MATH200C, LECTURE 3

GOLSEFIDY

Perfect fields.

Lemma 1.  (1) $f(x) \in F[x]$ does not have multiple zeros if and only if

$$\gcd(f(x), f'(x)) = 1.$$

(2) Suppose $f(x)$ is irreducible in $F[x]$. Then there is an irreducible separable polynomial $g(x) \in F[x]$ and a positive integer $k$ such that $f(x) = g(x^k)$ where

$$p = \begin{cases} \text{char}(F) & \text{if char}(F) \neq 0, \\ 1 & \text{otherwise}. \end{cases}$$

In particular, if char($F$) = 0, then any polynomial in $F[x]$ is separable.

Proof. (1) Suppose $\overline{F}$ is an algebraic closure of $F$. As we proved in the previous lecture, $\gcd(f(x), f'(x))$ over $F$ is the same as $\gcd(f(x), f'(x))$ over $\overline{F}$. So we consider $f(x)$ over $\overline{F}$. Then $f(x) = \prod_{i=1}^{n}(x - \alpha_i)^{m_i}$ for some distinct elements $\alpha_i$ of $\overline{F}$. Based on the product theorem, we have

$$f'(x) = \sum_{i=1}^{n} m_i \prod_{j \neq i}(x - \alpha_j)^{m_j} (x - \alpha_i)^{m_i - 1} = \left( \prod_{i=1}^{n} (x - \alpha_i)^{m_i - 1} \right) \left( \sum_{i=1}^{n} m_i \prod_{j \neq i}(x - \alpha_j)^{m_j} \right).$$

Notice that $g(\alpha_i) = m_i \prod_{j \neq i}(\alpha_i - \alpha_j) \neq 0$; therefore $\gcd(f, g) = 1$. Hence

$$\gcd(f, f') = \prod_{i=1}^{n} (x - \alpha_i)^{m_i - 1}.$$

Thus $\gcd(f, f') = 1$ if and only if $m_i = 1$ for any $i$; and claim follows.

(2) If $f(x)$ is separable, we let $k = 0$ and $g(x) = f(x)$. So assume $f(x)$ is not separable. Since $f(x)$ is irreducible, it means that $f(x)$ has multiple zeros. Hence by the first part, $\gcd(f, f') \neq 1$. Since $f(x)$ is irreducible, it means $\gcd(f, f') = f$. As $\deg f' < \deg f$ and $f \mid f'$, we deduce that $f' = 0$. Suppose $f(x) = \sum_{i=0}^{n} a_i x^i$; $f' = 0$ implies that $ia_i = 0$ for any $i$. If char($F$) = 0, then $ia_i = 0$ implies $a_i = 0$
for \( i \neq 0 \); this means \( f(x) \) is a constant which contradicts the assumption that \( f(x) \) is irreducible.

Next we assume that \( \text{char}(F) = p > 0 \). Then \( ia_i = 0 \) implies \( a_i = 0 \) when \( p \nmid i \).

Hence \( f(x) = g_1(x^p) \) for some \( g_1(x) \in F[x] \).

**Claim.** \( g_1(x) \) is irreducible in \( F[x] \).

**Proof of Claim.** Suppose to the contrary that \( g_1(x) = h_1(x)h_2(x) \) and \( \deg h_i > 0 \). Then \( f(x) = h_1(x^p)h_2(x^p) \), which contradicts the assumption that \( f(x) \) is irreducible in \( F[x] \).

By the strong induction hypothesis, there is a separable irreducible polynomial \( g(x) \in F[x] \) such that \( g_1(x) = g(x^{p^k}) \). Hence

\[
f(x) = g_1(x^p) = g((x^p)^{p^k}) = g(x^{p^{k+1}}).
\]

\( \Box \)

**Theorem 2.** Suppose \( F \) is a field and \( \overline{F} \) is an algebraic closure of \( F \). Then the following statements are equivalent.

1. Either \( \text{char}(F) = 0 \), or \( \text{char}(F) = p > 0 \) and \( F^p = F \).
2. \( \overline{F}/F \) is a Galois group.
3. Any algebraic extension \( E/F \) is separable.

**Proof.** (1)\( \Rightarrow \)(2) The assumption \( F^p = F \) implies that \( \sigma : F \to F, \sigma(a) := a^p \) is an automorphism of \( F \). Hence \( \sigma^k \in \text{Aut}(F) \); and so for any \( a \in F \), there is \( a' \in F \) such that \( (a')^{p^k} = a \).

Since \( \overline{F}/F \) is a normal extension, to show it is a Galois extension it is enough to prove that it is a separable extension. For \( \alpha \in \overline{F} \), since \( m_{\alpha,F}(x) \) is irreducible in \( F[x] \) by the previous lemma, there is a separable polynomial \( g(x) \in F[x] \) such that \( m_{\alpha,F}(x) = g(x^{p^k}) \). Suppose \( g(x) = \sum_{i=0}^n a_i x^i \). By the above comment, there are \( a'_i \in F \) such that \( (a'_i)^{p^k} = a_i \). Thus

\[
m_{\alpha,F}(x) = \sum_{i=0}^n a_i x^{ip^k} = \sum_{i=0}^n (a'_i)^{p^k} x^{ip^k} = (\sum_{i=0}^n a'_i x^i)^{p^k}.
\]

As \( m_{\alpha,F}(x) \) is irreducible in \( F[x] \) and \( \sum_{i=0}^n a'_i x^i \in F[x] \), we have \( p^k = 1 \). Hence \( m_{\alpha,F}(x) = g(x) \) is separable; and claim follows.

(2)\( \Rightarrow \)(3) Since \( E/F \) is algebraic, \( E \) can be embedded into \( \overline{F} \). Since \( \overline{F}/F \) is separable, we deduce that \( E/F \) is separable.
(3) ⇒ (1) (In the midst of questions, I forgot to prove this during lecture.) If char(F) = 0, there is nothing to prove. So we assume that char(F) = p > 0. For a ∈ F, let α ∈ F be a zero of xp − a = 0. Hence \( m_{α,F}(x)|x^p − α = x^p − α^p = (x − α)^p \). Since \( F/F \) is separable, \( m_{α,F}(x) \) does not have multiple zeros. Hence \( m_{α,F}(x) = x − α \), which implies \( α ∈ F \); and so \( a = α^p ∈ F^p \). This implies that \( F^p = F \).

A field is called perfect if it satisfies the above properties.

**Galois group of finite fields**

Suppose \( \mathbb{F}_p \) is an algebraic closure of \( \mathbb{F}_p \). Let’s recall that we can identify \( \mathbb{F}_{p^d} \) with \( \{ α ∈ \mathbb{F}_p | α^{pd} = α \} \) and \( \mathbb{F}_p = \bigcup_{d ∈ \mathbb{Z}_+} \mathbb{F}_{p^d} \). As \( \mathbb{F}_p = \mathbb{F}_p, \mathbb{F}_p \) is a perfect field. Hence \( \mathbb{F}_p/\mathbb{F}_p \) is a Galois extension. Notice that \( σ : \mathbb{F}_p → \mathbb{F}_p, σ(α) := α^p \) is an embedding and, since \( x^p − α \) has a zero in \( \mathbb{F}_p, σ \) is onto. Hence \( σ ∈ \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \).

We know that \( \mathbb{F}_{p^d} \) is a splitting field of \( xp^d − x \) over \( \mathbb{F}_p \). Hence \( \mathbb{F}_{p^d}/\mathbb{F}_p \) is a normal extension. Since \( \mathbb{F}_p \) is a perfect field, \( \mathbb{F}_{p^d}/\mathbb{F}_p \) is a separable extension. Hence \( \mathbb{F}_{p^d}/\mathbb{F}_p \) is a Galois extension. Hence \( |\text{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p)| = |\mathbb{F}_{p^d} : \mathbb{F}_p| = d \).

Since \( \mathbb{F}_{p^d}/\mathbb{F}_p \) is a normal extension, \( σ_d := σ|_{\mathbb{F}_{p^d}} \) is in \( \text{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \). Notice that \( σ_d^d(α) = α^{pd} = α \) for any \( α ∈ \mathbb{F}_{p^d} \). Hence \( σ_d^d = \text{id} \); and so \( o(σ_d)|d \). Suppose \( o(σ_d) =: d' \). Then for any \( α ∈ \mathbb{F}_{p^d} \), we have \( α = σ_d^d(α) = α^{pd'} \). And so any element of \( \mathbb{F}_{p^d} \) is a zero of \( xp^{d'} − x \). Therefore \( p^d ≤ \text{deg}(xp^{d'} − x) = p^{d'} \), which implies that \( d ≤ d' \). As \( d'|d \) and \( d ≤ d' \), we deduce that \( d = d' \). Hence

\[ \text{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) = \langle σ_d \rangle ∼ \mathbb{Z}/d\mathbb{Z}. \]

This implies that \( \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) ∼ \varprojlim \mathbb{Z}/d\mathbb{Z} \); and in your HW assignment you have seen how this can help you to show \( \mathbb{F}_p \) does not have a non-trivial subfield \( E \) such that \( \mathbb{F}_p : E < ∞ \).

The following remarks were mentioned in the lecture in response to your questions. I am including proof of some of them here.

**Question.** Is \( \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) = \langle σ \rangle ^? \) No, \( \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \) is a very large compact group; in particular it is not countable. \( \langle σ \rangle \) is, however, dense in \( \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \). Notice that \( \varprojlim \mathbb{Z}/d\mathbb{Z} \) is a closed subgroup of \( \prod d \mathbb{Z}/d\mathbb{Z} \); open sets in the product topology are of the form \( X × \prod_{d ∈ S} \mathbb{Z}/d\mathbb{Z} \) where \( S \) is a finite subset of \( \mathbb{Z}_+ \) and \( X \) is a subset of \( \prod_{d ∈ S} \mathbb{Z}/d\mathbb{Z} \), and under the above isomorphism \( σ \) is sent to \( 1 := \{ 1 + d\mathbb{Z} \}_d ∈ \prod_d \mathbb{Z}/d\mathbb{Z} \). If \( \{ x_d + d\mathbb{Z} \}_d ∈ (\varprojlim \mathbb{Z}/d\mathbb{Z}) ∩ (X × \prod_{d ∈ S} \mathbb{Z}/d\mathbb{Z}) \), then
\[ x_n \equiv x_d \pmod{d} \text{ for any } d \in S \text{ where } n := \prod_{d \in S} d. \text{ Hence} \]
\[ x_n \mathbb{I} = \{x_n + d\mathbb{Z}\}_d \in X \times \left( \prod_{d \in S} \mathbb{Z}/d\mathbb{Z} \right) ; \]

this means \( \mathbb{I} \) intersects any non-empty open subset of \( \varprojlim \mathbb{Z}/d\mathbb{Z} \); and so \( \mathbb{I} \) is dense in \( \varprojlim \mathbb{Z}/d\mathbb{Z} \). Hence \( \langle \sigma \rangle \) is dense in \( \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \).

**Question.** What is the topology on \( \text{Gal}(\overline{F}/F) \)? Let’s recall that

\[ \theta : \text{Gal}(\overline{F}/F) \to \varprojlim_{E} \text{Gal}(E/F), \theta(\sigma) := \{\sigma|_E\}_E \]

is an isomorphism where \( \varprojlim_{E} \text{Gal}(E/F) \) is equal to

\[ \{\{\sigma_E\}_E \in \prod_{E} \text{Gal}(E/F)/|E/F \text{ is finite Galois;} E \subseteq E' \text{ implies } \sigma_{E'}|_E = \sigma_E \}. \]

We consider the discrete topology on finite groups \( \text{Gal}(E/F) \); and by Tychonoff’s theorem \( \prod_{E} \text{Gal}(E/F) \) is a compact group. One can check that \( \varprojlim_{E} \text{Gal}(E/F) \) is a closed subgroup of \( \prod_{E} \text{Gal}(E/F) \); and so it is a compact group. An open subset of \( \prod_{E} \text{Gal}(E/F) \) is of the form \( X \times \prod_{E \notin S} \text{Gal}(E/F) \) where \( S = \{E_1, \ldots, E_n\} \) is a finite set consisting of some finite Galois extensions of \( F \). And so the collections sets of the form \( \prod_{E \in S} \{\text{id}_E\} \times \prod_{E \notin S} \text{Gal}(E/F) \) make a basis for neighborhoods of the identity. Notice that there is a finite Galois extension \( E' \) of \( F \) such that \( \bigcup_{i=1}^{n} E_i \subseteq E' \). And so

\[ \theta^{-1}((\prod_{E \in S} \{\text{id}_E\} \times \prod_{E \notin S} \text{Gal}(E/F)) \cap \varprojlim_{E} \text{Gal}(E/F)) \supseteq \{\sigma \in \text{Gal}(\overline{F}/F)|\sigma|_E = \text{id}_E\} ; \]

and \( \theta(\{\sigma \in \text{Gal}(\overline{F}/F)|\sigma|_E = \text{id}_E\}) \) is an open subset of \( \varprojlim \text{Gal}(E/F) \). So overall we get that \{ker \( r_E \)\}_E forms a basis of neighborhoods of the identity of \( \text{Gal}(\overline{F}/F) \) where \( E \) runs over finite Galois extensions of \( F \) and

\[ r_E : \text{Gal}(\overline{F}/F) \to \text{Gal}(E/F), r_E(\sigma) := \sigma|_E \]

is the restriction map.

**Question.** Is any subfield of \( \mathbb{F}_p \) finite? No, \( \mathbb{F}_p \) has many infinite subfields. In fact, similar to the finite Galois extensions, we can understand intermediate subfields of \( E/F \) using subgroups of \( \text{Gal}(E/F) \). In the infinite Galois extension case, however, we have to restrict ourselves to closed subgroups: there is a bijection between intermediate subfields of \( E/F \) and closed subgroups of \( \text{Gal}(E/F) \).
For instance, one can check that
\[ E_2 := \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n} \]
is a subfield of \( \mathbb{F}_p \); and one has
\[ \text{Gal}(E_2/\mathbb{F}_p) \simeq \lim_{\to} \mathbb{Z}/2^n\mathbb{Z} =: \mathbb{Z}_2; \]
is the group of 2-adic integers. (This can be regarded as a definition for this group.)

**Cyclotomic extensions**

Suppose either \( \text{char}(F) \) is either 0, or \( \text{char}(F) = p > 0 \) and \( p \nmid n \). Let \( E \) be a splitting field of \( x^n - 1 \) over \( F \). Since \( E \) is a splitting field over \( F \), \( E/F \) is a normal extension. If \( \text{char}(F) = 0 \), \( E/F \) is separable. Suppose \( \text{char}(F) = p > 0 \). Since \( p \nmid n \), \( nx^{n-1} \) is not zero. Since 0 is not a zero of \( x^n - 1 \) and \( nx^{n-1} \neq 0 \), \( \gcd(x^n - 1, nx^{n-1}) = 1 \). Hence all the zeros of \( x^n - 1 \) are distinct in \( E \). Thus \( E/F \) is separable, and \( \mu_n := \{ \zeta \in E^\times | \zeta^n = 1 \} \) has \( n \) elements. Notice that for any positive integer \( d \) we have \( |\{ \zeta \in \mu_n | \zeta^d = 1 \} | \leq d \); and so \( \mu_n \) is a cyclic group of order \( n \). Thus there is \( \zeta_n \in E^\times \) such that
\[ \mu_n = \{ 1, \zeta_n, \ldots, \zeta_n^{n-1} \} \simeq \mathbb{Z}/n\mathbb{Z}. \]

Overall we have that \( E = F[1, \zeta_n, \ldots, \zeta_n^{n-1}] = F[\zeta_n] \) is a Galois extension of \( F \). For any \( \sigma \in \text{Gal}(E/F) \), \( \sigma \) is uniquely determined by \( \sigma(\zeta_n) \) as \( E = F[\zeta_n] \). Since \( \sigma(\zeta_n) \) is a zero of \( x^n - 1 \), \( \sigma(\zeta_n) \in \mu_n \); that means \( \sigma(\zeta_n) = \zeta_n^a \) for some \( a \in \{0, \ldots, n-1\} \). As \( \sigma \) is an automorphism, the multiplicative order of \( \zeta_n \) is equal to the multiplicative order of \( \sigma(\zeta_n) = \zeta_n^a \); hence
\[ n = o(\zeta_n) = o(\sigma(\zeta_n)) = o(\zeta_n^a) = o(\zeta_n)/\gcd(o(\zeta_n), a) = n/\gcd(n, a), \]
which implies that \( \gcd(a, n) = 1 \). Let \( \theta : \text{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times, \theta(\sigma) := a_\sigma + n\mathbb{Z} \)
where \( \sigma(\zeta_n) = \zeta_n^{a_\sigma} \).

**Claim.** \( \theta \) is a group homomorphism.

**Proof of Claim.** We have
\[ \zeta_n^{a_{\sigma_1 \circ \sigma_2}} = (\sigma_1 \circ \sigma_2)(\zeta_n) = \sigma_1(\zeta_n^{a_{\sigma_2}}) = \sigma_1(\zeta_n)^{a_{\sigma_2}} = (\zeta_n^{a_{\sigma_1}})^{a_{\sigma_2}} = \zeta_n^{a_{\sigma_1} + a_{\sigma_2}}. \]

Hence \( a_{\sigma_1 \circ \sigma_2} \equiv a_{\sigma_1} a_{\sigma_2} \) (mod \( n \)). Hence \( \theta(\sigma_1 \circ \sigma_2) = \theta(\sigma_1) \theta(\sigma_2) \). We also notice that \( \theta(\text{id}_E) = 1 \) and so claim follows.
Claim. \( \theta \) is injective.

Proof of Claim. This is immediate as \( \sigma \) is uniquely determined by \( \sigma(\zeta_n) \) and \( \sigma(\zeta_n) \) is uniquely determined by \( \theta(\sigma) = a_\sigma \mod n \).

Overall we get the following result.

Proposition 3. Suppose either \( \text{char}(F) = 0 \), or \( \text{char}(F) = p > 0 \) and \( p \nmid n \). Let \( E \) be a splitting field of \( x^n - 1 \) over \( F \). Then \( E/F \) is Galois and \( \text{Gal}(E/F) \) can be embedded into \((\mathbb{Z}/n\mathbb{Z})^\times\).

Next we want to show that the above mentioned \( \theta \) is an isomorphism when \( F = \mathbb{Q} \). To motivate our next definition, we start with the following lemma.

Lemma 4. (1) Suppose \( E/F \) is a finite Galois extension. For \( \alpha \in E \), let 
\[ f_\alpha(x) := \prod_{\sigma \in \text{Gal}(E/F)} (x - \sigma(\alpha)). \]
Then \( f_\alpha(x) \in F[x] \) and \( m_{\alpha,F}(x) \mid f_\alpha(x) \).

(2) Suppose \( F[\alpha] \) is a finite Galois extension of \( F \). Then \( f_\alpha(x) = m_{\alpha,F}(x) \).

Proof. (1) For any \( \tau \in \text{Gal}(E/F) \),
\[ \tau(f_\alpha(x)) = \prod_{\sigma \in \text{Gal}(E/F)} (x - \tau(\sigma(\alpha))) = \prod_{\sigma \in \text{Gal}(E/F)} (x - \sigma(\alpha)) = f_\alpha(x). \]
Hence \( f_\alpha(x) \in \text{Fix}(\text{Gal}(E/F))[x] = F[x] \). As \( f_\alpha(\alpha) = 0 \), we deduce that \( m_{\alpha,F}(x) \mid f_\alpha(x) \).

(2) We have that \( \text{deg } f_\alpha(x) = |\text{Gal}(E/F)| = |E : F| = [F[\alpha] : F] = \text{deg } m_{\alpha,F}(x) \); and claim follows using part (1).

So if \( \theta \) is an isomorphism, then \( m_{\zeta_n,\mathbb{Q}}(x) \) is equal to \( \prod_{1 \leq a \leq n, \gcd(a,n) = 1} (x - \zeta_n^a) \).

We let
\[ \Phi_n(x) := \prod_{1 \leq a \leq n, \gcd(a,n) = 1} (x - \zeta_n^a) \in \mathbb{C}[x] \]
where \( \zeta_n := e^{2\pi i/n} \); and it is called the \( n \)-th cyclotomic polynomial. In the next lecture we will prove that \( \Phi_n(x) \) is in \( \mathbb{Z}[x] \) and it is irreducible in \( \mathbb{Q}[x] \). Using this, we will deduce that \( \text{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \).