Title

D. Zack Garza

January 6, 2020

Contents

1 Fields

Let k denote a field.

Lemmas:

- The characteristic of $\mathbb{F}$ is either 0 or p a prime.
- All fields are simple rings
- Any homomorphism of fields is either 0 or injective
- If L/k is algebraic, then $\min(\alpha, L)$ divides $\min(\alpha, k)$.

Lemma: Every finite extension is algebraic.

Eisenstein's Criterion: If $f(x) = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{Q}[x]$ and $\exists p$ such that

- p divides every coefficient *except* a_n and
- p^2 does not divide a_0,

then f is irreducible.

Definition: For R a UFD, a polynomial $p \in R[x]$ is **primitive** iff the greatest common divisors of its coefficients is a unit.

Gauss' Lemma: Let R be a UFD and F its field of fractions. Then a primitive $p \in R[x]$ is irreducible in $R[x] \iff p$ is irreducible in $F[x]$.

Corollary: A primitive polynomial $p \in \mathbb{Q}[x]$ is irreducible iff p is irreducible in $\mathbb{Z}[x]$.

1.1 Finite Fields

Lemma: If char $k = p$ then $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$.

Theorem: $\mathbb{GF}(p^n) \cong \dfrac{\mathbb{F}_p}{(f)}$ where $f \in \mathbb{F}_p[x]$ is any irreducible of degree n, and $\mathbb{GF}(p^n) \cong \mathbb{F}[\alpha] \cong \operatorname{span}_{\mathbb{F}} \left\{1, \alpha, \cdots, \alpha^{n-1}\right\}$ for any root α of f.

Lemma: $\mathbb{GF}(p^n)$ is the splitting field of $x^{p^n} - x$.

> Every element is a root by Cauchy's theorem, and the p^n roots are distinct since its derivative is identically -1.

Lemma: Let $\rho_n := x^{p^n} - x$. Then $f(x) \,\Big|\, \rho_n(x) \iff \deg f \,\Big|\, n$ and f is irreducible.

Lemma: $x^{p^n} - x = \prod f_i(x)$ over all irreducible monic $f_i \in \mathbb{F}_p[x]$ of degree d dividing n.

> *Proof:*
> $\Longleftarrow:$
> Suppose f is irreducible of degree d. Then $f \,\Big|\, x^{p^d} - x$ (consider $F[x]/\langle f \rangle$) and $x^{p^d} - x \,\Big|\, x^{p^n} - x \iff d \,\Big|\, n$.
> $\Longrightarrow:$
>
> - $\alpha \in \mathbb{GF}(p^n) \iff \alpha^{p^n} - \alpha = 0$, so every element is a root of ϕ_n and $\deg \min(\alpha, \mathbb{F}_p) \,\Big|\, n$ since $\mathbb{F}_p(\alpha)$ is an intermediate extension.
> - So if f is an irreducible factor of ϕ_n, f is the minimal polynomial of some root α of ϕ_n, so $\deg f \,\Big|\, n$.
>
> $\phi_n'(x) = p^n x^{p^{n-1}} \neq 0$, so ϕ_n has distinct roots and thus no repeated factors. So ϕ_n is the product of all such irreducible f.

1.2 Galois Theory

Definition: A field extension L/k is **algebraic** iff every $\alpha \in L$ is the root of some polynomial $f \in k[x]$.

Definition: Let L/k be a finite extension. Then TFAE:

- L/k is **normal**.
- Every irreducible $f \in k[x]$ that has one root in L has *all* of its roots in L
  - i.e. every polynomial splits into linear factors
- Every embedding $\sigma : L \hookrightarrow \overline{k}$ that is a lift of the identity on k satisfies $\sigma(L) = L$.
- If L is separable: L is the splitting field of some irreducible $f \in k[x]$.

Definition: Let L/k be a field extension, $\alpha \in L$ be arbitrary, and $f(x) := \min(\alpha, k)$. TFAE:

- L/k is **separable**
- f has no repeated factors/roots
- $\gcd(f, f') = 1$, i.e. f is coprime to its derivative
- $f' \not\equiv 0$

> **Lemma:** If char $k = 0$ or k is finite, then every *algebraic* extension L/k is separable.

Definition: $\operatorname{Aut}(L/k) = \left\{ \sigma : L \to L \;\middle|\; \sigma|_k = \mathrm{id}_k \right\}$.

Lemma: If L/k is algebraic, then $\operatorname{Aut}(L/k)$ permutes the roots of irreducible polynomials.

Lemma: $|\operatorname{Aut}(L/k)| \leq [L : k]$ with equality precisely when L/k is normal.

Definition: If L/k is Galois, we define $\operatorname{Gal}(L/k) \coloneqq \operatorname{Aut}(L/k)$.

Lemmas about towers: Let $L/F/k$ be a finite tower of field extensions

- Multiplicativity: $[L : k] = [L : F][F : k]$
- L/k normal/algebraic/Galois $\implies$ L/F normal/algebraic/Galois.
  - *Proof (normal):* $\min(\alpha, F) \;\Big|\; \min(\alpha, k)$, so if the latter splits in L then so does the former.
  - *Corollary:* $\alpha \in L$ algebraic over $k \implies \alpha$ algebraic over F.

$$\begin{tikzcd}
L \arrow[d, dotted, bend right] \arrow[dd, bend left] \\
F \\
k
\end{tikzcd}$$

- F/k algebraic and L/F algebraic $\implies$ L/k algebraic.

$$\begin{tikzcd}
L \arrow[d, bend right] \arrow[dd, dashed, bend left] \\
F \arrow[d, bend right] \\
k
\end{tikzcd}$$

- F/k Galois and L/K Galois $\implies$ F/k Galois **only if** $\operatorname{Gal}(L/F) \trianglelefteq \operatorname{Gal}(L/k)$
  - $\implies \operatorname{Gal}(F/k) \cong \dfrac{\operatorname{Gal}(L/k)}{\operatorname{Gal}(L/F)}$

$$\begin{tikzcd}
L \arrow[d, dotted, bend right] \arrow[dd, bend left] \\
F \arrow[d, bend right] \\
k
\end{tikzcd}$$

- E, F normal over $k \implies EF, E \bigcap F$ normal over k.

Common Counterexamples:

- $\mathbb{Q}(\zeta_3, 2^{1/3})$ is normal but $\mathbb{Q}(2^{1/3})$ is not since the irreducible polynomial $x^3 - 2$ has only one root in it.

Definition (Characterizations of Galois Extensions): Let L/k be a finite field extension. TFAE:

- L/k is **Galois**
- L/k is finite, normal, and separable.
- L/k is the splitting field of a separable polynomial
- $|\mathrm{Aut}(L/k)| = [L:k]$
- The fixed field of $\mathrm{Aut}(L/k)$ is exactly k.

Fundamental Theorem of Galois Theory: Let L/k be a Galois extension, then there is a correspondence:

$$\left\{ \text{Subgroups } H \leq \mathrm{Gal}(L/k) \right\} \iff \left\{ \substack{\text{Fields } F \text{ such} \\ \text{that } L/F/k} \right\}$$
$$H \to \left\{ \text{The subfield fixed by } H \right\}$$
$$\left\{ \sigma \in \mathrm{Gal}(L/k) \;\middle|\; \sigma(F) = F \right\} \leftarrow F.$$

- This is contravariant wrt subgroups/subfields.
- $[F:k] = [G:H]$, so degrees of extensions over the base field correspond to indices of subgroups.
- $[K:F] = |H|$
- L/F is Galois and $Gal(K/F) = H$
- F/k is Galois $\iff$ H is normal, and $\mathrm{Gal}(F/k) = \mathrm{Gal}(L/k)/H$.
- The compositum F_1F_2 corresponds to $H_1 \bigcap H_2$.
- The subfield $F_1 \bigcap F_2$ corresponds to H_1H_2.

1.2.1 Examples

1. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/(n)^\times$ and is generated by maps of the form $\zeta_n \mapsto \zeta_n^j$ where $(j, n) = 1$.

   I.e., the following map is an isomorphism:

$$\begin{aligned} \mathbb{Z}/(n)^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q}) \\ r \mod n &\mapsto (\phi_r : \zeta_n \mapsto \zeta_n^r). \end{aligned}$$

2. $\mathrm{Gal}(\mathbb{GF}(p^n)/\mathbb{F}_p) \cong \mathbb{Z}/(n)$, a cyclic group generated by powers of the Frobenius automorphism:

$$\begin{aligned} \varphi_p : \mathbb{GF}(p^n) &\to \mathbb{GF}(p^n) \\ x &\mapsto x^p. \end{aligned}$$

Theorem: Every quadratic extension is Galois.

Definition: TFAE

- k is a **perfect** field.
- Every irreducible polynomial $p \in k[x]$ is separable
- Every finite extension F/k is separable.
- If char $k > 0$, the Frobenius is an automorphism of k.

Theorem:

- If char $k = 0$ or k is finite, then k is perfect.

- $k = \mathbb{Q}, \mathbb{F}_p$ are perfect, and any finite normal extension is Galois.
- Every splitting field of a polynomial over a perfect field is Galois.

1.3 Cyclotomic Polynomials

Definition: Let $\zeta_n = e^{2\pi i/n}$, then

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (j,n)=1}}^{n} \left(x - \zeta_n^k\right),$$

which is a product over primitive roots of unity.

Lemma: $\deg \Phi_n(x) = \phi(n)$ for ϕ the totient function.

Computing Φ_n:

1.
$$\Phi_n(z) = \prod_{d|n, d>0} \left(z^d - 1\right)^{\mu\left(\frac{n}{d}\right)}$$

   where

$$\mu(n) \equiv \begin{cases} 0 & \text{if } n \text{ has one or more repeated prime factors} \\ 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes,} \end{cases}$$

2.
$$x^n - 1 = \prod_{d|n} \Phi_d(x) \implies \Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)},$$

   so just use polynomial long division.

Lemma:

$$\begin{aligned} \Phi_p(x) &= x^{p-1} + x^{p-2} + \cdots + x + 1 \\ \Phi_{2p}(x) &= x^{p-1} - x^{p-2} + \cdots - x + 1. \end{aligned}$$

Lemma:

$$k \mid n \implies \Phi_{nk}(x) = \Phi_n\left(x^k\right)$$

Definition: An extension F/k is **simple** if $F = k[\alpha]$ for a single element α.

Theorem (Primitive Element): If F/k is a finite separable extension, then it is simple.

Corollary: $\mathbb{GF}(p^n)$ is a simple extension over $\mathbb{F}_p$.