# MAU34101 Galois theory

# 1 - More on field extensions

Nicolas Mascot
mascotn@tcd.ie
Module web page

Michaelmas 2021–2022
Version: October 2, 2023

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

# Reminders on algebraic extensions

# Reminders

Let $K \subset L$ be a field extension, and let $\alpha \in L$.
Write $K[\alpha] = \{F(\alpha) \mid F(x) \in K[x]\}$ for the subring generated by $K$ and $\alpha$, and $K(\alpha)$ for the subfield generated by $K$ and $\alpha$.

$I_\alpha = \{F(x) \in K[x] \mid F(\alpha) = 0\}$ is an ideal of $K[x]$. We say that $\alpha$ is algebraic over $K$ if $I_\alpha \neq \{0\}$; as $K[x]$ is a PID, we then have $I_\alpha = (P(x))$ for a unique monic $P(x) \in K[x]$, the minimal polynomial of $\alpha$, which is irreducible over $K$.

Besides, we then have

$$K[\alpha] = K(\alpha) = \bigoplus_{j=0}^{d-1} K\alpha^j \quad (d = \deg P),$$

so $[K(\alpha) : K] = d$.
Indeed, let $0 \neq F(\alpha) \in K[\alpha]$; then $F(x)$ and $P(x)$ are coprime, so (Bézout) there exist $U(x), V(x) \in K[x]$ such that $U(x)F(x) + V(x)P(x) = 1$, so $1/F(\alpha) = U(\alpha) \in K[\alpha]$.

# Stem fields, splitting fields

# Stem fields, splitting fields

Let $K$ be a field.

**Definition (Stem field)**

*Let $P(x) \in K[x]$ irreducible. A stem field of $P$ over $K$ is an extension $K \subseteq L$ containing a root $\alpha \in L$ of $P(x)$ and such that $L = K(\alpha)$ (minimality).*

**Definition (Splitting field)**

*Let $F(x) \in K[x]$. A splitting field of $F$ over $K$ is an extension $K \subseteq L$ containing $\alpha_1, \cdots, \alpha_d$ such that $F(x) = \prod_{j=1}^{d}(x - \alpha_j)$ and such that $L = K(\alpha_1, \cdots, \alpha_d)$ (minimality).*

# Stem fields, splitting fields

## Definition (Stem field)

*Let $P(x) \in K[x]$ irreducible. A stem field of $P$ over $K$ is an extension $K \subseteq L$ containing a root $\alpha \in L$ of $P(x)$ and such that $L = K(\alpha)$ (minimality).*

## Definition (Splitting field)

*Let $F(x) \in K[x]$. A splitting field of $F$ over $K$ is an extension $K \subseteq L$ containing $\alpha_1, \cdots, \alpha_d$ such that $F(x) = \prod_{j=1}^{d}(x - \alpha_j)$ and such that $L = K(\alpha_1, \cdots, \alpha_d)$ (minimality).*

## Example

Let $K = \mathbb{Q}$ and $P(x) = x^3 - 2$, whose roots in $\mathbb{C}$ are $\alpha = \sqrt[3]{2}$, $\beta = \zeta\sqrt[3]{2}$, and $\gamma = \zeta^2\sqrt[3]{2}$, where $\zeta = e^{2\pi i/3}$ (so $\zeta^3 = 1$).
Then $\mathbb{Q}(\alpha)$ is a stem field of $P(x)$ over $\mathbb{Q}$, but not a splitting field, e.g. because $\mathbb{Q}(\alpha) \subset \mathbb{R}$ whereas $\beta, \gamma \notin \mathbb{R}$.
A splitting field of $P(x)$ is $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt[3]{2}, \zeta)$.

# Stem fields, splitting fields

Let $K$ be a field.

**Definition (Stem field)**

*Let $P(x) \in K[x]$ irreducible. A stem field of $P$ over $K$ is an extension $K \subseteq L$ containing a root $\alpha \in L$ of $P(x)$ and such that $L = K(\alpha)$ (minimality).*

**Definition (Splitting field)**

*Let $F(x) \in K[x]$. A splitting field of $F$ over $K$ is an extension $K \subseteq L$ containing $\alpha_1, \cdots, \alpha_d$ such that $F(x) = \prod_{j=1}^{d}(x - \alpha_j)$ and such that $L = K(\alpha_1, \cdots, \alpha_d)$ (minimality).*

Existence? Uniqueness?

# Stem fields: existence

**Theorem**

*Let $P(x) \in K[x]$ irreducible. Then $L = K[x]/\big(P(x)\big)$ is a stem field of $P$ over $K$.*

**Proof.**

$L$ is a field: Let $0 \neq \overline{F(x)} \in L$. Then $P(x) \nmid F(x)$, so they are coprime, so there are $U, V \in K[x]$ such that $UF + VP = 1$. Then $\overline{U(x)}$ is an inverse of $\overline{F(x)}$.

Extension of $K$: if $k \neq k' \in K$, then $\overline{k} \neq \overline{k'} \in L$.

Stem field: let $\alpha = \overline{x} \in L$. Then $P(\alpha) = \overline{P(x)} = 0 \in L$, and clearly $L = K(\alpha)$. □

**Remark**

The quotient ring $K[x]/\big(F(x)\big)$ is a field iff. $F(x)$ is irreducible over $K$ (compare with $\mathbb{Z}/n\mathbb{Z}$).

# $K$-morphisms

## Definition

*Let $K$ be a field, and let $K \subset L$, $K \subset M$ be extensions of $K$.*
*A $K$-morphism from $L$ to $M$ is a morphism $f : L \longrightarrow M$ such that $f_{|K} = \mathrm{Id}_K$, i.e. $f(k) = k$ for all $k \in K$.*
*Notation: $\mathrm{Hom}_K(L, M)$.*
*Similarly define $K$-isomorphisms and $K$-automorphisms.*

## Remark

Ring morphisms between fields are always injective, and always respect inverses: $f(l)f(l^{-1}) = f(ll^{-1}) = 1$.

## Remark

$\mathrm{Aut}_K(L)$ is a subgroup of $\mathrm{Aut}(L)$.

# Stem fields: uniqueness

## Theorem

*Let $P(x) \in K[x]$ irreducible. Stem fields of $P(x)$ over $K$ are unique up to $K$-isomorphism.*

## Proof.

Let $L = K(\alpha)$ be a stem field of $P$, where $P(\alpha) = 0$. The isomorphism theorem applied to

$$\begin{array}{rcl} \operatorname{ev}_\alpha : K[x] & \longrightarrow & L \\ F(x) & \longmapsto & F(\alpha) \end{array}$$

yields $K[x]/\operatorname{Ker}\operatorname{ev}_\alpha \simeq \operatorname{Im}\operatorname{ev}_\alpha$.
But $\operatorname{Ker}\operatorname{ev}_\alpha = I_\alpha = \big(P(x)\big)$, and $\operatorname{Im}\operatorname{ev}_\alpha = K[\alpha] = K(\alpha) = L$ by minimality. □

# Stem fields: uniqueness

**Theorem**

*Let $P(x) \in K[x]$ irreducible. Stem fields of $P(x)$ over $K$ are unique up to $K$-isomorphism.*

**Example**

Let $K = \mathbb{Q}$, $P(x) = x^3 - 2$, $\alpha = \sqrt[3]{2}$, $\beta = \zeta\sqrt[3]{2}$, and $\gamma = \zeta^2\sqrt[3]{2}$ ($\zeta = e^{2\pi i/3}$). Then

$$\mathbb{Q}[x]/(x^3 - 2) \simeq_{\mathbb{Q}} \mathbb{Q}(\alpha) \simeq_{\mathbb{Q}} \mathbb{Q}(\beta) \simeq_{\mathbb{Q}} \mathbb{Q}(\gamma).$$

**Example**

Let $K = \mathbb{R}$, $P(x) = x^2 + 1$. Then

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

# Splitting fields: existence

**Theorem**

*Let $F(x) \in K[x]$. A splitting field of $F(x)$ over $K$ exists.*

**Proof.**

If $F(x)$ already splits into linear factors over $K$, we are done. Else, take an irreducible factor $P(x)$ of degree $\geq 2$ of $F(x)$, and start over with $L = K[x]/\big(P(x)\big)$ instead of $K$ and $F(x)/(x - \alpha)$ instead of $F(x)$, where $\alpha = \overline{x} \in L$. □

# Splitting fields: existence

## Example (Splitting field of $x^3 - 2$ over $\mathbb{Q}$)

Take $K = \mathbb{Q}$, $F(x) = x^3 - 2$ over $\mathbb{Q}$.
Since $F(x)$ is irreducible over $K$, first enlarge $K$ into $L = K[x]/(x^3 - 2) = K(\alpha)$, where $\alpha = \overline{x} \in L$.
We compute $F(y)/(y - \alpha) = y^2 + \alpha y + \alpha^2$
$\rightsquigarrow$ factorisation $F(y) = (y - \alpha)(y^2 + \alpha y + \alpha^2)$ over $L$.
Two alternatives: If $y^2 + \alpha y + \alpha^2$ splits over $L$, then $L$ is a splitting field of $F$, so done; else, must further enlarge $L$.
Actually, $y^2 + \alpha y + \alpha^2$ is irreducible over $L$ because $\Delta = -3\alpha^2$ is not a square in $L$ (embed in $\mathbb{R}$),
$\rightsquigarrow$ $M = L[y]/(y^2 + \alpha y + \alpha^2)$. Then $y^2 + \alpha y + \alpha^2$ has a root in $M$, so splits completely over $M$, so
$M = L[y]/(y^2 + \alpha y + \alpha^2) = \big(K[x]/(x^3 - 2)\big)[y]/(y^2 + xy + x^2)$
$= \mathbb{Q}[x, y]/(x^3 - 2, y^2 + xy + x^2)$ is a splitting field of $F(x)$ over $\mathbb{Q}$. The roots are $\overline{x}$, $\overline{y}$, and $\overline{-x - y}$.

# Extension of automorphisms to splitting fields

## Lemma

*Let* $\sigma : K_1 \simeq K_2$ *be a field isomorphism.*
*Let* $F_1(x) \in K_1[x]$*, and* $F_2(x) = F_1^\sigma(x) \in K_2[x]$*.*
*Finally, for* $i = 1, 2$*, let* $L_i$ *be a splitting field of* $F_i(x)$ *over* $K_i$*.*
*Then there exists* $\tau : L_1 \simeq L_2$ *such that* $\tau_{|K_1} = \sigma$*.*

## Proof.

Induction on $[L_1 : K_1]$.

If $[L_1 : K_1] = 1$, then $L_1 = K_1$, so $F_1(x) = \prod_j (x - \alpha_j)$ with $\alpha_j \in K_1$. So $F_2(x) = \prod_j \left(x - \sigma(\alpha_j)\right) \in K_2[x]$, so $L_2 = K_2 \rightsquigarrow$ take $\tau = \sigma$.

# Extension of automorphisms to splitting fields

**Proof.**

If $[L_1 : K_1] > 1$, then $F_1(x)$ not totally split over $K_1$, so has irreducible factor $P_1(x) \in K_1[x]$. Let $P_2(x) = P_1^\sigma(x) \in K_2[x]$, and for $i = 1, 2$, let $\alpha_i \in L_i$ be a root of $P_i(x)$, and let $E_i = K_i(\alpha_i) \subseteq L_i$. Then $E_i$ is a stem field of $P_i(x)$ over $K_i$, so

$$E_1 = K_1(\alpha_1) \simeq_{K_1} K_1[x]/\big(P_1(x)\big) \overset{\sigma}{\simeq} K_2[x]/\big(P_2(x)\big) \simeq_{K_2} K_2(\alpha_2) = E_2$$

$\rightsquigarrow \sigma' : E_1 \simeq E_2$ extending $\sigma$.

By tower law, $[L_1 : E_1] = [L_1 : K_1]/[E_1 : K_1] < [L_1 : K_1]$
$\rightsquigarrow$ induction. □

# Extension of automorphisms to splitting fields

**Lemma**

*Let $\sigma : K_1 \simeq K_2$ be a field isomorphism.*
*Let $F_1(x) \in K_1[x]$, and $F_2(x) = F_1^\sigma(x) \in K_2[x]$.*
*Finally, for $i = 1, 2$, let $L_i$ be a splitting field of $F_i(x)$ over $K_i$.*
*Then there exists $\tau : L_1 \simeq L_2$ such that $\tau_{|K_1} = \sigma$.*

**Corollary (Uniqueness of splitting fields)**

*Let $F(x) \in K[x]$. Splitting fields of $F(x)$ over $K$ are unique up to $K$-isomorphism.*

**Proof.**

Apply lemma with $K_1 = K_2 = K$ and $\sigma = \mathrm{Id}$. □

# Algebraic closure (proofs omitted)

**Theorem (Steinitz)**

*Let $K$ be any field. There exists an extension $K \subset \overline{K}$ such that every $F(x) \in K[x]$ splits over $\overline{K}$, and which is algebraic over $K$ (minimality). It is unique up to $K$-isomorphism.*

**Example**

$\overline{\mathbb{R}} = \mathbb{C}$.

**Counter-example**

$\overline{\mathbb{Q}}$ is not $\mathbb{C}$ (not algebraic $\rightsquigarrow$ too large), but

$$\{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}.$$

**Remark**

It may be shown that every $F(x) \in \overline{K}[x]$ splits over $\overline{K}$.

# Galois conjugacy

# $K$-morphisms and roots

## Lemma

*Let $K$ be a field, $F(x) \in K[x]$, $L, M$ extensions of $K$, and $\sigma : L \longrightarrow M$ a $K$-morphism. If $\alpha \in L$ a root of $F$, then $\sigma(\alpha) \in M$ is also a root of $F$.*

## Proof.

Write $F(x) = \sum_j k_j x^j$ with $k_j \in K$. Then

$$0 = \sigma(0) = \sigma\big(F(\alpha)\big) = \sigma\left(\sum_j k_j \alpha^j\right)$$

$$= \sum_j \sigma(k_j)\sigma(\alpha)^j = \sum_j k_j \sigma(\alpha)^j = F\big(\sigma(\alpha)\big).$$

□

# $K$-morphisms and roots

**Lemma**

*Let $K$ be a field, $F(x) \in K[x]$, $L, M$ extensions of $K$, and $\sigma : L \longrightarrow M$ a $K$-morphism. If $\alpha \in L$ a root of $F$, then $\sigma(\alpha) \in M$ is also a root of $F$.*

**Example**

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be complex conjugation. As $\sigma \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$, the set of complex roots of any $F(x) \in \mathbb{R}[x]$ is stable by $\sigma$.

# Galois conjugacy

**Theorem**

*Let $F(x) \in K[x]$, $L$ a splitting field of $F(x)$ over $K$, and $\alpha, \beta \in L$. TFAE:*

- *$\alpha$ and $\beta$ have the same minimal polynomial over $K$,*
- *There exists $\sigma \in \mathrm{Aut}_K(L)$ such that $\sigma(\alpha) = \beta$.*

**Proof.**

$\Downarrow$: $K_1 = K(\alpha)$ and $K_2 = K(\beta)$ are stem fields of $P$ over $K$ $\rightsquigarrow$ $K$-isomorphism $\sigma : K(\alpha) \simeq_K K(\beta)$ sending $\alpha$ to $\beta$, which extends to $\tau \in \mathrm{Aut}(L)$.

$\Uparrow$: Let $P(x) \in K[x]$ min poly of $\alpha$. Then $P(\alpha) = 0$, so $P(\beta) = 0$ as well by lemma.
$\rightsquigarrow$ min poly of $\beta$ over $K$ divides $P$, so $= P$ (irr+monic). □

# Galois conjugacy

**Theorem**

*Let $F(x) \in K[x]$, $L$ a splitting field of $F(x)$ over $K$, and $\alpha, \beta \in L$. TFAE:*

- $\alpha$ *and* $\beta$ *have the same minimal polynomial over* $K$,
- *There exists* $\sigma \in \mathrm{Aut}_K(L)$ *such that* $\sigma(\alpha) = \beta$.

**Definition (Galois conjugacy)**

*In this case,* $\alpha$ *and* $\beta$ *are said to be conjugate over* $K$.

# Galois conjugacy

## Theorem

*Let $F(x) \in K[x]$, $L$ a splitting field of $F(x)$ over $K$, and $\alpha, \beta \in L$. TFAE:*

- *$\alpha$ and $\beta$ have the same minimal polynomial over $K$,*
- *There exists $\sigma \in \mathrm{Aut}_K(L)$ such that $\sigma(\alpha) = \beta$.*

## Definition (Galois conjugacy)

*In this case, $\alpha$ and $\beta$ are said to be conjugate over $K$.*

## Example

The conjugates of $\alpha = \sqrt[3]{2}$ over $\mathbb{Q}$ are $\alpha$ itself, $\beta = \zeta\sqrt[3]{2}$, and $\gamma = \zeta^2\sqrt[3]{2}$ ($\zeta = e^{2\pi i/3}$).
So there exist $\mathbb{Q}$-automorphisms of $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ which permute $\alpha, \beta, \gamma$ transitively.

# Galois conjugacy

**Example (Complex conjugacy as Galois conjugacy)**

Take $K = \mathbb{R}$, $F(x) = x^2 + 1 \rightsquigarrow L = \mathbb{C}$, and let $\alpha \in \mathbb{C}$.

As $\mathbb{R} \subseteq \mathbb{R}(\alpha) \subseteq \mathbb{C}$, $\alpha$ is algebraic over $\mathbb{R}$ of degree $\leq 2$.

If $\alpha \in \mathbb{R}$, then its min poly over $\mathbb{R}$ is $x - \alpha$, so the only $\mathbb{R}$-conjugate of $\alpha$ is $\alpha$ itself.

If $\alpha \notin \mathbb{R}$, then its min poly over $\mathbb{R}$ must be $(x - \alpha)(x - \overline{\alpha})$, so the $\mathbb{R}$-conjugates of $\alpha$ are $\alpha$ and $\overline{\alpha}$.

# Finite fields 1/4: Characteristic

# The characteristic of a ring

## Definition (Characteristic of a ring)

*Let $R$ be a ring. Its characteristic is the $c \in \mathbb{Z}_{\geq 0}$ such that*

$$\begin{aligned} i_R : \mathbb{Z} &\longrightarrow R \\ n &\longmapsto \underbrace{1 + \cdots + 1}_{n \text{ times}} \end{aligned}$$

*satisfies* $\operatorname{Ker} i_R = c\mathbb{Z}$.

In other words, char $R$ is the smallest $c \in \mathbb{N}$ such that $\underbrace{1 + \cdots + 1}_{c \text{ times}} = 0$ in $R$, or 0 if there is no such $c$.

## Example

$\operatorname{char} \mathbb{Z}/m\mathbb{Z} = m$.
$\operatorname{char} \mathbb{Q}[x] = 0$.

# The characteristic of a ring

**Definition (Characteristic of a ring)**

*Let $R$ be a ring. Its characteristic is the $c \in \mathbb{Z}_{\geq 0}$ such that*

$$\begin{aligned} i_R : \mathbb{Z} &\longrightarrow R \\ n &\longmapsto \underbrace{1 + \cdots + 1}_{n \text{ times}} \end{aligned}$$

*satisfies* $\operatorname{Ker} i_R = c\mathbb{Z}$.

In other words, char $R$ is the smallest $c \in \mathbb{N}$ such that $\underbrace{1 + \cdots + 1}_{c \text{ times}} = 0$ in $R$, or 0 if there is no such $c$.

**Remark**

For all $x \in R$, $(\operatorname{char} R)x = (\underbrace{1 + \cdots + 1}_{\operatorname{char} R \text{ times}})x = 0x = 0$.

**Remark**

If $R$ is finite, then char $R \neq 0$ since $i_R$ cannot be injective.

# The characteristic of a domain

**Proposition**

*If $R$ is a domain, then* char $R$ *is either* 0 *or a prime number.*

**Proof.**

Suppose char $R = ab$ with $a, b <$ char $R$. Then

$$0 = \underbrace{1 + \cdots + 1}_{ab \text{ times}} = (\underbrace{1 + \cdots + 1}_{a \text{ times}})(\underbrace{1 + \cdots + 1}_{b \text{ times}})$$

but $\underbrace{1 + \cdots + 1}_{a \text{ times}} \neq 0$ and $\underbrace{1 + \cdots + 1}_{b \text{ times}} \neq 0$ in $R$. □

**Remark**

char $\mathbb{Q} = 0$.
char $\mathbb{Z}/p\mathbb{Z} = p$.

# The prime subfield

**Definition (Prime subfield)**

*Let $K$ be a field. The prime subfield of $K$ is the smallest subfield of $K$, i.e. that generated by $0$ and $1$.*

**Example**

The prime subfield of $\mathbb{R}$ is $\mathbb{Q}$.

**Proposition**

*Let $K$ be a field.*

- *If* $\operatorname{char} K = 0$, *then $K$ contains a copy of $\mathbb{Q}$.*
- *If* $\operatorname{char} K = p$, *then $K$ contains a copy of $\mathbb{Z}/p\mathbb{Z}$.*

**Proof.**

Consider the prime subfield of $K$. □

# The cardinal of a finite field

**Theorem**

*If $K$ is a finite field, then there exists $d \in \mathbb{N}$ such that $\#K = p^d$, where $p = \operatorname{char} K$.*

**Proof.**

We know that $K$ is a finite extension of $\mathbb{Z}/p\mathbb{Z}$.
Let $d = [K : \mathbb{Z}/p\mathbb{Z}]$. Then $K \simeq (\mathbb{Z}/p\mathbb{Z})^d$ as $(\mathbb{Z}/p\mathbb{Z})$-vector spaces; in particular, they have the same cardinal. □

**Example**

There does not exist a field with 6 elements.

# An identity in finite fields

**Lemma**

*Let $K$ be a finite field with $q$ elements. Then $k^q = k$ for all $k \in K$.*

**Proof.**

If $k = 0$, OK.
Else, $k \in K^\times$, which is a group of order $q-1$, so $k^{q-1} = 1$ by Lagrange. □

# Finite fields 2/4: Frobenius

# The Frobenius morphism

**Proposition**

*Let $R$ be a commutative ring such that* char $R$ *is a prime number $p$. Then*

$$(a+b)^p = a^p + b^p$$

*for all $a, b \in R$.*

**Proof.**

Since $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$, if suffices to prove that $p \mid \binom{p}{k}$ for $0 < k < p$. And indeed $p \mid p! = \binom{p}{k} k!(p-k)!$, but $p \nmid k!$ nor $(p-k)!$. $\square$

# The Frobenius morphism

## Proposition

*Let $R$ be a commutative ring such that* char $R$ *is a prime number $p$. Then*

$$(a+b)^p = a^p + b^p$$

*for all $a, b \in R$.*

## Corollary (Frobenius map)

*If* char $R = p$*, then the Frobenius map*

$$\text{Frob} : \begin{array}{ccc} R & \longrightarrow & R \\ r & \longmapsto & r^p \end{array}$$

*is a ring morphism.*

# The Frobenius morphism

**Corollary (Frobenius map)**

*If* char $R = p$, *then the Frobenius map*

$$\text{Frob} : \begin{array}{ccc} R & \longrightarrow & R \\ r & \longmapsto & r^p \end{array}$$

*is a ring morphism.*

**Example**

Take $R = \mathbb{Z}/p\mathbb{Z}$. Then $\text{Frob}(a) = a^p = a$ for all $a \in R$, so $\text{Frob} = \text{Id}$.

# The Frobenius morphism

## Corollary (Frobenius map)

*If* char $R = p$, *then the* *Frobenius map*

$$\text{Frob} : \begin{array}{ccc} R & \longrightarrow & R \\ r & \longmapsto & r^p \end{array}$$

*is a ring morphism.*

## Example

Take $R = (\mathbb{Z}/p\mathbb{Z})[x]$, and let $F(x) = \sum_j f_j x^j \in R$. Then

$$\text{Frob}(F(x)) \overset{\text{def}}{=} \left( \sum_j f_j x^j \right)^p = \sum_j f_j^p (x^j)^p = \sum_j f_j x^{pj}$$

so $\text{Frob} : F(x) \longmapsto F(x^p)$.

# Finite fields 3/4: Structure theorems

# Finite multiplicative subgroups in fields

**Lemma**

*Let $K$ be a field, and $G \leq K^\times$ a finite subgroup. Then $G$ is cyclic.*

**Proof (Non-examinable).**

Let $n = \#G$, and for all $d \mid n$, let $\psi(d)$ be the number of elements of $G$ of order exactly $d$.

Claim: $\psi(d) \leq \phi(d)$ for all $d$.

If $\psi(d) = 0$ OK. Else, let $h \in G$ have order $d$, and let $H = \langle h \rangle \leq G$, so $H \simeq \mathbb{Z}/d\mathbb{Z}$. For all $k \in H$, $k^d = 1$ by Lagrange. But $x^d - 1$ has at most $d$ roots in the field $K$
$\rightsquigarrow$ for all $x \in K$, $x^d = 1 \implies x \in H$.
$\rightsquigarrow \psi(d) = \phi(d)$ if $\psi(d) \neq 0$.

Thus $n = \sum_{d|n} \psi(d) \underset{\text{claim}}{\leq} \sum_{d|n} \phi(d) = n$

$\rightsquigarrow \psi(d) = \phi(d)$ for all $d$. In particular, $\psi(n) = \phi(n) \geq 1$. □

# Summary of results so far

## Theorem

*Let $K$ be a finite field with $q$ elements.*
*Then $q = p^d$ where $p = \operatorname{char} K$ is prime, $K \supseteq \mathbb{Z}/p\mathbb{Z}$, and $d = [K : \mathbb{Z}/p\mathbb{Z}]$.*
*Besides,*

$$(K, +) \simeq (\mathbb{Z}/p\mathbb{Z})^d,$$

$$(K^\times, \times) \simeq \mathbb{Z}/(q-1)\mathbb{Z},$$

*and* $\operatorname{Frob} \in \operatorname{Aut}_{\mathbb{Z}/p\mathbb{Z}}(K)$.

# Summary of results so far

**Theorem**

*Let $K$ be a finite field with $q$ elements.*
*Then $q = p^d$ where $p = \operatorname{char} K$ is prime, $K \supseteq \mathbb{Z}/p\mathbb{Z}$, and $d = [K : \mathbb{Z}/p\mathbb{Z}]$.*
*Besides,*

$$(K, +) \simeq (\mathbb{Z}/p\mathbb{Z})^d,$$

$$(K^\times, \times) \simeq \mathbb{Z}/(q-1)\mathbb{Z},$$

*and $\operatorname{Frob} \in \operatorname{Aut}_{\mathbb{Z}/p\mathbb{Z}}(K)$.*

**Corollary (Primitive element theorem for finite fields)**

*If $K \subseteq L$ are finite fields, then $L = K(\alpha)$ for some $\alpha \in L$.*
*In particular, $L \simeq_K K[x]/\big(m_\alpha(x)\big)$, where $m_\alpha(x) \in K[x]$ is the minimal polynomial of $\alpha$ over $K$.*

# Summary of results so far

**Corollary (Primitive element theorem for finite fields)**

*If $K \subseteq L$ are finite fields, then $L = K(\alpha)$ for some $\alpha \in L$.*
*In particular, $L \simeq_K K[x]/\big(m_\alpha(x)\big)$, where $m_\alpha(x) \in K[x]$ is the minimal polynomial of $\alpha$ over $K$.*

**Proof.**

Take $\alpha \in L$ to be a generator of the cyclic group $L^\times$. □

# Fundamental theorem of finite fields

**Theorem**

- *The number of elements of a finite field is a prime power. Conversely, for each prime power* $q = p^d$*, there exists a finite field with* $q$ *elements.*
- *Two finite fields with the same number of elements are isomorphic.*
- *Let* $K$ *and* $L$ *be two finite fields. Then* $L$ *contains a copy of* $K$ *iff.* $\#L$ *is a power of* $\#K$*.*

The first two points justify the notation $\mathbb{F}_q$ for "the" finite field with $q$ elements.

**Example**

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

# Fixed points of field morphisms

**Lemma**

*Let $K$ be a field, and $\sigma : K \longrightarrow K$ be a field morphism. Then $\{\alpha \in K \mid \sigma(\alpha) = \alpha\}$ is a subfield of $K$.*

**Proof.**

Routine. □

# Fundamental theorem of finite fields : proof (1/3)

Suppose $q = p^d$ is a prime power. Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and let

$$Z_q = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^q = \alpha\}.$$

Claim: $Z_q$ is a subfield of $\overline{\mathbb{F}}_p$ with $q$ elements.
Indeed, since $\Phi_q = \underbrace{\mathrm{Frob} \circ \cdots \circ \mathrm{Frob}}_{d \text{ times}} : x \longmapsto x^q$ is a field morphism, $Z_q$ is a subfield of $\overline{\mathbb{F}}_p$.
Besides, let $F(x) = x^q - x \in \mathbb{F}_p[x]$. It has all its roots in $\overline{\mathbb{F}}_p$; and since $F'(x) = qx^{q-1} - 1 = -1$ as $p = 0 \in \mathbb{F}_p$, $\gcd(F, F') = 1$, so $F$ has no repeated roots $\rightsquigarrow \#Z_q = q$.

# Fundamental theorem of finite fields : proof (2/3)

Suppose now that $M$ is another field with $q$ elements.

Then $M = \mathbb{F}_p(\alpha)$ for some $\alpha \in M$; let $m_\alpha(x) \in \mathbb{F}_p[x]$ be its minimal polynomial, and let $\beta \in \overline{\mathbb{F}_p}$ be a root of $m_\alpha(x)$.

As $\mathbb{F}_p(\alpha) = M$ and $\mathbb{F}_p(\beta) \subseteq \overline{\mathbb{F}_p}$ are stem fields of $m_\alpha(x)$, they are isomorphic.
Besides, $\#\mathbb{F}_p(\beta) = \#M = q$, so $\gamma^q = \gamma$ for all $\gamma \in \mathbb{F}_p(\beta)$, so $\mathbb{F}_p(\beta) \subseteq Z_q$; and actually $\mathbb{F}_p(\beta) = Z_q$ by cardinals.

# Fundamental theorem of finite fields : proof (3/3)

Let $K$ and $L$ be finite fields with $\#K = q = p^d$ and $\#L = q' = p'^{d'}$.

If $K \subseteq L$, then $\#L = \#K^{[L:K]}$, so $p' = p$ and $d \mid d'$.

Conversely, suppose that $p' = p$ and $d \mid d'$.
Then $Z_q \subseteq Z_{q'}$ in $\overline{\mathbb{F}_p}$.
But up to isomorphism, $K = Z_q$, and $L = Z_{q'}$.

**Example**

$\mathbb{F}_4$ and $\mathbb{F}_8$ are both extensions of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, but $\mathbb{F}_8$ does not contain any copy of $\mathbb{F}_4$!

In fact, the smallest finite field containing both a copy of $\mathbb{F}_4$ and a copy of $\mathbb{F}_8$ is $\mathbb{F}_{64}$.

# Finite fields 4/4: Explicit construction

# Construction of finite fields

Let $q = p^d$ be a prime power. We know that $\mathbb{F}_q$ exists, and is an extension of $\mathbb{F}_p$ of degree $d$
$\rightsquigarrow \mathbb{F}_q = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_q$
$\rightsquigarrow m_\alpha(x) \in \mathbb{F}_p[x]$ is irreducible of degree $d$.

Conversely, if $P(x) \in \mathbb{F}_p[x]$ is any irreducible polynomial of degree $d$, then

$$\mathbb{F}_p[x]/\big(P(x)\big)$$

is a finite field with $p^d = q$ elements.

# Example: small extensions of $\mathbb{F}_2$

We have $\mathbb{F}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

To construct $\mathbb{F}_4$, we need $P(x) \in \mathbb{F}_2[x]$ irreducible of deg 2.
A polynomial of degree 2 is irreducible iff. it has no roots, and the only possible roots are $\{0, 1\} = \mathbb{F}_2$
$\rightsquigarrow P(x) = x^2 + x + 1$ (only choice!)

$$\rightsquigarrow \quad \mathbb{F}_4 \simeq \mathbb{F}_2[x]/(x^2 + x + 1).$$

To construct $\mathbb{F}_8$, we need $Q(x) \in \mathbb{F}_2[x]$ irreducible of deg 3.
A polynomial of degree 3 is irreducible iff. it has no roots.
$\rightsquigarrow Q(x) = x^3 + x + 1$ (other choice: $x^3 + x^2 + 1$)

$$\rightsquigarrow \quad \mathbb{F}_8 \simeq \mathbb{F}_2[x]/(x^3 + x + 1).$$

# Example: small extensions of $\mathbb{F}_2$

To construct $\mathbb{F}_4$, we need $P(x) \in \mathbb{F}_2[x]$ irreducible of deg 2.
$\rightsquigarrow P(x) = x^2 + x + 1$ (only choice!)

$$\rightsquigarrow \quad \mathbb{F}_4 \simeq \mathbb{F}_2[x]/(x^2 + x + 1).$$

To construct $\mathbb{F}_8$, we need $Q(x) \in \mathbb{F}_2[x]$ irreducible of deg 3.

$$\rightsquigarrow \quad \mathbb{F}_8 \simeq \mathbb{F}_2[x]/(x^3 + x + 1).$$

To construct $\mathbb{F}_{16}$, we need $R(x) \in \mathbb{F}_2[x]$ irreducible of deg 4.
A polynomial of degree 4 is irreducible iff. it has no roots and is not the product of two irreducibles of degree 2.
The only product of irreducibles of degree 2 is

$$(x^2 + x + 1)^2 = (x^2)^2 + x^2 + 1^2 = x^4 + x^2 + 1.$$

$\rightsquigarrow$ can take $R(x) = x^4 + x + 1$ (there are other choices)

$$\rightsquigarrow \quad \mathbb{F}_{16} \simeq \mathbb{F}_2[x]/(x^4 + x + 1).$$

# Polynomials and their roots

# Symmetric polynomials

Fix $n \in \mathbb{N}$, and let $K$ be a field.

**Definition**

*A polynomial $F(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ is symmetric if it is invariant under any permutation of the variables $x_1, \cdots, x_n$.*

**Example ($n = 3$)**

$x_1^2 + x_2^2 + x_3^2$ is a symmetric polynomial.
$x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1$ is not.

# Elementary symmetric polynomials

## Definition

*The elementary symmetric polynomials in n variables are*

- $\sigma_1 = x_1 + x_2 + \cdots + x_n$,
- $\vdots$
- $\sigma_j = \sum_{\substack{I \subseteq \{1, \cdots, n\} \\ \#I = j}} \prod_{i \in I} x_i$,
- $\vdots$
- $\sigma_n = x_1 x_2 \cdots x_n$.

## Example

For $n = 4$, the elementary symmetric polynomials are

- $\sigma_1 = x_1 + x_2 + x_3 + x_4$,
- $\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$,
- $\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$,
- $\sigma_4 = x_1x_2x_3x_4$.

# Fundamental theorem on symmetric polynomials

**Theorem (Proof omitted)**

*Let $K$ be a field, and let $F(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$. Then $F$ is symmetric $\iff$ $F$ is a polynomial in $\sigma_1, \cdots, \sigma_n$ with coefficients in $K$.*

**Remark**

$\Longleftarrow$ is obvious.

**Example ($n = 3$)**

$F = x_1^2 + x_2^2 + x_3^2$ is symmetric, so it can be expressed in terms of $\sigma_1$, $\sigma_2$, $\sigma_3$. Indeed,

$\sigma_1^2 = (x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3 = F + 2\sigma_2$

$\leadsto F = \sigma_1^2 - 2\sigma_2$.

# Relations between coefficients and roots

**Theorem (Vieta)**

*Let* $F(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$ *have roots* $\alpha_1, \cdots, \alpha_n \in \overline{K}$. *Then* $a_j = (-1)^j \sigma_j(\alpha_1, \cdots, \alpha_n)$ *for all* $j$.

**Proof.**

Expand $F(x) = \prod_{j=1}^n (x - \alpha_j)$. □

# Relations between coefficients and roots

## Theorem (Vieta)

*Let* $F(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$ *have roots* $\alpha_1, \cdots, \alpha_n \in \overline{K}$. *Then* $a_j = (-1)^j \sigma_j(\alpha_1, \cdots, \alpha_n)$ *for all* $j$.

## Corollary

*We can read the value of any symmetric polynomial in the roots of* $F(x)$ *off its coefficients* $a_j$, *even if we do not know these roots.*

## Example

Let $F(x) = x^3 - x^2 + 2x + 8$ have roots $\alpha_1, \alpha_2, \alpha_3$. Then we have $\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 1$, $\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = 2$, and $\sigma_3 = \alpha_1\alpha_2\alpha_3 = -8$.
Therefore, $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = \sigma_1^2 - 2\sigma_2 = -3$.

# Relations between coefficients and roots

## Theorem (Vieta)

*Let* $F(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in K[x]$ *have roots* $\alpha_1, \cdots, \alpha_n \in \overline{K}$. *Then* $a_j = (-1)^j \sigma_j(\alpha_1, \cdots, \alpha_n)$ *for all* $j$.

## Corollary

*We can read the value of any symmetric polynomial in the roots of* $F(x)$ *off its coefficients* $a_j$*, even if we do not know these roots.*

## Example

Let $F(x) = x^3 - x^2 + 2x + 8$ have roots $\alpha_1, \alpha_2, \alpha_3$.
In contrast, we cannot evaluate $\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1$ that way.
In fact, this value depends on the ordering of the roots!

# Relations between coefficients and roots

**Theorem (Vieta)**

*Let* $F(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$ *have roots* $\alpha_1, \cdots, \alpha_n \in \overline{K}$. *Then* $a_j = (-1)^j \sigma_j(\alpha_1, \cdots, \alpha_n)$ *for all* $j$.

**Corollary**

*We can read the value of any symmetric polynomial in the roots of* $F(x)$ *off its coefficients* $a_j$, *even if we do not know these roots.*

**Corollary**

*The value of any symmetric polynomial in the roots with coefficients in* $K$ *lies in* $K$.

# Resultants

# Resultant: definition

**Definition (Resultant of two polynomials)**

*Let $R$ be a commutative ring. The resultant of $A = \sum_{j=0}^m a_j x^j \in R[x]$ and $B = \sum_{k=0}^n b_k x^k \in R[x]$ is the $(m+n) \times (m+n)$ determinant*

$$\operatorname{Res}(A,B) = \begin{vmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{vmatrix} \in R$$

*($n$ rows of $A$, $m$ rows of $B$).*

# Resultant: definition

**Example**

$$\mathrm{Res}(x^2 - 2, x^2 + 1) = \begin{vmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{vmatrix} = 9.$$

# Resultant: properties

## Theorem (Proof admitted)

*Let $K$ be a field, and $A(x), B(x) \in K[x]$.*
*If we have (over $K$ or an extension)*

$$A = a \prod_{j=1}^{\deg A} (x - \alpha_j) \text{ and } B = b \prod_{k=1}^{\deg B} (x - \beta_k), \text{ then}$$

$$\operatorname{Res}(A, B) = a^{\deg B} \prod_{j=1}^{\deg A} B(\alpha_j) = a^{\deg B} b^{\deg A} \prod_{j=1}^{\deg A} \prod_{k=1}^{\deg B} (\alpha_j - \beta_k)$$

$$= (-1)^{\deg A \deg B} b^{\deg A} \prod_{k=1}^{\deg B} A(\beta_k) = (-1)^{\deg A \deg B} \operatorname{Res}(B, A).$$

## Example ($K = \mathbb{Q}$)

Let $A = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, $B = x^2 + 1 = (x - i)(x + i)$. Then

$$\operatorname{Res}(A, B) = B(\sqrt{2})B(-\sqrt{2}) = A(i)A(-i)$$
$$= (\sqrt{2} - i)(\sqrt{2} + i)(-\sqrt{2} - i)(-\sqrt{2} + i) = 9.$$

# Resultant: properties

## Theorem (Proof admitted)

*Let $K$ be a field, and $A(x), B(x) \in K[x]$.*
*If we have (over $K$ or an extension)*

$$A = a \prod_{j=1}^{\deg A} (x - \alpha_j) \text{ and } B = b \prod_{k=1}^{\deg B} (x - \beta_k), \text{ then}$$

$$\operatorname{Res}(A, B) = a^{\deg B} \prod_{j=1}^{\deg A} B(\alpha_j) = a^{\deg B} b^{\deg A} \prod_{j=1}^{\deg A} \prod_{k=1}^{\deg B} (\alpha_j - \beta_k)$$

$$= (-1)^{\deg A \deg B} b^{\deg A} \prod_{k=1}^{\deg B} A(\beta_k) = (-1)^{\deg A \deg B} \operatorname{Res}(B, A).$$

## Corollary

$\operatorname{Res}(A, B) = 0 \iff$ *$A$ and $B$ have a common root in $\overline{K}$* $\iff$ *$A$ and $B$ have a common nontrivial factor over $K$.*

# Application: preservation of algebraicness

**Theorem**

*Let $K \subseteq L$ be fields, and let $\alpha, \beta \in L$. If $\alpha$ and $\beta$ are algebraic over $K$, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and $\alpha/\beta$ ($\beta \neq 0$).*

**Non-constructive proof.**

$\alpha, \beta$ alg. $/ K \rightsquigarrow$ minpoly $A(x), B(x) \in K[x]$. Then $[K(\alpha) : K] = \deg A < \infty$, and $[K(\alpha, \beta) : K(\alpha)] \leqslant \deg B < \infty$ since the minpoly of $\beta$ over $K(\alpha)$ divides $B(x)$.
By tower law, $[K(\alpha, \beta) : K] < \infty$, so $K(\alpha, \beta)$ is an algebraic extension of $K$. □

# Application: preservation of algebraicness

**Theorem**

*Let $K \subseteq L$ be fields, and let $\alpha, \beta \in L$. If $\alpha$ and $\beta$ are algebraic over $K$, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and $\alpha/\beta$ ($\beta \neq 0$).*

**Constructive proof with resultants.**

$\alpha, \beta$ alg. $/ K \rightsquigarrow$ minpoly $A(x), B(x) \in K[x]$. Factor (over $\overline{L}$)

$$A(x) = \prod_{j=1}^{m}(x - \alpha_j), \quad B(x) = \prod_{k=1}^{n}(x - \beta_k),$$

where $\alpha = \alpha_1$ and $\beta = \beta_1$, and view $A(y), B(x - y) \in K[x][y]$.
Then $C(x) = \operatorname{Res}\left(A(y), B(x - y)\right) \in K[x]$ satisfies

$$C(x) = \prod_{j=1}^{m} B(x-y)|_{y=\alpha_j} = \prod_{j=1}^{m} B(x-\alpha_j) = \prod_{j=1}^{m}\prod_{k=1}^{n}(x-\alpha_j-\beta_k),$$

so $\alpha + \beta$ root of $C(x) \rightsquigarrow$ algebraic $/ K$.
Same idea for $\alpha - \beta$, $\alpha\beta$ and $\alpha/\beta$. $\square$

# Application: preservation of algebraicness

## Theorem

*Let $K \subseteq L$ be fields, and let $\alpha, \beta \in L$. If $\alpha$ and $\beta$ are algebraic over $K$, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and $\alpha/\beta$ ($\beta \neq 0$).*

## Example

$\alpha = \sqrt{2}$, $\beta = \sqrt{3}$ algebraic / $\mathbb{Q}$ $\rightsquigarrow$ $\alpha + \beta$ algebraic / $\mathbb{Q}$.
More specifically, since $A(x) = x - 2$ and $B(x) = x - 3$, $\alpha + \beta$ is a root of

$$\begin{aligned}
\operatorname{Res}_y(y^2 - 2, (x-y)^2 - 3) &= \operatorname{Res}_y(y^2 - 2, y^2 - 2xy + x^2 - 3) \\
&= \begin{vmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 1 & -2x & x^2 - 3 & 0 \\ 0 & 1 & -2x & x^2 - 3 \end{vmatrix} \\
&= x^4 - 10x^2 - 1 \in \mathbb{Q}[x].
\end{aligned}$$

# Application: preservation of algebraicness

**Theorem**

*Let $K \subseteq L$ be fields, and let $\alpha, \beta \in L$. If $\alpha$ and $\beta$ are algebraic over $K$, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and $\alpha/\beta$ ($\beta \neq 0$).*

**Example**

$$\mathcal{A} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}$$

is a subfield of $\mathbb{C}$ ($\rightsquigarrow \mathcal{A} = \overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$).

# Discriminants

# Reminder on multiple roots

Let $K \subseteq L$ be fields, $F(x) \in K[x]$, and $\alpha \in L$.

**Lemma**

$F(\alpha) = 0 \iff F(x) = (x - \alpha)G(x)$ *for some* $G(x) \in L[x]$.

**Proof.**

Euclidean-divide $F(x)$ by $x - \alpha$ in $L[x]$:

$$F(x) = (x - \alpha)Q(x) + R(x)$$

where $\deg R < \deg(x - \alpha)$ so $R$ is constant.

Evaluate at $x = \alpha \rightsquigarrow R = F(\alpha)$. □

# Reminder on multiple roots

Let $K \subseteq L$ be fields, $F(x) \in K[x]$, and $\alpha \in L$.

**Definition (Multiple root)**

*$\alpha$ is a multiple root of $F(x)$ if $F(x) = (x-\alpha)^2 H(x)$ for some $H(x) \in L[x]$.*

**Proposition (Derivatives detect multiple roots)**

*Let $\alpha \in L$ be a root of $F(x)$. Then*

$$\alpha \text{ is a multiple root of } F(x) \iff F'(\alpha) = 0.$$

**Proof.**

$F(x) = (x-\alpha)G(x) \rightsquigarrow F'(x) = G(x) + (x-\alpha)G'(x)$, so $F'(\alpha) = 0 \iff G(\alpha) = 0 \iff G(x) = (x-\alpha)H(x)$ for some $H(x) \in L[x]$. □

# Discriminant: definition

## Definition

*Let $A(x) \in K[x]$ have degree $n \in \mathbb{N}$ and leading coefficient $a \in K$. Its discriminant is*

$$\operatorname{disc} A = \frac{(-1)^{n(n-1)/2}}{a} \operatorname{Res}(A, A') \in K.$$

## Example

Let $A(x) = ax^2 + bx + c$, $a \neq 0$. Then $A'(x) = 2ax + b$, so that

$$\operatorname{Res}(A, A') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = 4a^2c - ab^2,$$

$$\rightsquigarrow \quad \operatorname{disc} A = \frac{-1}{a} \operatorname{Res}(A, A') = b^2 - 4ac.$$

# Discriminant: properties

**Theorem**

*Let $A(x) \in K[x]$ have degree $n \in \mathbb{N}$, leading coefficient $a \in K$, and roots $\alpha_1, \cdots, \alpha_n \in \overline{K}$. Then*

$$\begin{aligned} \operatorname{disc} A &= (-1)^{n(n-1)/2} a^{n-2} \prod_{j=1}^{n} A'(\alpha_j) \\ &= (-1)^{n(n-1)/2} a^{2n-2} \prod_{j \neq k} (\alpha_j - \alpha_k) \\ &= a^{2n-2} \prod_{j<k} (\alpha_j - \alpha_k)^2. \end{aligned}$$

**Proof.**

Since $A(x) = a \prod_{j=1}^{n} (x - \alpha_j)$, we have $A'(x) = a \sum_{j=1}^{n} \prod_{k \neq j} (x - \alpha_k)$

$\rightsquigarrow A'(\alpha_j) = a \prod_{k \neq j} (\alpha_j - \alpha_k)$. □

# Discriminant: properties

**Theorem**

*Let $A(x) \in K[x]$ have degree $n \in \mathbb{N}$, leading coefficient $a \in K$, and roots $\alpha_1, \cdots, \alpha_n \in \overline{K}$. Then*

$$\begin{aligned}\operatorname{disc} A &= (-1)^{n(n-1)/2} a^{n-2} \prod_{j=1}^{n} A'(\alpha_j) \\ &= (-1)^{n(n-1)/2} a^{2n-2} \prod_{j \neq k} (\alpha_j - \alpha_k) \\ &= a^{2n-2} \prod_{j<k} (\alpha_j - \alpha_k)^2.\end{aligned}$$

**Corollary**

*$A(x)$ has multiple roots in $\overline{K}$* $\iff \operatorname{disc} A = 0$.

# Discriminant: properties

**Corollary**

*$A(x)$ has multiple roots in $\overline{K}$* $\iff \operatorname{disc} A = 0$.

**Definition (Separable polynomial)**

*A polynomial $A(x) \in K[x]$ is separable if* $\operatorname{disc} A \neq 0$, *and inseparable if* $\operatorname{disc} A = 0$.