Math 1540

George C.

February 10, 2023

Contents

List of Theorems

Lecture 1

0 Motivation

Galois theory is a branch of mathematics that studies the connection between algebraic equations and their solutions. One of the main motivations for studying Galois theory is the Abel-Ruffini Theorem:

Theorem 1 (Abel-Rufin)**.** There exists a polynomial of degree 5 with solutions that are not expressible using algebraic operators $(+, -, \cdot, /, \sqrt[n]{\ })$

1 Classical Formulas

Polynomials of degree $[2, 4]$ have equations for their solutions. These equations are often found by reducing a polynomial using a shift: Given a polynomial:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots a_0$$

A shift will get rid of the x^{n-1} term

$$f(x - \frac{a_{n-1}}{na_n}) = a_n x^n + \dots a_0$$

Example (Quadratic Formula)**.**

$$\begin{aligned}
X^2 + bX + c = 0 \\
\text{Using a shift of } -\frac{b}{2} \text{ removes the linear term:} \\
(x - \frac{b}{2})^2 + b(x - \frac{b}{2}) + c = 0 \\
(x^2 - bx + \frac{b^2}{4}) + bx - \frac{b^2}{2} + c = 0 \\
x^2 + \frac{b^2}{4} - \frac{b^2}{2} + c = 0 \\
x^2 - \frac{b^2}{4} + c = 0 \\
x^2 = \frac{b^2}{4} - c \\
x = \pm\sqrt{\frac{b^2}{4} - c} \\
X = \pm\sqrt{\frac{b^2}{4} - c} - \frac{b}{2}
\end{aligned}$$

Lecture 2

Lecture 3

2 Splitting Fields

Lemma 1 (Euclid's Lemma). Let F be a field, if $p(x)$ divides $q_1(x)q_2(x)\dots q_n(a)$ with $p(x)$ irreducible then $p(x)$ divides one of the $q_i(x)$

> **Note.** Irreducibility is important because for example $x^2|x{\cdot}x$ but x^2 doesn't factor either

Proof. By induction:

Base Case: Let $f(x) = 1$ then, $p(x)|f(x)q_1(x)$ Trivial since there is only one polynomial for $p(x)$ to divide

Inductive Step: Let $f(x) = q_1(x)q_2(x)\dots q_n(a)$ $(p(x), f(x)) = 1$, so there exist $a(x)$ and $b(x)$ s.t. $a(x)p(x) + b(x)f(x) = 1$ Therefore,

$$p(x)a(z)q_{n+1}(x) + f(x)q_{n+1}(x)b(x) = q_{n+1}(x)p(x)|q_{n+1}(x)$$

■

Proposition 1. Let F be a field and $p(x)$ be irreducible. Then $F[x](p(x))$ is a field and contains a root to $p(x) = 0$

> **Note.** $(\forall a \in F)(p(a) \neq 0)$ since it's irreducible F is inside $F[x]/(p(x))$

Lecture 4

Definition 1 (splits). A polynomial, $f(x)$, splits in $F[x]$ iff it can be written as a product of linear factors i.e F contains all the roots of $f(x)$

Theorem 2. Let $f(x) \in F[x]$, there exists a field extension $\frac{E}{F}$ for which $f(x)$ splits

Proof. By induction:

Base Case: Trivial

Inductive Step: let $f(x)$ be deg(f) = n + 1 Write $f(x) = p(x)g(x)$ $p(x)$ irreduaclie. Find a field (B/F) for which $p(x)$ has a root $p(x) = (x-a)h(x)$then $f(x) = (x-a)h(x)g(x)$ then falls to previous case ■

> **Note.** This result is similar to the FTA

Definition 2 (prime subfield). Let F be a field, then

$$P = \bigcap_{0 \neq S \in F} S$$

P be the prime subfield of F

Theorem 3. P a prime subfield is either isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$

Lecture 5

Theorem 4 (mod p-criterion). Let R domain, F field, $s : R \to F$ be a ring map Let $p(x) \in R[x]$ if $deg(s(p)) = deg(p)$ and $s(p)$ irreducible in $F[x]$, then $p(x)$ irreducible in $R[x]$

Example. $p(x) = 8x^3 - 6x - 1$ in $\mathbb{Z}[x]$ irreducible? $s : \mathbb{Z} \to \mathbb{Z}_5$ $s(p) = 3x^3 - x - 1$ And then we can check with 5 inputs in $\mathbb{Z}_5$

Theorem 5 (Eisenstein criterion). Let $f(x) \in \mathbb{Z}[x]$

$$f(x) = a_n x^n \dots a_1 x + a_0$$

If there exists a prime p so that $p|a_i$ for $0 \leq i \leq n$ and $p^2 \not| a_0$ then $f(x)$ is irreducible over $Q[x]$

Definition 3 (splitting field). A splitting field is the smallest field extension over the field of the coefficients of a polynomial such that it contains all roots of the polynomial.

Theorem 6. Let $a \in E$ and $p(x) \in F[x]$ here $\frac{E}{F}$ $p(x)$ monic irreducible has a as a root

Lecture 6

If there exists another $q(x) \in F[x]$ with $q(a) = 0$, monic irreducible, then $(p - q)(x) = 0$ at a and $deg(p - q) < deg(p)$ which contridicts the first part.

Definition 4 (E/F as vector-space). We call the degree of $\frac{E}{F} = [E : F]$

Example. $\mathbb{Q}(\sqrt[3]{2})$ is a 3-dimentional extension

Example. $Q(\sqrt{2}, \sqrt{3})$ is 4-dimentional extension

Theorem 7. Let $p(x) \in F[x]$ be irreducible of $deg(p) = d$ then $E = F[x]/(p(x))$ is an extension of degree d

Note. E contains a root of $p(x)$, a. We should claim that an F-basis of E looks like powers of a

Definition 5 (Field Extension).

$$F(a_1 \dots a_n) = \bigcap_{F \subseteq S \subseteq E} S$$

where $a_1, \dots a_n \in S$

Definition 6 (simple). a field extension is called simple if it only adds one element

Theorem 8. E/F is a finite extension $\Rightarrow$ it's algebraic (each element $a \in E$ is algebraic)

Proof. Pick a $a \in E$ if a is a root if there's a linear combination of it's powers that equals zero ■

Theorem 9. Let E/F be field extension, $a \in E$ be algebraic over F then

1. There's a monic irreducible $p(x) \in F[x]$ having a as a root
2. There exists an isomorphism between $F[x]/(p(x)) \to F(a)$
3. $p(x)$ unique monic of the least degree in $F[x]$ with a as a root
4. $[F(a) : F] = deg(p)$

ß

Lecture 0

Proof. To show this let's define a map $\varphi : F[x] \to E$ s.t. $\varphi(f) = f(a)$. The kernel of this map would be $(p(x))$. Because E is a field then the image of phi is a domain. Since $\ker(\varphi) = (p(x))$ is prime then $2 \Rightarrow 1, 3$

Let's define another map $\tau : F[x]/(p(x)) \to img(\varphi)$. Then $img(\varphi) = F(a)$ and so $\tau(c) = c \forall c \in F$, $\tau(\bar{x}) = a$.

We know that $F(a) \subseteq img(\varphi)$, so we want to also show $F(a) \supseteq img(\varphi)$

If $F, a \subseteq S$ then all polynomials in a are in S Therefore, $F(a) \supseteq img(\varphi)$ ■

Theorem 10 (existence of splitting field)**.** We know there exists some field such that $f(x)$ splits. We can write $f(x)u(x-a_1)\dots(x-a_n)$. Then $f(x)$ must split in $S = F(a_1 \dots a_n)$

Lecture 8

Let F be a feild, $\sigma : F(\alpha_1, \dots a_n) \to F(\alpha_1 \dots a_n)$ so that $\sigma(1_F) = 1_F$ and $\sigma(a_i) \to a_i$ then $\sigma =$ identity

Definition 7 (seperable field)**.** Let $f(x) \in F[x]$ has factorization $f(x) = up_1(x) \dots p_n(x)$ We say that $f(x)$ is seqperable iff each $p_i(x)$ has no repeated toots

Let $f(x) \in F[x]$ irreducable, if $f'(x) \neq 0$ then $f(x)$ is seperable

Definition 8 (perfect)**.** A field is called perfect if every non-constant $f(x) \in F[x]$ is seperable

Example (perfect fields)**.** Fields of charteristic 0 and finite fields

Definition 9 (seperable element)**.** Let $\alpha \in E/F$, we say α is seperable if it's minimal polynomial is seperable in $F[\alpha]$

Theorem 11 (1)**.** Let $f(x) \in F[x]$, $f'(x) = \sigma'(f(x))$, E a spliting feild of $f(x)$ and E' be a spliting feild of $f'(x)$ Then

1. $\exists \hat{\sigma} : E \to E'$
2. if $f(x)$ is seperabel, then of $\hat{\sigma}$ is $[E : F]$

Corollary. Any two finite feilds of order p^n are isomorphic