lect 8
MA, Fall 2020

Theorem Let $f \in F[x]$, F a field.

Then $F[x]/(f)$ is a field iff f is irreducible.

Suppose f is irreducible, let $E = F[\alpha]/(f(\alpha))$ ← a larger field $F \subset E$

↑ use a new variable, not x any other variable is fine $(t, y, \beta \ldots)$

$f(x) = a_n x^n + \ldots + a_0$

view $f(x)$ as a polynomial in $E[x]$

$f(x)$ has root in E.

$f(\alpha) = a_n \alpha^n + \ldots + a_0 = 0$ in E. $\quad x - \alpha \mid f(x)$ over E

Use f twice: to build a field, and to have $f(x) \in F[x] \subset E[x]$ ↑ enlarge possible coefficients from F to E

$f(x)$ irreducible over F ⇒ contains both α and x

$F \longrightarrow F[x] \longrightarrow E[x]$

α is a constant in E

x is a polyn. of degree 1 in E

$F[\alpha] \longrightarrow E = F[\alpha]/(f(\alpha))$ enlarge our field of constants from E to F.

Example: $f(x) = x^2 + 1$ is irreducible in $\mathbb{R}$.

$E = \mathbb{R}[\alpha]/(\alpha^2+1)$ a field, α is a root of x^2+1 in E

$x^2 + 1 = (x - \alpha)(x + \alpha)$

usually denote α by i, E by $\mathbb{C}$

$\mathbb{C} = \mathbb{R}[i]/(i^2+1)$ $\qquad x^2 + 1 = (x+i)(x-i)$

Example $\mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$ is a field, $\mathbb{F}_4$

x^2+x+1 is irreducible over $\mathbb{F}_2$ (low degree, no roots)

$\mathbb{F}_4$

irreducible polynomial over $\mathbb{F}_2$ $\quad x^2+x+1$ $\longrightarrow$ relabel x to α $\longrightarrow$ $\alpha^2+\alpha+1$ $\longrightarrow$ $\mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$

$0, 1, \alpha, \alpha+1$

$\alpha^2 = \alpha+1 \pmod 2$

$x^2+x+1 = (x+\alpha)(x+\alpha+1)$ over $\mathbb{F}_4$

2 roots $\alpha, \alpha+1$ in $\mathbb{F}_4$

no roots in $\mathbb{F}_2$

Use different variables x, α or x, y, etc. to avoid confusion

Theorem Let $f \in F[x]$ be a nonconstant polynomial. There exists a field E containing F such that f has a root in E.

Proof Take an irreducible factor $p(x) \mid f(x)$.

$E = F[\alpha]/(p(\alpha))$ is a field, $E \supset F$.

α is a root of $p(x)$ and a root of $f(x)$ in E. (unless $\deg p = 1$) in E, not in F.

$x-\alpha \mid p(x)$, $x-\alpha \mid f(x)$.

$f(x) = (x-\alpha)g(x)$ in E

$g(x)$ has coefficients in E, not in F

Theorem Let $f \in F[x]$ be a nonconstant polynomial. There exists a field E containing F such that f factors into linear factors in E,

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

$c \in F^*$ $\quad \alpha_i \in E$, E a field.

Proof Induction on $\deg f$.

1) $\deg f = 1$ f linear already factors in F

2) Induction step $n-1 \longmapsto n$.

$\deg f = n$. $\exists$ field $E_1 \supset F$, such that $x - \alpha_1 \mid f(x)$ for some $\alpha_1 \in E$

(use E and α in last proof).

$f(x) = (x-\alpha_1) g(x)$ $\deg g = n-1$

Apply induction step to $g(x)$ and E_1 (instead of F)

$\exists$ field $E \supset E_1$ where $g(x)$ factors into linear terms.

In E, f factors

$$g(x) = c(x-\alpha_2)\ldots(x-\alpha_n).$$

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$$

$F \subset E$ field extension

$F \subset R$, $F \subset F[x]$, $F \subset F[x]/(f(x))$, f not necessarily irreducible

other rings that contain F as a subring

Part of structure is R is an abelian group under addition,

can multiply by elements of F.

F acts as scalars.

<u>Definition</u> An F-vector space (or vector space over F) is a triple $(V, +, \cdot)$, where $(V, +)$ is an abelian group (vectors under addition), and $\cdot$ is a map $F \times V \longrightarrow V$ (scalar multiplication) $(a, v) \longmapsto av$ (or $a \cdot v$) such that

1) for $a, b \in F, v \in V$ $a(bv) = (ab)v$

2) for $a, b \in F, v \in V$ $(a+b)v = av + bv$

3) $a \in F$, $v, w \in V$ $a(v+w) = av + aw$

4) $1 \cdot v = v$ $\forall v \in V$

<u>Examples</u>: 1) Column vectors F^n, $v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ $av = \begin{pmatrix} aa_1 \\ \vdots \\ aa_n \end{pmatrix}$

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{pmatrix}$$

2) 0 vector space $V = \{0\}$

Axioms imply $0v = 0$ $\forall v \in V$, $(-1)v = -v$ $\forall v \in V$

A vector subspace $W \subset V$: a subgroup W of $(V, +)$ closed under multiplication by elements of F

$aw \in W$ for $a \in F, w \in W$

$S \subset V$. A subset S of V is called <u>linearly independent</u>
if for $\forall s_1 \ldots s_n \in S$, distinct, $\forall a_1 \ldots a_n \in F$

$$a_1 s_1 + a_2 s_2 \ldots + a_n s_n = 0 \Rightarrow a_1 = a_2 \ldots = a_n = 0$$

no linear relations on elements of S, except $0s_1 + 0s_2 \ldots + 0s_n = 0$.
(Make sense for infinite S as well).
A basis $B \subset V$ is a linearly independent set such that any element of V is a linear combination of elements of B. Such linear combination is then unique, since B is linearly independent.

Example $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, $e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ is a basis of F^n

<u>Dimension</u> of V is the cardinality of a basis B of V

<u>Thm</u> Dimension of a vector space is well-defined

V finite-dimensional when it has a finite basis.

All bases of V have the same cardinality (proof the same as over $\mathbb{R}$ or $\mathbb{C}$).

$\dim V$ or $\dim_F V$ $\qquad \dim_F F^n = n$

Some linear algebra theorems generalize directly to all fields, some (especially those about eigenvalues and eigenvectors) depend on a field.

$F \subset F[x]$

Prop $F[x]$ is a vector space over F with a basis $\{1, x, x^2, x^3, \ldots\}$

Proof Any element of $F[x]$ has a unique presentation

$$f(x) = a_0 + a_1 x + \quad + a_n x^n \qquad \text{for some } n, a_0, \ldots a_n$$

□

Let f be a polynomial of degree n

Prop $F[x]/(f)$ is an F-vector space with a basis $\{1, x, \ldots x^{n-1}\}$.

Proof elements of $F[x]/(f)$ are cosets.

$r + (f)$ $\deg r < \deg f$ r unique such representative of a coset

$r = b_0 + b_1 x + \quad + b_{n-1} x^{n-1}$ unique presentation.
Some b_i's may be 0.

Can add elements of $F[x]/(f)$, multiply by elements of F.

$\Rightarrow \{1, x, \ldots x^{n-1}\}$ is a basis of this vector space

Can encode r by its coefficients $(b_0, b_1, \ldots, b_{n-1})$ □.

Special case: f is irreducible, $E = F[x]/(f)$ is a field

E is an F-vector space of dimension $\deg f$, with basis

$\{1, x, x^2, \ldots x^{n-1}\}$

often use a different variable, $E = F[\alpha]/(f(\alpha))$, basis

$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

$F \subset E$ field extension $\Rightarrow$ E is an F-vector space

Extension is called <u>finite</u> if E is finite-dimensional / F

<u>infinite</u> if E is infinite-dimensional / F.

Dimension of E as F-vect space is called the <u>degree</u> of the extension

$[E:F]$ notation $\quad [E:F] = \dim_F E$

<u>Examples</u>

1) $E = F \quad [F:F] = 1$ extension of degree 1.

2) $\mathbb{R} \subset \mathbb{C}$ basis $\{1, i\}$ $\{a+bi \mid a,b \in \mathbb{R}\}$. $\mathbb{C} \simeq \mathbb{R}[i]/(i^2+1)$

3) $\mathbb{Q} \subset \mathbb{R}$ infinite extension ($\mathbb{Q}$ is countable, $\mathbb{R}$ is uncountable)

4) $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ $\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ basis of $\mathbb{Q}[\sqrt{2}]$ is $(1, \sqrt{2})$.

$[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}] = 2$.

5) $F \subset F[x] \subset F(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in F[x] + \text{equiv. relation} \right\}$

rational functions in x with coefficients in F

$F \subset F(x)$ infinite degree

6) $\mathbb{F}_2 \subset \mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2+1+\alpha)$ $(1, \alpha)$ basis $[\mathbb{F}_4 : \mathbb{F}_2] = 2$

7) $\mathbb{F}_2 \subset \mathbb{F}_8 = \mathbb{F}_2[\beta]/(\beta^3+\beta+1)$ $(1, \beta, \beta^2)$ basis $[\mathbb{F}_8 : \mathbb{F}_2] = 3$.

Prop A finite field E has order p^n for some prime p and $n \geq 1$.

Proof E has characteristic p, for some prime p (Char 0 fields are infinite).

$\mathbb{F}_p \subset E$. E is a vector space $/\mathbb{F}_p$, finite-dimensional. $\Rightarrow$

$\exists$ a basis $(e_1 .. e_n)$ of $E/\mathbb{F}_p$.

Then an element of E has a unique presentation $a_1 e_1 + a_2 e_2 + \dots + a_n e_n$

$a_1, a_2 \dots a_n \in \mathbb{F}_p$ p choices for each $a_1 \dots a_n$.

$\Rightarrow |E| = p^n$.

Theorem For each prime p and $n \geq 1$ there exists a unique, up to isomorphism, field $\mathbb{F}_{p^n}$ with p^n elements.

(will prove soon) $q = p^n$ notation.

$\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9 = \mathbb{F}_3[\alpha]/(\alpha^2+1)$

↑ use any irreducible deg 2 polynomial

Note $\mathbb{F}_4 \not\subset \mathbb{F}_8$ not a subfield. 8 is not a power of 4.

$\mathbb{F}_q^*$ - cyclic group of order $q-1$ $\quad |\mathbb{F}_q^*| = q-1$

Another reason: if $\mathbb{F}_4 \subset \mathbb{F}_8$, $(\mathbb{F}_4^*) \subset \mathbb{F}_8^*$ subgroup

order 3 7

$\mathbb{F}_p \subset R$ commutative ring of characteristic p

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p \qquad a, b \in R$$

Prop $p \mid \binom{p}{i}$ for $i = 1, 2, \ldots p-1$.

p - prime, does not cancel out from the numerator

Hint: $\binom{p}{i} = \dfrac{p(p-1)\ldots 2 \cdot 1}{i(i-1)\ldots 1\,(p-i)(p-i-1)\ldots 1} \in \mathbb{Z}$

$\Rightarrow \binom{p}{i} = 0 \bmod p$, $\binom{p}{i} = 0$ in $\mathbb{F}_p$ $\qquad i = 1, 2, \ldots p-1$.

Corollary $(a+b)^p = a^p + b^p$ for $a, b \in R$ as above.

$p = 2$ $\quad (a+b)^2 = a^2 + b^2$

Note $(a+b)^4 = \left((a+b)^2\right)^2 = \left(a^2+b^2\right)^2 = a^4 + b^4$. Can iterate

$$(a+b)^{2^n} = a^{2^n} + b^{2^n}.$$

Exercise $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ for $a, b \in R$, $\mathbb{F}_p \subset R$, $n \geq 1$.

this means $p \mid \binom{p^n}{i}$ $\quad i = 1, 2, \ldots p^n - 1$ $\quad \binom{p^n}{i} = 0 \bmod p$.

also $(ab)^p = a^p b^p$. $\quad 1^p = 1$.

$a \mapsto a^p$ is an additive operation

Corollary The map $a \mapsto a^p$ for $a \in R$, $\mathbb{F}_p \subset R$ (R a commutative ring)

is a ring homomorphism $R \to R$ (endomorphism is a homomorphism from an object to itself)

Called **Frobenius endomorphism**

$\mathrm{Fr}(a) = a^p$ $\quad \mathrm{Fr}: R \to R$

Fr respects addition, multiplication $\mathrm{Fr}(1) = 1$, $\mathrm{Fr}(0) = 0$.

Example $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$ $\quad Fr(a) = a^2$

$0 \longmapsto 0 \qquad \alpha \longmapsto \alpha^2 = \alpha+1$

$1 \longmapsto 1 \qquad \alpha+1 \longmapsto (\alpha+1)^2 = \alpha^2+1 = \alpha$

Exercise work out Fr action on $\mathbb{F}_8 \simeq \mathbb{F}_2[\alpha]/(\alpha^3+\alpha+1)$.

$\mathbb{F}_p$, $\mathbb{F}_p^* \simeq C_{p-1}$ cyclic group of order $p-1$ $\Rightarrow a^{p-1} = 1 \quad \forall a \in \mathbb{F}_p^*$
(Fermat's Little Theorem)

$\Rightarrow a^p = a \quad \forall a \in \mathbb{F}_p$ (add 0).

$\Rightarrow$ Polynomial $f(x) = x^p - x$ has p distinct roots in $\mathbb{F}_p$. $\Rightarrow$ factors

$x^p - x = x(x-1)(x-2)\ldots(x-(p-1))$ $\qquad x-a \mid x^p - x \quad \forall a \in \mathbb{F}_p$

$x^{p-1} - 1 = (x-1)(x-2)\ldots(x-(p-1))$

$p=3$ $\quad x^3 - x = x(x-1)(x-2)$ in $\mathbb{F}_3$ $\qquad p=5$ $\quad x^5 - x = x(x-1)(x-2)(x-3)(x-4)$ in $\mathbb{F}_5$

in $\mathbb{F}_4$ $\quad x^4 - x = x(x+1)(x+\alpha)(x+\alpha+1)$. use all elements of $\mathbb{F}_4$

$\mathbb{F}_4^* \simeq C_3$ $\Rightarrow$ roots of $x^3 - 1$.
add 0 $\quad x^4 - x$.

If $F \supset \mathbb{F}_p$, F has order $q = p^n$ (F is an $\mathbb{F}_p$-vect space of dim n)

$F^* \simeq C_{q-1}$ $\Rightarrow \forall a \in F^* \quad a^{q-1} = 1$ in F. $\Rightarrow a$ is a root of $x^{q-1} - 1$ in F

add 0 element $\Rightarrow \forall a \in F$ is a root of $x^q - x$

$\uparrow$
degree q.

We proved there exists a finite extension $\mathbb{F}_p \subset E$ such that $x^q - x$ factors in E.

Let $F = \{a \in E \mid a^q = a\}$. subset of all roots of $x^q - x$

Prop $F \subset E$ is a subfield.

Proof $a, b \in F$ $(a^p = a,\ b^p = b) \Rightarrow (a+b)^p = a^p + b^p = a+b$ $(ab)^p = a^p b^p = ab$ are in F.

$-a = \underbrace{a + a \cdots + a}_{p-1 \text{ times}}$

$\Rightarrow F$ is a subring of E

If $a \in F$, $a \neq 0 \Rightarrow (a^{-1})^p = a^{-p} = (a^p)^{-1} = a^{-1} \Rightarrow a^{-1} \in F$.

$\Rightarrow F$ is a subfield of E.

F consists of all roots of $x^q - x$ in E and $x^q - x$ factors into linear terms in E (and in F). $\deg(x^q - x) = q$

To check that $|F| = q$ need to show that $x^q - x$ has no repeat roots.

A polynomial $f(x)$ has a repeat root (multiple root) α if

$(x-\alpha)^2 \mid f(x)$ $\qquad f(x) = (x-\alpha)^2 g(x)$.

If f has a repeat root, (first over $\mathbb{R}$ or $\mathbb{C}$)

$f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha) g(x) = (x-\alpha)\left((x-\alpha)g'(x) + 2g(x)\right)$.

$\Rightarrow x - \alpha \mid f'(x)$. , $x - \alpha \mid f(x) \Rightarrow x - \alpha \mid \gcd(f(x), f'(x))$.

$f(x)$ has a multiple root $\Rightarrow \gcd(f(x), f'(x)) \neq 1$.

This works over any F. $(x^n)' = n x^{n-1}$, $n \in F$.

$(a_n x^n + \cdots + a_0)' = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$,

$(x^q)' = q x^{q-1} = 0$ $\quad (x^q - x)' = -1$ $\quad \gcd(x^q - x, -1) = 1 \Rightarrow$ all roots of $x^q - x$ are distinct