Galois theory lecture (April 1st 2020)

Midterm: How to prove that a polynomial \( f \in \mathbb{F}_2[x] \) over a finite field is irreducible?

Idea: Take \( \alpha \in \overline{\mathbb{F}}_2 \) a root of \( f \). If you can show that \( \deg \left( \alpha^r \right) = \deg (f) \Rightarrow \left( \begin{array}{l}
\text{Since } f^\alpha \mid f \\
\text{get } f^\alpha = f
\end{array} \right) \),

\[
\deg \left( \alpha^r \right) = \begin{cases}
\text{the smallest } r \geq 1 \text{ such that } \\
\alpha^r = \alpha
\end{cases}
\]

Why? Know \( \mathbb{F}_2(\alpha) \) is a subfield, it is finite and therefore equal to \( \{ x \in \overline{\mathbb{F}}_2 \mid x^r = x \} \), with \( r = \deg (\alpha) \).

Ex 4 of midterm: \( X^p - 2X + 1 = f \)

\( \Rightarrow f(1) = 0 \) so certainly \( f \) is reducible.

\[ f(1) = 0 \quad \Rightarrow f(1) = 0 \quad \Rightarrow f \text{ is reducible.} \]

\( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \quad \ast \text{Hom} \left( \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}), \mathbb{Q} \right) = 8 \)

\[ \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{5}) = \{ \pm \sqrt{2}, \pm \sqrt{3}, \pm \sqrt{5} \}, \mathbb{Q}(\sqrt{2}) \]

\( \varphi \mid \mathbb{Q}(\alpha) \quad \varphi \in \text{Hom}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}), \mathbb{Q}) \quad \varphi(\sqrt{2}) = \pm \sqrt{2} \)

\[ \varphi(\sqrt{3}) = \pm \sqrt{3} \]

\[ \varphi(\sqrt{5}) = \pm \sqrt{5} \]
Suppose \( \varphi \neq \varphi' \in \text{Hom}(\varphi(\sqrt{2}, \sqrt{3}, \sqrt{5}, \bar{a})) \),

but \( \varphi|_{\varphi(\alpha)} = \varphi'|_{\varphi(\alpha)} \).

\[
\Rightarrow \quad \varphi(\alpha) = \varphi'(\alpha) \quad \Rightarrow \quad \varepsilon_1 \sqrt{2} + \varepsilon_2 \sqrt{3} + \varepsilon_3 \sqrt{5} = \varepsilon_1' \sqrt{2} + \varepsilon_2' \sqrt{3} + \varepsilon_3' \sqrt{5}.
\]

\(\sim\) non-trivial linear relation between \(\sqrt{2}, \sqrt{3}, \sqrt{5}\). → \(\notin \mathbb{Q}\).
Plan: 
1. Perfect fields
2. Primitive elements
3. Normal extensions

Skip: Linear independence of characters (next week?)

4. Norm and trace (if time)
§ Perfect Fields

Lemma \( f \in K[x] \) irreducible, but \( f \) not separable. \( \Rightarrow \) \( f = g(x^p) \) for some \( p = \text{char}(K) > 0 \).

Def | perfect fields.

Thm | A field \( K \) is perfect \( \iff \) All finite extensions of it are separable.

---

Proof of the lemma \( K \) a field.

\( f \in K[x] \) irreducible, not separable.
\( f \) has a double root \( \alpha \in \overline{K} \).
\( \Rightarrow \) \( f, f' \) have a factor in common.
\( \Rightarrow \) \( f' \) and \( f \) are not coprime.
\( \Rightarrow \) \( \deg(f') < \deg(f) \) and \( f \) is irreducible.

Get \( f' = 0 \).

Write \( f = \sum_{i=0}^{\hat{n}} a_i x^i \) (\( \hat{n} = \deg(f) \)).

Get \( 0 = f' = \sum_{i=1}^{\hat{n}} i a_i x^{i-1} = 0 \).

If \( a_i \neq 0 \) for \( i \), then it is forced that \( i a_i = 0 \in K \).
\( \Rightarrow \text{char}(K) = p > 0 \) and \( p|\hat{n} \).
So indeed $f = g(X^p)$ for some $g \in K[X]$.

Additionally: Not every coefficient of $g$ is a power of $p$.

Why? Otherwise $f = h(x)^p \Rightarrow$ contradicts irr. of $f$.

**Def** We say that a field $K$ is *perfect* if
- $\text{char}(K) = 0$, or
- $\text{char}(K) = p > 0$ and $\text{Frob} : K \to K$
  $$x \mapsto x^p$$

**Thm** A field $K$ is perfect $\iff$ Every finite ext. $L/K$ is separable.

**Pf** "$\Rightarrow$" Assume $K$ is perfect. Let $\ell/K$ be finite, $\alpha \in \ell$ an element.

To prove $\ell/K$ is separable.

If it is not separable, then
$$f_{K}^\ell = g(X^p) \text{ for some } g \in K[X].$$

Additional remark: Not every coeff. of $g$ is a power of $p$.

Say $a \in K$ such a coefficient, $a$ is not of the form $\text{Frob}(b) = b^p$. $\Rightarrow$ Frob is not surjective!!
Assume every finite extension \( L/K \) is separable.

**Goal:** Prove \( \text{Frob}: K \rightarrow K \) is surjective.
\[
x \mapsto x^p
\]

Suppose not surjective: Take \( \alpha \in K \), \( \alpha \notin \text{Im}(\text{Frob}) \).

Consider the polynomial
\[
f = X^p - \alpha \in K[x].
\]

Take \( x \in \bar{K} \) a root of \( f \). Then
\[
f_x^* | f = (X - \sqrt[p]{\alpha})^p \in K[x].
\]

\[\Rightarrow f_x^* \text{ is separable } \iff f_x^* = X - \sqrt[p]{\alpha} \in K[x]. \]
\[\Rightarrow \sqrt[p]{\alpha} \in K. \quad \square\]
§ Primitive Elements.

**Def** | L/K finite, \( \alpha \in L \) is primitive if \( L = K(\alpha) \).

Then A | L/K finite separable \( \Rightarrow \exists \alpha \in L \quad L = K(\alpha) \).

Then B | L/K finite. TFAE:
- \( (i) \exists \alpha \in L \quad L = K(\alpha) \).
- \( (ii) \sum K \subseteq E \subseteq L \) E intermediate field \( \forall \beta < \infty \).

---

Proof of Thm A | Let L/K be finite separable.

To prove \( \exists \alpha \in L \quad L = K(\alpha) \).

Know : \( L = K(\alpha_1, \ldots, \alpha_n) \) for \( \alpha_1, \ldots, \alpha_n \in L \).

Enough to the case \( n = 2 \):

So | Enough to prove \( \forall L/K \) finite separ., \( L = K(\alpha, \beta) \),
- \( \exists \gamma \in L \) such that \( L = K(\gamma) \).

May assume \( K \) (and thus \( L \)) infinite.

Let's consider \( \gamma = \alpha + \lambda \cdot \beta \) for \( \lambda \in K \).

Goal : For well-chosen \( \lambda \), we have \( L = K(\gamma) \).

Know \( [L : K]_S = [L : K] = n \).

So there are \( n \) different morphisms \( \sigma_i : L \rightarrow K \).
Idea: Look at the restrictions \( \delta_i \mid_{K(f)} \).

If we can show that these restrictions are all different, then we win:

\[
\eta \leq [K(f) : K] \leq [K(g) : K] \leq [L : K] = n
\Rightarrow K(f) = L.
\]

To show (\(*\)), it is enough that \( \forall i \neq j \, \delta_i(f) \neq \delta_j(f) \)

Define

\[
0 \neq \hat{t} = \prod_{i \neq j} \left( \sigma_i(\alpha) + \chi \frac{\sigma_j(\alpha)}{\alpha} - \frac{\sigma_j(\alpha)}{\chi} \sigma_i(\alpha) + \chi \sigma_j(\alpha) \right).
\]

As \( K \) is infinite, we cannot have \( \hat{t}(\lambda) = 0 \) for all \( \lambda \in K \).

\[ \rightarrow \exists \lambda \in K \text{ such that } \hat{t}(\lambda) \neq 0. \]

Then, as \( \hat{t}(\lambda) \neq 0 \), get

\[(***) \quad \sigma_i(\alpha + \lambda \beta) \neq \sigma_j(\alpha + \lambda \beta) \quad \forall i \neq j \quad (i \neq j).\]

\[(***) \text{ means that } \frac{\sigma_i}{\sigma_j} = \alpha + \lambda \beta \text{ we have } \]

\[
\sigma_i \mid_{K(f)} \neq \sigma_j \mid_{K(f)} \quad \forall i \neq j \quad (i \neq j). \]
Then $L/K$ finite. TFAE:

(i) $\exists \alpha \in L \quad L = K(\alpha)$.
(ii) $\exists K \subset E \subset L$ $E$ intermediate fields $\exists f < \infty$.

Proof of Theorem B

$(i) \Rightarrow (ii)$ $L = K(\alpha)$. Let $E$ be an int. field, so $K \subset E \subset L$.

Consider $f^\alpha = f_{K}^\alpha \in K[x]$.

$\quad f_{E}^\alpha \in E[x]$.

Have $f_{E}^\alpha \mid f_{K}^\alpha \in E[x]$.

$\uparrow \quad \uparrow$ need not be irreducible in $E[x]$ (irred. in $E[x]$).

Consider $E_0 = \text{subfield of } E$ generated by the coeff of $f_{E}^\alpha$ and $K$.

Have $K \subset E_0 \subset E \subset L$.

Have $f_{E}^\alpha \in E_0[x]$. (and $f_{E}^\alpha$ is irred. in $E_0[x]$)
Furthermore \( L = K(\alpha) = E_0(\alpha) \).

As \( f^\alpha_E \) is irreducible, we find that

\[
[E_0(\alpha) : E_0] = \deg(f^\alpha_E) = [E(\alpha) : E].
\]

Tower law: \([E : E_0] = 1\). Hence \( E_0 = E \).

\( \implies \) Can only be finitely many different \( f \mid f^\alpha_k \in \mathbb{K}[x] \).

\( \implies \) Only finitely many \( E \). \( \Box \\

(\overset{\text{UT}}{\mapsto}) \Rightarrow (E) \).

Assume \( \exists \{E \mid K \leq E \leq L \text{ subfield} \} < \infty \).

To prove \( \exists f \in L \quad L = K(f) \).

As before: WLOG - \( K \) is infinite.

\( \implies L = K(\alpha, \beta) \)

Consider

\[ E_\lambda := K(\alpha + \lambda \beta) \quad \lambda \in K. \]

Have \( K \leq E_\lambda \leq L \), \( \lambda \) infinite.

There are infinitely many \( E_\lambda \) \((\lambda \in K)\)

\( \implies \exists \lambda \neq \lambda' \quad E_\lambda = E_{\lambda'} \).
\[ \Rightarrow \alpha + \lambda' \beta \in K(\alpha + \lambda \beta). \]
\[ \Rightarrow (\alpha + \lambda' \beta) - (\alpha + \lambda \beta) \in K(\alpha + \lambda \beta) \]
\[ (\lambda' - \lambda) \beta \in K(\alpha + \lambda \beta) \]
\[ \Rightarrow \beta \in K(\alpha + \lambda \beta) \]
\[ \Rightarrow \alpha \in K(\alpha + \lambda \beta) \]
\[ \Rightarrow K(\alpha, \beta) \subseteq K(\alpha + \lambda \beta) \]
\[ \subseteq : \quad K(\alpha + \lambda \beta) = K(\alpha, \beta). \]
\[ K(\alpha + \lambda \beta) \]
\[ \Rightarrow \beta \in K(\alpha + \lambda \beta) \]
§ Normal extensions

**Def** Decomposition field of a polynomial

**Def** Normal extensions.

**Thm** L/K finite. TFAE:

(i) L/K normal

(ii) $L = \Omega_1$ for some $f \in K[X]$

(iii) $\forall \sigma, \tau \in \Omega(L/K) \quad \sigma(L) = \tau(L) \subset \bar{K}$.

**Def** Normal closure.
\[ \text{Norm and trace} \]

**Def**: Norm and trace for $L/K$ finite and separable.

- Check basic properties, such as $N_{L/K}(x) \in K$, $Tr_{L/K}(x) \in K$.
- And compute $N_{L/K}(x)$ in case $L = K(\alpha)$. $Tr_{L/K}(x)$