MATH3345 Summary

Stanley Li

June 6, 2022

Symmetric polynomials and solubility by radicals

Definition (Symmetric polynomial): A polynomial $p(x_1, \dots, x_n)$ is *symmetric* if for every $\sigma \in S_n$,

$$p(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = p(x_1, \dots, x_n)$$

We denote the set of symmetric polynomials on a ring R in n variables $x_1, \dots, x_n$ by $R[x_1, \dots, x_n]^{S_n}$.

Definition (Elementary symmetric polynomial): Let $p(x)$ be a polynomial of degree $n \geq 1$ and with roots $\alpha_1, \dots, \alpha_n$, then the k^{th} *elementary symmetric polynomial* $e_k(\alpha_1, \dots, \alpha_n)$ is given by

$$e_k(\alpha_1, \dots, \alpha_n) = \sum_{\substack{S \subseteq \{1, \dots, n\} \\ |S| = k}} \prod_{i \in S} \alpha_i$$

In this case, if $p(x) = c_0 x^n + c_1 x^{n-1} + \dots + c_n$, then

$$\frac{c_i}{c_0} = (-1)^i e_i(\alpha_1, \dots, \alpha_n)$$

If p is monic (with $c_0 = 1$), this reduces to a formula for the coefficients solely in terms of symmetric polynomials.

Proposition (Solubility by radicals): Polynomials of degree $n \leq 4$ are soluble by radicals in the respective rings.

For polynomials of the form $x^n + c_1 x^{n-1} + \dots + c_n$, we can write $x = -c_1$ when $n = 1$, $x = \frac{-c_1 \pm \sqrt{c_1^2 - 4c_2}}{2}$ when $n = 2$.

For higher degree polynomials, there are telegraphed processes as given in lecture 1, assignment 1 and workshop 1.

In these cases, we also consider polynomials to be in the formal variables α_i (which bear resemblence to the roots of polynomials)

Definition (Orbit sum): Let $p(\alpha_1, \dots, \alpha_n) = \alpha_1^{r_1} \alpha_2^{r_2} \dots a_n^{r_n}$ be a monomial. The *orbit sum* of p is the sum of all elements in the set $X_p = \{\alpha_{\sigma(1)}^{r_1} \alpha_{\sigma(2)}^{r_2} \dots \alpha_{\sigma(n)}^{r_n} \mid \sigma \in S_n\} = \{\sigma(p) \mid \sigma \in S_n\}$.

The set of all such orbit sums clearly generates $R[z_1, \dots, z_n]^{S_n}$, but we give another set of generators below.

Theorem (Fundamental Theorem of Symmetric Functions): Every symmetric polynomial in α_1, …, α_n can be expressed uniquely as a polynomial in the symmetric polynomials e_i of $\alpha_1, \dots, \alpha_n$.

Equivalently,

$$\begin{aligned} \varphi : R[z_1, \ldots, z_n] &\xrightarrow{\sim} R[z_1, \ldots, z_n]^{S_n} \\ p(z_1, \ldots, z_n) &\mapsto p(e_1, \ldots, e_n) \end{aligned}$$

Review of ring theory

We give the definitiosn for relevant objects from algebra 1.

Definition (Ring, subring, integral domain, field, ideal): A [commutative, unital] *ring* $(R, +, \cdot, 1)$ is a set R with operations $+, \cdot$ such that $(R, +)$ is an abelian group, $(R, \cdot)$ is a semigroup, and $\cdot$ distributes over $+$.

A *subring* of a ring R is a subset $S \subseteq R$ which is a ring in itself.

An *integral domain* is a ring such that if $ab = 0$, then either $a = 0$ or $b = 0$.

For any ring R, the set of invertible elements is denoted $R^* := \{r \in R \mid \exists s \in R : r \cdot s = 1\}$

A *field* F is a ring such that $0 \neq 1$ and $F^* = F \setminus \{0\}$.

In a ring R, an *ideal* $I \subseteq R$ is such that $(I, +)$ is an abelian subgroup of R, and for any $r \in R$ and $a \in I$, $ra \in I$. Equivalently, $RI = I$.

The ideal generated by a set $S = \{s_1, \ldots, s_n\}$ is given by

$$\langle s_1, \ldots, s_n \rangle = \{r_1 s_1 + \ldots + r_n s_n \mid r_i \in R\}$$

Definition (Quotient ring): If I is an ideal, then $R/I = \{r + I \mid r \in R\}$ is a ring, and

$$\begin{aligned} \gamma : R &\to R/I \\ r &\mapsto r + I \end{aligned}$$

is a surjective ring homomorphism.

Universal property of quotients: If $\varphi : R \to S$ is a ring homomorphism, and $I \subseteq \ker(\varphi)$ is an ideal, then there is a unique map $\overline{\varphi} : R/I \to S$ such that $\overline{\varphi} \circ \gamma = \varphi$.

In any ring R, there is a bijection between ideals and quotient rings. Given an ideal I, we can form a quotient R/I; given a quotient ring R/I, we know that $\ker(\gamma : R \to R/I) = I$.

Definition (Further ideal properties): Let I be an ideal in a ring R. I is

1. *prime* if whenever $xy \in I$, $x \in I$ or $y \in I$.
2. *maximal* if there is no ideal J with $I \subsetneq J \subsetneq R$.

Proposition (Ideals in a field): A ring R is a field if and only if its only ideals are $\langle 0 \rangle$ and $\langle 1 \rangle = R$.

Proposition (Further relations between quotients and ideals): An ideal I is maximal if and only if R/I is a field. It is prime if and only if R/I is a integral domain.

Characteristic of a field

Definition (Characteristic of a field): Let F be a field. The characteristic $char(F)$ of F is the non-negative generator of $\ker(\varphi : \mathbb{Z} \to F)$.

Proposition (Possible characteristics of a field): Let F be a field. Then $char(F)$ is either 0 or prime.

Polynomials

Definition (Polynomial ring): Let R be a ring. The respective polynomial ring $R[x]$ is the set of sums $\{r_0 + r_1 x + \ldots \mid r_i \in R, r_i = 0 \text{ for all but finitely many } i\}$.

Proposition (Division algorithm): Let F be a field, and $f, g \in F[x]$, with $g(x)$ non-zero. Then there are unique $q(x), r(x) \in F[x]$ with $\deg(r) < \deg(g)$ such that $f(x) = q(x)g(x) + r(x)$.

Definition (Irreducible): A polynomial $f(x) \in F[x]$ is irreducible if

1. $f \notin F[x]^*$
2. If $f = gh$, then either $g \in F[x]^*$ or $h \in F[x]^*$

Theorem (Equivalences on a polynomial ring): Let F be a field and $f \in F[x]$. Then the following are equivalent

1. f is irreducible.
2. $\langle f(x) \rangle$ is a prime ideal.
3. $\langle f(x) \rangle$ is a maximal ideal.

Irreducibility criterion over fields

Over $\mathbb{C}$, a polynomial f is irreducible if and only if $\deg(f) = 1$.

Over $\mathbb{R}$, a polynomial f is irreducible if and only if either $\deg(f)$ is odd or it has a quadratic factor g with non-negative discriminant.

Any degree 2 or 3 polynomial over a field F is irreducible if and only if it has a root in F. This is not true for degrees 4 and above - consider $(x^2 + 1)^2 \in \mathbb{R}[x]$.

Proposition(Gauss' Lemma): A polynomial $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$. That is, if $f = gh$ where $g, h \in \mathbb{Q}[x]$, then there is $c \in \mathbb{Q}$ such that $cg, c^{-1}h \in \mathbb{Z}[x]$.

Corollary(Irreducibility over $\mathbb{F}_p$): Let $f \in \mathbb{Z}[x]$ be monic. Then if f is irreducible over some $\mathbb{F}_p[x]$, then f is irreducible over $\mathbb{Q}$.

Theorem(The Eisenstein criterion): Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, and suppose there is a prime $p \in \mathbb{Z}$ such that

1. $p \nmid a_n$
2. $p \mid a_i$, $0 \leq i \leq n - 1$

3. $p^2 \nmid a_0$

Then p is irreducible over $\mathbb{Q}$.

Fractional fields

Definition(Fractional field): Let R be an integral domain. Then $\text{Frac}(R)$ is the set of equivalence classes of $R \times (R \setminus \{0\})$ under the equivalence relation $(a, b) \sim (c, d) \iff ad = bc$. We write $\frac{a}{b}$ for the equivalence class of (a, b), and define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Proposition: $\text{Frac}(R)$ is a field, for any integral domain R.

Proposition(Minimal field containing R; universal property): If F is a field with R isomorphic to $S \subseteq F$, then there is an injective ring homomorphism $\varphi : \text{Frac}(R) \hookrightarrow F$.

Definition(Rational functions over a field): Let F be a field. The *rational functions over F* is given by $F(t) = \text{Frac}(F[t])$

R-algebras

Definition(R-algebra; homomorphism): Let R be a ring. An R-algebra (A, ι_A) is a ring A with an injective ring homomorphism $\iota_A : R \to A$.

An R-algebra homomorphism is a ring homomorphism $\varphi : (A, \iota_A) \to (B, \iota_B)$ such that $\iota_B = \varphi \circ \iota_A$.

Field extensions

Definition(Field extension, degree, finite): Let F be a field. We call any field E which can be made an F-algebra an extension of F, and write E/F.

We can view E as a vector space over F, and the degree of the extension E/F is then $[E : F] = \dim_F(E)$. An extension is finite if $[E : F]$ is finite.

Adjoining roots of polynomials

If $f(x) \in F[x]$, we consider the process of ‘adjoining a root to f in F’ as taking the quotient $F[x]/\langle f(x)\rangle$. We focus in particular on the case when $f(x)$ is irreducible (and so the quotient is a field, from previous results).

Basis of a quotient: By the division algorithm, given a quotient $F[x]/\langle f(x)\rangle$, the set $\{\overline{1}, \ldots, \overline{x^{\deg(f)-1}}\}$ is an F-basis for this quotient.

Arithmetic in $\mathbf{E = F[x]/\langle f(x)\rangle}$: Addition and multiplication are clear. For division, we have two processes:

Division by the Euclidean algorithm: For any $g(x) \in F[x]$ (where we can assume that $\deg(g) < \deg(f)$), notice that as $f(x)$ is irreducible and $g(x) \notin \langle f(x) \rangle$, $\langle f(x), g(x) \rangle = F[x]$, and so there are polynomials $q_1, q_2 \in F[x]$ such that

$$q_1(x)f(x) + q_2(x)g(x) = 1$$

We can compute this using the Euclidean algorithm, writing $f(x) = q(x)g(x) + r(x)$ and repeating, then reversing the process to express 1 as a linear combination of f and g.

Division by matrices: Let $M_{n\times n}(F)$ be the set of matrices over F. For each element $\beta \in E$, we have a homomorphism $M_\beta : E \to E$ given by left multiplication by $\beta(z \mapsto \beta z)$. This is linear over F, and so can be represented as a matrix $M_\beta \in M_{n\times n}(F)$. We also them get an injective homomorphism $E \hookrightarrow M_{n\times n}(F)$ by $\beta \mapsto M_\beta$. In particular, this then gives

$$M_{p(x)} = p(M_x)$$

and thus $M_{\frac{1}{g(x)}} = M_{g(x)}^{-1}$. We can compute $M_p(x)$ using the above formula and considering multiplication by x in E, and take its inverse using row reduction.

Generating subalgebras

Definition(Generating subalgebra): Let $F \subseteq C$ be fields and $S \subseteq C$ be a set. The generating subalgebra $F[S]$ is the set of polynomial expressions in S. That is,

$$F[S] := \left\{ \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} s_1^{i_1} \dots s_n^{i_n} \;\middle|\; n \geq 0, a_{i_1,\dots,i_n} \in F \text{ where all but finitely many are zero}, s_i \in S \right\}$$

This is also the image of the evaluation homomorphism

$$\begin{aligned} \varphi : F[x_S \mid s \in S] &\to C \\ f(\dots, x_s, \dots) &\mapsto f(\dots, s, \dots) \end{aligned}$$

This is the minimal ring containing F and S.

Definition(Generating subfield): Let $F \subseteq C$ be fields. The generating subfield $F(S)$ is the set of rational expressions in $F[S]$. That is,

$$F(S) := \left\{ \frac{x}{y} \in C \;\middle|\; x, y \in F[S], y \neq 0 \right\}$$

In this case, $F[S] = F(S)$ if and only if each element in S is the root of some polynomial in F.

One thing we may expect is that this is the minimal subfield, as this is generated in a similar way to the fractional field of $F[S]$.

Proposition($F(S)$ as a minimal field containing $F[S]$): $F(S) \cong \text{Frac}(F[S])$.

If $\alpha \in C$ has minimal polynomial $f(x) \in F[x]$, we can distinguish the fields $F(\alpha)$ and $F[x]/\langle f(x) \rangle$ by noting that the former consists of actual fractions in C, while the former consists of formal "syntactic" fractions. We do however have that $F(\alpha) = F[x]/\langle f(x) \rangle$.

Over a field F, we can then classify elements by the kernel of the evaluation homomorphism $\varphi : F[x] \mapsto F[\alpha]$. If this is non-zero (or has a non-zero generator in $F[x]$), we say that α is algebraic. Otherwise, we say that α is transcendental (such as in the case of α).

When α is algebraic, this $f(x)$ is then the unique monic generator of $\ker(ev_\alpha)$, and so is irreducible.

Proposition(Minimal polynomials and irreducibility): Let $g(x)$ be a polynomial with α as a root. If $g(x)$ is irreducible, then g is the minimal polynomial of α.

Proposition(Multiplicity of index): Let $L/E/F$, and suppose that $\{\alpha_i\}$ is an F-basis for E, and $\{\beta_j\}$ is an E-basis for L. Then $\{\alpha_i\beta_j\}$ is an F-basis for L, and in particular $[L:E][E:F]=[L:F]$.

Definition(Degree of an element): Let E/F and $\alpha \in E$ be algebraic over F. The degree of α over F is then given by $\deg_F(\alpha) = [F(\alpha):F]$.

Corollary(Divisibility of index and degree): Let $L/E/F$. Then $[E:F] \mid [L:F]$. If $\alpha \in L$ is algebraic over F, then $\deg_F(\alpha) \mid [L:F]$.

Cyclotomic polynomials

Denote the roots of unity $e^{\frac{2\pi i}{n}}$ by ζ. We write the set of such roots of unity as

$$\mu_n(\mathbb{C}) = \left\{ e^{\frac{2\pi i k}{n}} \mid k = 0, 1, \ldots, n-1 \right\}$$

Definition(Cyclotomic polynomial): Let $n \in \mathbb{N}$. The n^{th} cyclotomic polynomial is given by

$$\Phi_n(x) = \prod_{\zeta \in \mu_n(\mathbb{C})} (x - \zeta) = \prod_{\substack{k=0 \\ \gcd(k,n)=1}}^{n-1} \left(x - e^{\frac{2\pi i k}{n}} \right)$$

In this case, it is clear that

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

We can also see that $\deg(\Phi_n(x)) = \phi(n)$, by noting that there are exactly $\phi(n)$ numbers coprime to n in $\{0, 1, \ldots, n-1\}$.

Proposition(Cyclotomic polynomials are integral): $\Phi_n(x) \in \mathbb{Z}[x]$ for all $n \in \mathbb{N}$.

Frobenius homomorphisms and irreducibility of cyclotomic polynomials

Let A be an F_p algebra. Note that this structure is unique as there is a unique ring homomorphism $\mathbb{Z} \to A$, and by the universal property of quotients we then have a unique ring homomorphism $F_p \to A$.

The ***Frobenius homomorphisms*** take the form

$$\begin{aligned} \varphi : A &\to A \\ x &\mapsto x^p \end{aligned}$$

These are homomorphisms as $p = 0$ in A, and so the middle terms of $(x+y)^p$ (which are of the form $\binom{p}{k} x^k y^{n-k}$) are each 0 in A.

Properties of the Frobenius homomorphisms: Over any F_p algebra A and $g \in A$, $g(x^p) = g(x)^p$. We can see this by noting that $\varphi(g(x)) = g(\varphi(x))$ for any polynomial g over any ring R and any homomorphism $\varphi : R \to S$.

With prime power polynomials, we can note that $\Phi_{p^k}(x)\left(x^{p^{k-1}}-1\right)=\left(x^{p^k}-1\right)$, and so in F_p we have that $\overline{\Phi_{p^k}(x)}(x-1)^{p^{k-1}}=(x-1)^{p^k}$ and thus $\overline{\Phi_{p^k}(x)}=(x-1)^{p^k-p^{k-1}}$. We can thus apply Eisenstein's criterion to this, noting also that $\Phi_{p^k}(1)=p$.

Theorem(Irreducibility of $\Phi_n(x)$): $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

We prove this using the Frobenius homomorphisms, and show that $f(\alpha)=0 \implies f(\alpha^k)=0$ for k coprime to n (and in particular, it is sufficient to show this for the primes).

Corollary(Degree of ζ_n over $\mathbb{Q}$): $\Phi_n(x)$ is the minimal polynomial of $\zeta_n := e^{\frac{2\pi i}{n}}$ over $\mathbb{Q}$, and $\deg_{\mathbb{Q}}(\zeta_n) = [\mathbb{Q}(\zeta_n):\mathbb{Q}] = \deg(\Phi_n(x)) = \phi(n)$.

Algebraic extensions

Definition(Algebraic extension): An extension E/F is algebraic if every $\alpha \in E$ is algebraic over F.

Proposition(Preservation of algebraic numbers): Let E/F be an algebraic extension. Then $\alpha \in E$ is algebraic if and only if $\alpha \in F$ is algebraic.

Algebraic extensions, prerservation of algebraic numbers

Algebraic closures

Definition(Non-absolute algebraic closures): Let $F \subseteq C$ be a field. The algebraic closure of F with respect to C is given by

$$\overline{F} = \{x \in C \mid x \text{ is a root of some } p \in F[x]\}$$

Proposition(Double-closure): Let $F \subseteq C$. Then $\overline{\overline{F}} = \overline{F}$ with respect to C.

Definition(Split fields): We say that a field F is split if every irreducible polynomial is of degree 1

Proposition(Equivalent formulations of "closedness"): Let F be a field. The following are equivalent

1. F is split.
2. Every polynomial f has a root in F.
3. Every algebraic extension E of F is trivial. ($[E:F]=1$ and $E=F$)
4. Every finite extension E/F is trivial.

Definition(Absolutely algebraically closed): Let F be a field. We say that F is algebraically closed if all of the above hold.

Definition(Algebraic closure of a field): Let F be a field. An extension E/F is an algebraic closure if

1. E is algebraically closed.
2. E is minimal with this property, i.e. E is algebraic over F.

Ruler and compass constructions

A ruler and compass construction is as follows.

We begin with the two points $(0,0)$ and $(1,0)$ in $\mathbb{R}^2$. We can construct

1. A line between two points P, Q.
2. A circle centred at a point P through another point Q.
3. A point by taking the intersection of two lines or circles.

Definition(Constructible point): A point is constructible if we can reach it using the above process, beginning with $(0,0)$ and $(1,0)$.

With this, we have some basic procedures.

1. **Erecting a perpendicular given a line segment PQ:** Draw the circles through P centred at Q, and through Q centred at P. Take their intersection points, and then draw the line segment through them.
2. **Bisecting a line segment PQ:** Erect a perpendicular to PQ, and then take the midpoint.
3. **Doubling a line segment PQ:** Draw the line PQ out fully, and take the circle through P centred at Q and the new intersection point R.
4. **Bisecting an angle:** Draw a circle centred at the intersection between the two lines through one point on the line, take the other intersection point and draw circles through one another centred at each other. Connect the final intersection points to the original intersection.
5. **Constructing a parallelogram given a line segment:** Connect opposite points, and bisect this line segment. Draw a line through the other point and the midpoint, and double this. Connect the points accordingly.

Proposition(Constructibility of line segments and points): A line segment of length $|\alpha|$ is constructible if and only if the point $(\alpha, 0)$ is constructible.

Definition(Constructible number): We say a number α is constructible if a line segment of length $|\alpha|$ is constructible.

Proposition(Constructibility of a point (x,y)): A point (x,y) is constructible if and only if the numbers x and y are constructible.

Proposition(Constructible real numbers as a field): The set of constructible numbers is a field, closed under taking real square roots.

Proposition(Degree of constructible real numbers over $\mathbb{Q}$): Suppose P is constructible from $S \subseteq \mathbb{R}$, and let $\mathbb{Q}(S)$ be the corresponding field. Then $[\mathbb{Q}(S \cup \{P\}) : \mathbb{Q}(S)] = 1$ or 2.

Corollary(Degree of $\mathbb{Q}(\alpha)$ for any constructible α): Every constructible real number is in a tower of quadratic extensions, and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2^n.

Proposition(Doubling the cube, squaring the circle, bisecting the angle): $\sqrt[2]{2}, \sqrt{\pi}, \cos(20°)$ are not constructible numbers.

Proposition(Constructibility of a polygon and $\cos\left(\frac{2\pi}{n}\right)$): The n-gon is constructible if and only if $\cos\left(\frac{2\pi}{n}\right)$ is constructible.

Proposition(Degree of $\cos\left(\frac{2\pi}{n}\right)$ over $\mathbb{Q}$): For any $n \in \mathbb{N}$, $\deg_{\mathbb{Q}}\left(\cos\left(\frac{2\pi}{n}\right)\right) = \frac{1}{2}\phi(n)$.

Proposition(The integral Chinese Remainder Theorem over rings): If $\gcd(a, b) = 1$, then

$$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

Corollary(Multiplicity and a formula for $\phi(n)$): If $\gcd(a, b) = 1$, $\phi(ab) = \phi(a)\phi(b)$. For any prime power, $\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$. Thus, if $n = p_1^{r_1} \dots p_k^{r_k}$,

$$\phi(n) = (p_1 - 1)p_1^{r_1 - 1} \dots (p_k - 1)p_k^{r_k - 1}$$

Theorem(Equivalent formulation of the constructibility of an n-gon): An n-gon is constructible if and only if it is the product of a power of 2 and distinct Fermat primes.

Precursors to Galois theory

Splitting fields

Key points:

1. The splitting field for any non-constant polynomial $p(x)$ exists and is unique up to isomorphism.
2. The degree of a splitting field E/F for a polynomial p must divide $\deg(p)!$.

Definition(Splitting field): Let $p \in F[x]$ be a polynomial with $\deg(p) \geq 1$ and roots $\alpha_1, \dots, \alpha_n$. A splitting field E/F for p is such that

1. p splits in E.
2. E is minimal with this property, that is, $E = F(\alpha_1, \dots, \alpha_n)$

Proposition(Existence of splitting fields): Each non-constant polynomial p has a splitting field, which has degree $[E : F] \mid \deg(p)!$.[1]

Proposition(Uniqueness of splitting fields): All splitting fields for a polynomial $p \in F[x]$ are isomorphic as F-algebras.

Separability, perfection, normality

Key points:

1. The separability of a polynomial can be determined by computing $\gcd(f(x), f'(x))$.
2. Finite fields and characteristic 0 fields are perfect.
3. $\mathbb{F}_p(\sqrt[p]{t})$ is an imperfect field.

[1] The second part of this statement comes from a corollary of the following theorem.

Definition(Separable polynomial): A polynomial $p \in F[x]$ is separable if in a splitting field E/F, its roots $\alpha_1, \ldots, \alpha_n$ are distinct (i.e. $\alpha_i \neq \alpha_j$ for $i \neq j$).

Definition(gcd of polynomials): Let $p, q \in F[x]$ be polynomials. The gcd of p and q is the unique monic generator of $\langle p(x), q(x) \rangle$, or 0 if $p = q = 0$.

Proposition(Independence of gcd over field): If E/F and $h_K(x)$ denotes the gcd of p and q as computed in the field K, then $h_E(x) = h_F(x)$.

Proposition(Criteria for separability): A polynomial $f \in F[x]$ with $\deg(f) \geq 1$ is separable if and only if $\gcd(f(x), f'(x)) = 1$.

Thus, given a polynomial $f \in F[x]$, we can determine separability by taking its algebraic derivative.

Definition(Perfect): A field F is perfect if every irreducible polynomial is separable.

Proposition(Perfectness of characteristic 0 fields): Every characteristic 0 field is perfect.

Proposition(Imperfectness in non-zero characteristic): Let $char(F) = p > 0$. Then $x^p - t$ is irreducible if and only if $t^{\frac{1}{p}} \notin F$.

Proposition(Equivalent formulations of imperfection): Let F be a field of characteristic p, and $f \in F[x]$. The following are equivalent.

1. f is inseparable.
2. f is a polynomial in x^p.
3. $f'(x) = 0$.

Proposition(Perfection in positive characteristic): Let $char(F) > 0$. Then the Frobenius homomorphism φ_F is surjective if and only if F is perfect.

Corollary(Perfection of finite fields): All finite fields are perfect.

Finite fields

Key points

1. There is a unique finite field up to isomorphism of cardinality p^n for any prime p, $n \in \mathbb{N}$.
2. $\mathbb{F}_q$ is the splitting field for $x^q - x$.
3. $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ iff $m \mid n$
4. $\prod_{\substack{f(x) \text{irreducible over} \mathbb{F}_p \\ \deg(f) \mid n}} f(x) = x^{p^n} - x$
5. $\mathbb{F}_q^*$ is cyclic.

Proposition($\mathbb{F}_q$ as a splitting field): Let $q = p^n$. Then $\mathbb{F}_q$ is the splitting field of $x^q - x$ over $\mathbb{F}_p$.

Corollary(Uniqueness of finite fields): Every finite field of order q is isomorphic.

Theorem(Cyclicness of finite multiplicative subgroups): Let F be a field and $G \leq F^*$ be finite. Then G is cyclic.

Automorphism groups

Key points:

1. F-algebra automorphisms are decided by their action on a basis.
2. The automorphisms of a splitting field can be viewed as a group of permutations (on the indices).

Definition(Automorphism group): Let E/F be an extension of fields. The automorphism group $Aut(E/F)$ is the group of F-algebra automorphisms $\varphi : E \to E$.

The number of homomorphisms $\varphi : F(\alpha) \to K$ is equal to the number of roots of the minimal polynomial of α in K.

For any finite extension E/F, an F-algebra homomorphism $\varphi : E \to E$ is an automorphism. This is not true for infinite extensions: e.g. $\mathbb{C}(t)/\mathbb{C}$ and $\varphi : t \mapsto t^2$.

If $E = F(\alpha_1, \ldots, \alpha_n)$, this is uniquely determined by its action on $\alpha_1, \ldots, \alpha_n$ (as these are all polynomial expressions in the α_i).

Given a splitting field E/F, $Aut(E/F)$ can be seen as a subgroup of $Perm\{\alpha_1, \ldots, \alpha_n\} \cong S_n$ (by the actions on the roots).

Proposition($\mathbb{F}_{p^n}/\mathbb{F}_p$): The extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ can be generated by a single element α.

Definition(Primitive element): For a finite extension E/F, a primitive element $\alpha \in E$ is such that $E = F(\alpha)$.

Normal and separable extensions

Key points:

1. An extension is Galois if and only if the minimal polynomial of every $\alpha \in E$ over F has exactly $\deg_F(\alpha)$ roots in E.
2. For a tower $E/M/F$, E/F is separable iff E/M and M/F are separable[2]; E/F normal/Galois implies E/M normal/Galois.
3. Subpoints:
   (a) Every extension of degree 2 is normal.

Definition(Separable extension): An algebraic extension E/F is separable if the minimal polynomial of every $\alpha \in E$ over F is separable.

Definition(Normal extension): An algebraic extension E/F is normal if the minimal polynomial of every $\alpha \in E$ over F splits in E.

Definition(Galois extension): An algebraic extension E/F is Galois if it is normal and separable.

These are each properties of elements in E corresponding to their minimal polynomials in F.

[2] This is a corollary of the counting lemma, but the nature of the result puts it here.

The counting lemma

Key points:

1. In a splitting field, the size of the Galois group is the degree of the splitting field over F.
2. The separability of a finite extension E/F is determined by whether the generators α_i have separable minimal polynomials.

Theorem(Counting lemma): Let $E = F(\alpha_1, \ldots, \alpha_n)/F$ and K be a field. Then $|Hom_F(E, K)| \leq [E : F]$. This is an equality if and only if each minimal polynomial f_i is separable and splits in K.

Corollary(Closedness): If F is perfect and K is algebraically closed,

$$|Hom_F(E, K)| = [E : F]$$

Corollary: For any finite extension E/F, $|Aut(E/F)| \leq [E : F]$.

Corollary(Splitting fields): If E is the splitting field for a separable polynomial $f \in F[x]$, then $|Aut(E/F)| = [E : F]$.

Corollary(Separability by generators): A finite extension E/F is separable iff $E = F(\alpha_1, \ldots, \alpha_n)$ and each α_i has separable minimal polynomial.

Corollary(Separability): If $E/M/F$, E/F is separable if and only if E/M and M/F are separable.

Fixed fields

Key points:

1. We can correspond every subgroup $H \leq Aut(E/F)$ to a subfield $E/E^H/F$.

Definition(Fixed field): Let E/F be *any field extension* and $H \leq Aut(E/F)$. Then

$$E^H := \{x \in E \mid \sigma(x) = x \text{ for any } \sigma \in H\}$$

Proposition(E^H relative to E, F): E^H is a subfield of E containing F.

Definition(Conjugate subfield)[3]**:** Let E/F be *any field extension*, and $F \subseteq K_1, K_2 \subseteq E$. Then K_1 and K_2 are conjugate if there is an automorphism $\varphi : E \to E$ with $\varphi(K_1) = K_2$.

Galois Theory

Foundations of Galois Theory

Key points:

[3] This doesn't seem to be included in the notes, but was mentioned and is probably an important addition.

1. An extension is Galois if and only if it is a splitting field for some separable polynomials over F.
2. Given a Galois extension E/F, the properties of its subfields correspond directly to the properties of its Galois group $Gal(E/F)$. Namely:
   (a) Taking fixed fields of automorphism groups and automorphism groups fixing fields are mutual inverses.
   (b) Two subfields are conjugate if and only if the respective automorphism groups fixing them are conjugate.
   (c) A subfield is normal if and only if the automorphism group fixing it is normal.
   (d) The indices and inclusions within a Galois group are reversed for subfields of a finite extension.
   (e) The subgroups of $Gal(E/F)$ take the form $Gal(E/K)$ where $E/K/F$, while the quotient groups take the form $Gal(K/F)$ where E/K

General tips for determining subfield diagrams:

1. If α is fixed by a subgroup H, then so is $\mathbb{Q}(\alpha)$.

Theorem A(Degree counting): Let E/F be *a field extension* and $H \leq Aut(E/F)$ have finite index. Then $|H| = [E : E^H]$.

Theorem B(Equivalent formulations of Galois extensions): Let E/F be a finite extension. The following are equivalent.

1. E/F is a Galois extension.
2. E is a splitting field for some separable polynomials over F.
3. $F = E^{Aut(E/F)}$
4. $F = E^H$ for some $H \leq Aut(E/F)$

Theorem(The Fundamental Theorem of Galois Theory): Let E/F be a finite Galois extension, and let $G = Gal(E/F)$.

1. The maps $H \mapsto E^H$ and $K \mapsto Gal(E/K)$ (between subgroups of G and subfields of E) are inverse bijections.
2. These maps reverse inclusions:
   (a) $H_1 \supseteq H_2 \iff E^{H_1} \subseteq E^{H_2}$
   (b) $Gal(E/K_1) \supseteq Gal(E/K_2) \iff K_1 \subseteq K_2$
3. $[E^{H_2} : E^{H_1}] = [H_1 : H_2] = \frac{|H_1|}{|H_2|}$
4. $\sigma(E^H) = E^{\sigma H \sigma^{-1}}$
5. A subgroup H is normal in G if and only if E^H/F is a normal extension, and in this case $Gal(E^H/F) \cong G/H$.

The Galois theory of finite fields; cyclotomic extensions

Key points:

1. The Galois group $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$, and is generated by the Frobenius homomorphism φ_q.

2. The Galois group of a cyclotomic extension is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.
3. Every finite "abelian extension" is related in some way to a cyclotomic extension (namely, contained in one).

Theorem(Galois group for finite fields): $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension, and $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ is generated by $\varphi_q : \alpha \mapsto \alpha^q$.

Theorem(Galois group of a cyclotomic extension): If for each $\sigma \in Gal(F(\zeta_n)/F)$, $\zeta_n \mapsto \zeta_n^{\chi(\sigma)}$, then

$$\begin{aligned} \chi : Gal(F(\zeta_n)/F) &\hookrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\mapsto \chi(\sigma) \end{aligned}$$

is an injective group homomorphism.

In this case, as $|Gal(F(\zeta_n)/F)| = [F(\zeta_n) : F]$, $Gal(F(\zeta_n)/F) \cong (\mathbb{Z}/n\mathbb{Z})^*$ is an isomorphism if and only if $\Phi_n(x)$ is irreducible.

Theorem(Kronecker-Weber): Every finite Galois extension with abelian Gaois group is contained in some cyclotomic extension.

Theorem(Constructibility of n-gons): The regular n-gon is contructible if and only if n is a product of a power of 2 and distinct Fermat primes.

Lemma(Constructibility)[4]**:** Let E/F be a fomote Galois extension with abelian Galois group. Then $[E : F] = 2^k$ for some k if and only if E/F is a tower of quadratic extensions.

Transitivity, discriminant subfields, cubic and quartic extensions

Key points:

1. There are only a few possibilities for Galois groups of cubics and quartics.
2. There are a few important things to note in determining a cubic or quartic extension.
   (a) Whether or not the polynomial is irreducible.
   (b) Whether the discriminant is a square. (This determines a cubic extension.)
   (c) (Quartics): The degree of the quartic over the resolvent cubic extension.
3. The resolvent cubic of $x^4 + bx^3 + cx^2 + dx + e$ is $y^3 - cy^2 + (bd - 4e)y + (4ce - b^2e - d^2)$

Definition(Galois group of a polynomial): Let $f \in F[x]$, and let E be a splitting field for f over F. The Galois group of f is $G_{f(x)} := Gal(E/F)$.

Proposition(Transitivity of Galois groups): If $f(x)$ is irreducible, then the action of $G_{f(x)}$ on $\{\alpha_1, \ldots, \alpha_n\}$ has a single orbit.

Corollary(Size of a Galois group): If $f(x)$ is irreducible, then $n \mid \left|G_{f(x)}\right|$.

Definition(Discriminant): Let $f \in F[x]$ have roots $\alpha_1, \ldots, \alpha_n$. The discriminant of f is

$$\Delta := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

[4] This holds generally, but is only relevant and was only proved in the abelian case.

Proposition(Discriminant and $G_{f(x)}$): Let $char(F) \neq 2$. Then $\sqrt{\Delta} \in F \iff G_{f(x)} \leq A_n$.

Corollary(Possible Galois groups for cubics): Let F be a field with $char(F) \neq 2$, and $f \in F[x]$. Then

$$G_{f(x)} = \begin{cases} A_3 & \text{if } \sqrt{\Delta} \in F \\ S_3 & \text{otherwise} \end{cases}$$

The full diagram of subgroups for S_3: $\{e\} \subseteq A_3, \langle(23)\rangle, \langle(13)\rangle, \langle(12)\rangle \subseteq S_3$.

Proposition(The resolvent cubic): Let $x^4 + bx^3 + cx^2 + dx + e$ have roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. The resolvent cubic (with roots $\beta_1 := \alpha_1\alpha_4 + \alpha_2\alpha_3$, $\beta_2 := \alpha_2\alpha_4 + \alpha_1\alpha_3$, $\beta_3 := \alpha_3\alpha_4 + \alpha_1\alpha_2$) is

$$y^3 - cy^2 + (bd - 4e)y + (4ce - b^2e - d^2)$$

In a quartic extension, the principal extension is usually referred to as E, while the resolvent cubic extension is usually referred to as M.

Proposition(Possible quartic Galois groups): The transitive subgroups of S_4 are

G	$[G \cap V : \{e\}]$ or $[E : M]$	$[G : G \cap V]$ or $[M : F]$
S_4	4	6
A_4	4	3
K_4	4	1
D_4	4	2
C_4	2	2

Galois Theory of radical extensions

Key points:

1. The Galois group of a polynomial of the form $x^n - a$ can be expressed as a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.
2.

Let F be a field and $f(x) = x^n - a \in F[x]$ be separable $(a \neq 0)$ with $char(F) \nmid n$.

The splitting field of f takes the form $F(\sqrt[n]{a}, \zeta_n)$ (where $\sqrt[n]{a}$ is any root of $x^n - a$).

In this case, an automorphism σ of E is determined by its action on $\sqrt[n]{a}$ and ζ_n.

Proposition(Semi-direct product): Let $\sigma(\sqrt[n]{a}) = \zeta_n^{\rho(\sigma)} \sqrt[n]{a}$ and $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$. Then the map

$$\begin{aligned} \psi : G_{f(x)} &\hookrightarrow \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}/n\mathbb{Z}) \;\middle|\; a \in (\mathbb{Z}/n\mathbb{Z})^*, b \in \mathbb{Z}/n\mathbb{Z} \right\} \\ \sigma &\mapsto \begin{bmatrix} \chi(\sigma) & \rho(\sigma) \\ 0 & 1 \end{bmatrix} \end{aligned}$$

is an injective group homomorphism.

We can decompose $F(\sqrt[n]{a}, \zeta_n)/F$ into $F(\sqrt[n]{a}, \zeta_n)/F(\zeta_n)/F$, and in this case $N = \left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \lhd G_{f(x)}$ is normal and the Galois group of $F(\sqrt[n]{a}, \zeta_n)/F(\zeta_n)$ (and so decomposes into a series of abelian groups). In particular, $\{e\} \lhd N \lhd G$.

Solvable groups

Key points:

1. An extension is solvable (contained in a Galois extension with solvable Galois group) if and only if it is *contained* in an iterated radical extension. [It may itself not be Galois...]

Definition(Abelian series; solvable group): Let G be a group. A sequence of subgroups $G = G_0 \geq G_1 \geq \ldots \geq G_m = \{e\}$ is called an abelian series if for each i,

1. $G_{i+1} \lhd G_i$
2. G_i/G_{i+1} is abelian

If a group G has an abelian series, we say that G is solvable.

Key examples:

1. $m = 1$: Abelian groups
2. $m = 2$: Galois groups of radical extensions
3. $m = n$: Upper triangular matrices in $GL_n(R)$

Theorem(Feit-Thompson): Every group of odd order is solvable.

Definition(Radical extension): An extension E/F is radical if there is some $\alpha \in E$ with $E = F(\alpha)$ and $\alpha^n \in F$ for some $n \geq 1$.

Theorem(Iterated radical and solvable extensions): A finite extension L/F is contained in an iterated radical extension if and only if it is contained in a finite Galois extension with solvable Galois group.

[[We say that an extension E/F is solvable if it is contained in a finite Galois extension with solvable Galois group.]]

Theorem(Kummer): Let E/F be a Galois extension of degree n. If $Gal(E/F)$ is cyclic and F contains a primitive n^{th} root of 1, then $E = F(\sqrt[n]{a})$ for some $a \in F$.

Definition(Polynomial solvable by radicals): Let F be a field and $f \in F[x]$. Then f is solvable by radicals if its splitting field E is contained in an iterated radical extension.

Corollary(Solvability): A polynomial $f(x)$ is solvable by radicals if and only if its Galois group $G_{f(x)}$ is solvable by radicals.

Proposition(Quotient and subgroup abelian series):

1. The image under $\gamma : G \twoheadrightarrow G/N$ of an abelian series is also an abelian series (in G/N).
2. The intersection of an abelian series with a subgroup $H \leq G$ is an abelian series of H.

Some examples: Polynomials over $\mathbb{C}, \mathbb{R}, \mathbb{F}_q, \mathbb{C}((t)), \mathbb{R}((t)), \mathbb{F}_q((t))$[5] have only solvable Galois groups

[5] Fractional fields of formal power series

Proposition(Unsolvable group): A_5 is unsolvable.

Theorem(Solvability of A_n, S_n): S_n and A_n are solvable if and only if $n \leq 4$.

Corollary(Unsolvability of polynomials): A generic extension $K(t_1, \ldots, t_n)/K(t_1, \ldots, t_n)^{S_n}$ has Galois group S_n, and so there is no formula for solving a polynomial of degree ≥ 5 by radicals.

Theorem(Unsolvability over $\mathbb{Q}$): Over $\mathbb{Q}$, for each $n \in \mathbb{N}$ there exist polynomials of degree n with Galois group S_n.

Assignment and workshop questions and results

Assignment 1

(1): Power sums - using the Symmetric Functions Theorem: Build up formula continually starting with $n = 1$, noting that $e_k = 0$ for any $n < k$.

(2): Solving quartics by radicals - We can compute the roots of a quartic by considering $\beta_i, i = 1, 2, 3$ in α_i.

(3): Morphisms from quotient rings - morphisms $\mathbb{Z}[x]/\langle f(x) \rangle \to R$ are equivalent to giving $f(x)$ roots in R (the number of such morphisms is equal to the number of roots of f in R).

(4): Galois groups, relations, exceptional and ordinary relations.

Workshop 1

(1): Orbit sums and elementary symmetric polynomials

(2): Computations and an alternate way to reduce a quartic to a cubic

(3): Quotients can be seen as equivalence relations and both ideals

Assignment 2

(1): Irreducible polynomials - Counting monic irreducible polynomials

(2): The Eisenstein criterion for $F = K(t)$

(3): The division algorithm over any ring $R[x]$

(4): Arithmetic in an extension

(6): Properties of R-algebra homomorphisms

Workshop 2

(1), (2), (3): Computations in a field

(4): Trace and norm of an element $\beta \in E$

Assignment 3

(1): Subextensions can be isomorphic but not equal

(2): $[L : F] = [L : E][E : F]$ for a basis

(3): Radical extensions, quadratic extensions; properties

(4): Minimal polynomials over various fields and degrees; solubility of quadratics and cubics.

Workshop 3

(1): Multiple adjoinments of roots; generators

(2): Degrees of extensions; solubility of cubics

(3): Minimal polynomials over various fields and degrees

(4): Transcendentality of elements related to transcendental numbers

Assignment 4

(1): $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

(4): The determinant of a degree n polynomial satisfies $\Delta = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i)$.

Workshop 4

(2): If $char(F) = p > 0$, the polynomials $x^p - x - c \in F[x]$ are either split or irreducible.

Assignment 5

(2): $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$; $x^{p^n} - x = \prod_{\substack{f(x) \text{ irreducible} \\ \deg(f) | n}} f(x)$

(4): The only continuous automorphisms of $\mathbb{C}$ are id and conjugation; the only automorphism of $\mathbb{R}$ is the identity map.

Workshop 5

haha

Assignment 6

haha

Workshop 6

haha

Other miscellaneous results

If m, n coprime, $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m, \zeta_n) = [\mathbb{Q}(\zeta_m)](\zeta_n)$