Definition

① A field K is <u>algebraically closed</u> if any nonconstant polynomial $f(x) \in K[x]$ has a root in K (i.e. $f(k)=0$ for some $k \in K$). (equivalently splits into linear factors in $K[x]$)

② An extension L/K is an <u>algebraic closure</u> of K if
(i) Every $f \in K[x]$ splits into linear factors in $L[x]$
(ii) L is algebraic over K.

Example: $\mathbb{C}$ algebraically closed.

Lemma: (1) If $\overline{K}/K$ is an algebraic closure then $\overline{K}$ is algebraically closed.

(2) If L/K is any extension such that L is algebraically closed, then

$$\overline{K} := \{ \ell \in L \mid \ell \text{ is algebraic over } K \}.$$

is an algebraic closure of K.

Proof: (2) last time, (1) exercise for you.

Hint: If $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \overline{K}[x]$ then $K(a_0, a_1, \dots, a_n)$ is finite over K.

Example: $\overline{\mathbb{Q}} = \{ z \in \mathbb{C} \mid z \text{ is algebraic} / \mathbb{Q} \}$ is an algebraic closure of $\mathbb{Q}$. (Lemma-(2) + $\mathbb{C}$ algebraically closed).

Theorem: If K is a field then there exists an algebraic closure $\overline{K}/K$ and it is unique up to isomorphism.

E.g. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$
so is $\mathbb{R}[x]/x^2+1$

$$\mathbb{R}[x]/x^2+1 \underset{x \mapsto -i}{\overset{x\mapsto i}{\underset{\sim}{\overset{\sim}{\rightrightarrows}}}} \mathbb{C}$$

Proof: (of existence): By lemma, suffices to produce <u>any</u> algebraically closed field L containing K.

$S =$ set of irreducible polynomials $/K$.

$$R = K[x_f \mid f \in S] / (f(x_f) \mid f \in S)$$

$\hookleftarrow$ ring containing a root of f for every $f \in S$.

Take a maximal ideal m of R $\leftarrow$ Zorn's lemma.

$K_1 = R/m$ is now a field containing K with a root of all irreducibles.

Need R to not be the zero ring.

i.e. need $(f(x_f) \mid f \in S) \neq K[x_f \mid f \in S]$.

Exercise: Show this. Hint: if not $1 = \sum_{i \in I} a_i f_{S_i}(x_{f_i})$ only uses finitely many variables.

K_1 contains a root of every irreducible in $K[x]$.

Do the same thing to K_1 to get K_2.

. Keep going

$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n \subseteq \dots$

Easy to see: If $f(x) \in K[x]$ of degree n
then it splits completely in K_{n-1}.

$$L = \bigcup_{i=0}^{\infty} K_i = \operatorname{colim}_{i \in I} K_i.$$

is an algebraically closed field.

if $f \in L[x]$ coefficients all contained in K_i for $i \gg 0$

$f \in K_i[x] \Rightarrow f$ has a root in $K_{i+1} \subseteq L$.

Terminology: splitting fields are unique only up to isomorphism. But if you fix an algebraic closure $\overline{K}/K$ (or any algebraically closed L/K).
then for any $f(x) \in K[x]$ there is a unique splitting field of f inside $\overline{K}$.

$$= K(\alpha_1, \dots, \alpha_n)$$

where $\alpha_i \in \overline{K}$ are the roots of f.

Finite Fields $\mathbb{F}$ is finite if $|\mathbb{F}| < \infty$

$\Rightarrow |\mathbb{F}| = p^n$

p is characteristic of $\mathbb{F}$.

Any finite field $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$

$$|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]}.$$

Exercise: Construct a field with 4 elements (i.e. $|\mathbb{F}|=4$).

$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}.$

$$\mathbb{F}_4 = \mathbb{F}_2[x]/x^2+x+1 \quad \checkmark$$

x^2+x+1 is irreducible over $\mathbb{F}_2$

$$[\mathbb{F}_4 : \mathbb{F}_2] = 2$$

So $|\mathbb{F}_4| = 2^2 = 4.$

Lemma: If $\mathbb{F}$ is a finite field then $\mathbb{F}^\times$ ($= \mathbb{F}\setminus\{0\}$, group law is multiplication) is cyclic of order $|\mathbb{F}|-1$.

Proof: Recall: If A is a finite abelian group with at most n elements of order n for every n then A is cyclic.

If $a \in \mathbb{F}^\times$ s.t. $a^n = 1$ then a is a root of $x^n - 1 \in \mathbb{F}[x]$.

degree n so it has at most n roots

in $\mathbb{F}$.

Theorem: $[\mathbb{F}:\mathbb{F}_p]=d$ if and only if $\mathbb{F}$ is a splitting field for $x^{p^d}-x$ $\left(=(x^{p^d-1}-1)x\right)$.

In particular, for every prime power p^d there exists a field of order p^d and it is unique up to isomorphism.

Proof: If $[\mathbb{F}:\mathbb{F}_p]=d$ then

$\mathbb{F}^\times$ has size p^d-1

so every element is a root of

$$x^{p^d-1}-1=0$$

$$x^{p^d}-x=(x^{p^d-1}-1)x=\prod_{\alpha\in\mathbb{F}}(x-\alpha)$$

So $\mathbb{F}=\mathbb{F}_p(\alpha \mid f(\alpha)=0)=\mathbb{F}_p(\alpha \mid \alpha\in\mathbb{F})$.

$\mathbb{F}$ is a splitting field. ✓ one direction.

Conversely: If $\mathbb{F}$ is a splitting field for $x^{p^d}-x$.

Note: Then roots of $x^{p^d}-x$ are unique.

$$(x^{p^d}-x)'=-1$$

So then $[\mathbb{F}:\mathbb{F}_p]\geq d$.

Claim: subfield of order p^d

Come back to next time.