (nec. prime)
Then $|E| = p^n$ for some n.

Proof Since $\mathbb{Z}_p \cong \langle 1_E \rangle \subseteq E$ is a subring of E,
E is a vector space over $\langle 1_E \rangle \cong \mathbb{Z}_p$
Since E is finite, E is a finite dim v. space over $\mathbb{Z}_p$.
$\Rightarrow$ E is isomorphic to $(\mathbb{Z}_p)^n$ for some n.
$\Rightarrow$ $|E| = |(\mathbb{Z}_p)^n| = p^n$.

□

Definition Let F, L be two fields and $F \subseteq L$ is a subring
(or, more generally suppose we have an injective ring homomorphism $\varphi: F \to L$).
We say that F is a subfield of L
and L is a field extension of F.

Ex $\mathbb{Q}$ is a subfield of $\mathbb{R}$, $\mathbb{C}$ is an extension of $\mathbb{R}$.
$L = \mathbb{Z}_2[x] / \langle x^2 + x + 1 \rangle$ is an extension of $\mathbb{Z}_2$

Field extensions and roots of polynomials.

Suppose F is a field, $p(x) \in F[x]$ an irreducible polynomial with $\deg p \geq 2$.
Then $\nexists\, \alpha \in F$, s.t. $p(\alpha) = 0$.
If it did, $(x - \alpha) \mid p(x)$. $\Rightarrow$ p wouldn't be irreducible

On the other hand, since p is irreducible,
$E = F[x] / \langle p \rangle$ is a field and
$\varphi: F \to F[x] / \langle p \rangle$, $\varphi(a) = a + \langle p \rangle$

is an extension of F.

By suppressing φ, we have $F \subseteq E$, hence $F[x] \leq E[x]$.

<u>Claim</u> $p(x) \in E[x]$ has a root in E.

<u>Proof</u>

$p(x) = a_0 + a_1 x + \cdots + a_n x^n$ for some $a_0, \ldots a_n \in F$.

$\Rightarrow$ Let $\alpha = x + \langle p \rangle$. Then

$$p(\alpha) = a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_n \alpha^n$$
$$= a_0 + \langle p \rangle + a_1 (x + \langle p \rangle) + a_2 (x + \langle p \rangle)^2 + \cdots + a_n (x + \langle p \rangle)^n$$
$$= (a_0 + a_1 x + \cdots + a_n x^n) + \langle p \rangle = p + \langle p \rangle = 0 + \langle p \rangle.$$

$\therefore$ $\alpha = x + \langle p \rangle$ is a root of $p(x) \in E[x]$.

<u>Ex</u> $F = \mathbb{R}$, $p(x) = x^2 + 1$

$\alpha = x + \langle x^2 + 1 \rangle \in \mathbb{R}[x] / \langle x^2 + 1 \rangle \simeq \mathbb{C}$ is a root of $x^2 + 1$:

$\alpha^2 + 1 = 0$ So α "is" $\sqrt{-1}$.

<u>Ex</u> $F = \mathbb{Q}$ $p(x) = x^2 - 2$,

$\alpha = x + \langle x^2 - 2 \rangle \in \mathbb{Q}[x] / \langle x^2 - 2 \rangle$ is a root of $x^2 - 2$!

$\alpha^2 - 2 = 0$. So α "is" $\sqrt{2}$ in $E = \mathbb{Q}[x] / \langle x^2 - 2 \rangle$.