MATH 404 Notes

Contents

1 General

1.1 Ideals

A subring I of ring R is an ideal in R if $ra \in I$ and $ar \in I$ for all $r \in R$ and $a \in I$

- A proper ideal I in R satisfies $I \subset R$
- A subset I of a ring R is an ideal in R if and only if has the following properties
  - I is non-empty
  - If $a, b \in I$, then $a - b \in I$
  - If $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$

1.2 Maximal Ideals

Let R be a commutative ring with identity. Then ideal M in R is maximal if $M \subset R$ and the only ideals containing M are M and R

- There does not exist an ideal J such that $M \subset J \subset R$
- i.e. M is as large as possible while being a proper subset of R

1.3 Prime Ideals

An ideal P in ring R is called prime if $bc \in P$ implies $b \in P$ or $c \in P$

- P is a prime ideal in ring R if and only if R/P is an integral domain
- Prime ideals in $\mathbb{Z}$ are (p) where p is prime

1.4 Principal Ideals Generated by c

Let R be a commutative ring with identity and $c \in R$. Then $I = \{rc \mid r \in R\}$ is the principal ideal generated by c, denoted (c)

- If $(m) \subseteq (n)$, then $n \mid m$

1.5 Principal Ideal Domains

A principal ideal domain (PID) is an integral domain in which every ideal is principal

- An integral domain is a commutative ring with identity with no zero divisors
- If $\mathbb{F}$ is a field, then $\mathbb{F}$ is a principal ideal domain
- i.e. $\mathbb{Z}$, $\mathbb{F}[x]$, $\mathbb{Z}[i]$

1.6 Ring Automorphisms

A ring automorphism is an isomorphism from a ring to itself

- Let R be a ring. Then the set of all ring automorphisms from R to R forms a group under function composition, denoted $\mathrm{Aut}(R)$

1.7 Unital Ring Homomorphism

A ring homomorphism $\varphi : R \to S$ is unital if $\varphi(1_R) = 1_S$ where R and S are rings with identity

- Let F be a field, let R be any non-zero commutative ring with identity, and let $\varphi : F \to R$ be a unital ring homomorphism. Then φ is injective
- All ring homomorphisms with field domains are unital
- A unital ring homomorphism φ induces an isomorphism $F \cong \varphi(F)$

1.8 Kernels

The kernel of a ring homomorphism $f : R \to S$ is $\mathrm{Ker}(f) = \{r \in R \mid f(r) = 0_S\}$

- $\mathrm{Ker}(f)$ contains every element in the domain R that has 0 value in the co-domain S
- $\mathrm{Ker}(f)$ is an ideal in R
  - Given $a, b \in \mathrm{Ker}(f)$, $a - b \in \mathrm{Ker}(f)$ since $f(a-b) = f(a) - f(b) = 0_S - 0_S = 0_S$
  - Given $r \in R$ and $a \in \mathrm{Ker}(f)$, $ra \in \mathrm{Ker}(f)$ since $f(ra) = f(r) \cdot f(a) = f(r) \cdot 0_S = 0_S$
- $\mathrm{Ker}(f) = \{0_R\}$ if and only if
  - f is injective
  - R is isomorphic to $f(R)$

1.9 Vector Spaces

Let F be a field. Then a vector space V over F is an additive abelian group equipped with a scalar multiplication such that for all $a, a_1, a_2 \in F$ and $v, v_1, v_2 \in V$

- $a(v_1 + v_2) = av_1 + av_2$
- $(a_1 + a_2)v = a_1 v + a_2 v$
- $a_1(a_2 v) = (a_1 a_2)v$
- $1_F v = v$

1.10 Spanning Sets

A set $\{v_1, ..., v_n\}$ spans a vector space V over a field F if every element of V is a linear combination of $v_1, ..., v_n$

- Given any arbitrary element $v \in V$, there exists $\alpha_1, ..., \alpha_n \in F$ such that $v = \alpha_1 v_1 + ... + \alpha_n v_n$

1.11 Bases

A basis of a vector space V over a field F is a linearly independent spanning set of V over F

- A set $\{v_1, ..., v_n\}$ is linearly independent if $\alpha_1 v_1 + ... + \alpha_n v_n = 0$ has only the trivial solution
- The dimension of V over F is the number of elements in any basis of V over F, denoted $[V : F]$
  - Any two bases of V over F have the same number of elements

2 Geometric Constructions

2.1 Algebraic Representation of Lines

Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be distinct points in $\mathbb{R}^2$. Then

$$L(P,Q) = \{(x,y) \in \mathbb{R}^2 \mid (x - x_P)(x_Q - x_P) = (y - y_P)(y_Q - y_P)\}$$

represents a straight line through P and Q

- A line is constructible if P and Q are constructible points

2.2 Algebraic Representation of Circles

Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be distinct points in $\mathbb{R}^2$. Then

$$C(P,Q) = \{(x,y) \in \mathbb{R}^2 \mid (x - x_P)^2 + (y - y_P)^2 = (x_Q - x_P)^2 + (y_Q - y_P)^2\}$$

represents a circle whose center is P and passes through Q

- A circle is constructible if P and Q are constructible points

2.3 Constructible Points

A point $P \in \mathbb{R}^2$ is a constructible point if there exists a finite sequence of points $P_0, ..., P_n \in \mathbb{R}^2$ where $P_0 = (0,0)$, $P_1 = (1,0)$, and $P_n = P$ such that at least one of the following is true for all P_i with $i \geq 2$

- $P_i \in L(P_{i_1}, P_{i_2}) \cap L(P_{i_3}, P_{i_4})$ where $L(P_{i_1}, P_{i_2}) \neq L(P_{i_3}, P_{i_4})$
- $P_i \in C(P_{i_1}, P_{i_2}) \cap C(P_{i_3}, P_{i_4})$ where $P_{i_1} \neq P_{i_3}$
- $P_i \in L(P_{i_1}, P_{i_2}) \cap C(P_{i_3}, P_{i_4})$

where $0 \leq i_1, i_2, i_3, i_4 \leq i - 1$

2.4 Elementary Constructions

A construction is elementary if it can be accomplished using a compass and a straightedge

- Given a line L and a point P, we can construct a line L' such that $P \in L'$ and $L \perp L'$
- Given a line L and a point P, we can construct a line L' such that $P \in L'$ and $L \mid\mid L'$
- Given two lines $L(P_1, Q_1)$ and $L(P_2, Q_2)$, we can construct a point $P' \in L(P_2, Q_2)$ such that $d(P', P_2) = d(P_1, Q_1)$

2.5 Constructible Numbers

An element $r \in \mathbb{R}$ is a constructible number if $(r, 0) \in \mathbb{R}^2$ is a constructible point

- A point $(x, y) \in \mathbb{R}^2$ is constructible if and only if $x, y \in \mathscr{C}$
- The set of constructible numbers $\mathscr{C}$ is a subfield of $\mathbb{R}$
  - Let a, b, c, d be constructible numbers with $c \neq 0$ and $d > 0$. Then

    $$a + b,\ a - b,\ ab,\ a/c, \text{ and } \sqrt{d}$$

    are constructible numbers

2.6 Constructible Numbers in Subfields of $\mathbb{R}$

Let $P_i = (x_i, y_i) \in \mathbb{R}^2$ be points for $1 \leq i \leq 4$ such that $P_1 \neq P_2$ and $P_3 \neq P_4$. Let F be a subfield of $\mathbb{R}$ containing $\{x_i, y_i\}_{1 \leq i \leq 4}$ and let $P = (x, y) \in \mathbb{R}^2$

- If $P \in L(P_1, P_2) \cap L(P_3, P_4)$ where $L(P_1, P_2) \neq L(P_3, P_4)$, then $x, y \in F$
- If $P \in L(P_1, P_2) \cap C(P_3, P_4)$, then there exists some $u \in F$ such that $x, y \in F(\sqrt{u})$
- If $P \in C(P_1, P_2) \cap C(P_3, P_4)$ and $P_1 \neq P_3$, then there exists some $u \in F$ such that $x, y \in F(\sqrt{u})$

Let $[F(x, y) : F]$ denote the number of elements in any basis of $F(x, y)$ over F

- There always exists some $u \in F$ such that $x, y \in F(\sqrt{u})$
  - $[F(\sqrt{u}) : F] = 1$ if $\sqrt{u} \in F$
  - $[F(\sqrt{u}) : F] = 2$ if $\sqrt{u} \notin F$
- $F \subseteq F(x, y) \subseteq F(\sqrt{u})$ such that $[F(x, y) : F] \in \{1, 2\}$

If $\mathrm{char}(F) \neq 2$ and K/F is an extension of degree $[K : F] = 2$, then $K = F(u)$ for some $u \in K$ such that $u^2 \in F$

2.7 Constructible Real Numbers

For a real number $r \in \mathbb{R}$, the following are equivalent

- The number r is a constructible number
- There exists a finite chain of fields

$$\mathbb{Q} = F_0 \subseteq ... \subseteq F_n \subseteq \mathbb{R}$$

  such that $r \in F_n$ and $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq n$

2.8 Constructible Roots of Polynomials

- Let F be a subfield of $\mathbb{R}$ and $f(x) \in F[x]$. Suppose that $k \in F$ and $\sqrt{k} \notin F$. If $a + b\sqrt{k}$ is a root of $f(x)$, then $a - b\sqrt{k}$ is also a root of $f(x)$
- Let F be a subfield of a field K. Let $f(x), g(x) \in F[x]$ and $h(x) \in K[x]$. If $f(x) = g(x)h(x)$, then $h(x)$ is in $F[x]$
- Let $f(x)$ be a cubic polynomial in $\mathbb{Q}[x]$. If $f(x)$ has no roots in $\mathbb{Q}$, then $f(x)$ has no constructible numbers as roots

3 Field Extensions

3.1 Fields

A field is a commutative ring with identity where all non-zero elements are units

- All fields are integral domains

3.2 Field Extensions

Let F be a subfield of a field K. Then K is a field extension of F, denoted K/F or $F \subseteq K$

- F is called the base of the extension

3.3 Field Embeddings

Let F and K be fields. Then the unital ring homomorphism $\varphi : F \to K$ is a field embedding

$$\begin{tikzcd} F \arrow[r, "\varphi"] \arrow[d, "\cong"'] & K \\ \varphi(F) \arrow[ur, "\varphi(F)/K"'] & \end{tikzcd}$$

- F is isomorphic to $\varphi(F)$
- K is a field extension of $\varphi(F)$

3.4 Field Construction

Let R be a commutative ring with identity and let I be an ideal of R

- I is a prime ideal if and only if the quotient ring R/I is an integral domain
- I is a maximal ideal if and only if the quotient ring R/I is a field

Let R be a PID and let f be an irreducible element in R

- Since (f) is irreducible, (f) is a maximal ideal
- Since (f) is a maximal ideal, $R/(f)$ is a field

Let F be a field and let $f(x)$ be an irreducible polynomial in $F[x]$. Then $K = F[x]/(f(x))$ is a field extension of F which contains a root of $f(x)$

- $f(x)$ is irreducible if and only if it cannot be non-trivially factored such that $f(x) = p(x)q(x)$, where $p(x)$ and $q(x)$ are polynomials of lesser degrees

3.5 Fraction Fields

Let R be an integral domain and let $S = R \times R \backslash \{0_R\} = \{(a, b) \mid a, b \in R,\ b \neq 0_R\}$. Then the fraction field of R, denoted $\mathrm{Frac}(R)$, is the set of equivalence classes of S

- $[a, b] = \{(c, d) \in S \mid (a, b) \sim (c, d)\} = \{(c, d) \in S \mid ad = cb\}$
- $[a, b] +_{\mathrm{Frac}(R)} [c, d] = [ad + bc, bd]$
- $[a, b] \cdot_{\mathrm{Frac}(R)} [c, d] = [ac, bd]$
- Additive identity is $0_{\mathrm{Frac}(R)} = [0_R, 1_R]$
- Multiplicative identity is $1_{\mathrm{Frac}(R)} = [1_R, 1_R]$
- $\mathrm{Frac}(R)$ is a commutative ring with identity
- Fraction fields are analogous to numerical fractions in $\mathbb{Q}$

Let R be an integral domain. Then there exists an injective unital ring homomorphism $\xi : R \to \mathrm{Frac}(R)$ defined as $\xi(r) = [r, 1_R]$

- The integral domain R is isomorphic to the integral domain$\{[r, 1_R] \mid r \in R\} \subseteq \mathrm{Frac}(R)$
- Let F be a field and $\varphi : R \to F$ be an injective unital ring homomorphism
  - Then there exists a field embedding $\varphi' : \mathrm{Frac}(R) \to F$ such that $\varphi = \varphi' \circ \xi$

$$\begin{tikzcd}
R \arrow[r, "\xi"] \arrow[d, "\varphi"'] & \mathrm{Frac}(R) \arrow[dl, "\varphi'"] \\
F &
\end{tikzcd}$$

3.6 Polynomial Fraction Fields

Let F be a field. Then $F(x) = F[x] \times F[x] \backslash \{0_{F[x]}\}$ is the fraction field of $F[x]$

- All fields are integral domains
- If F is an integral domain, then $F[x]$ is also an integral domain

3.7 Residue Fields

Let R be a commutative ring with identity and let P be a prime ideal of R such that the quotient ring R/P is an integral domain. Then $\mathrm{Frac}(R/P)$ is the residue field of P

3.8 Field Characteristic

Let F be a field and let $\varepsilon_F : \mathbb{Z} \to F$ be the unique unital ring homomorphism between $\mathbb{Z}$ and F. Then $\mathrm{Ker}(\varepsilon_F)$ is the characteristic of F, denoted $\mathrm{char}(F)$

- $\mathrm{Ker}(\varepsilon_F) = (\ell)$ where ℓ is either 0 or a positive prime
  - If $\mathrm{char}(F) = 0$, then F is an extension of the field $\mathbb{Q}$
  - If $\mathrm{char}(F) = p$, then F is an extension of the field $\mathbb{F}_p$
  - The prime subfield of F is the field that F is an extension of
  - The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ have characteristic 0 and prime subfield $\mathbb{Q}$
- If K/F is a field extension, then $\mathrm{char}(K) = \mathrm{char}(F)$
- If $K \cong F$, then $\mathrm{char}(K) = \mathrm{char}(F)$
- If F and K are fields with a field embedding $\varphi : F \to K$, then $\mathrm{char}(F) = \mathrm{char}(K)$
- There exists an injective ring homomorphism $\varphi : \mathbb{Z}/\mathrm{Ker}(\varepsilon_F) \to F$
- $\mathbb{Z}/\mathrm{Ker}(\varepsilon_F)$ is an integral domain

3.9 Degree of a Field Extension

Let K/F be a field extension where K is a vector space over F. Then the degree of the extension K/F is the dimension of K as an F-vector space, denoted $[K : F] = \dim_F K$

- If $[K : F]$ is finite, then K/F is a finite extension
- $[K : F] \geq 1$ for all field extensions K/F
- $[K : F] = 1$ if and only if $K = F$

Let $F \subseteq K \subseteq L$ be field extensions

- If $V = \{v_1, ..., v_n\}$ is an F-basis for K and $W = \{w_1, ..., w_m\}$ is a K-basis for L, then $U = \{v_i w_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$ is an F-basis for L
  - V is an F-basis for K such that $V \subseteq K$ and W is a K-basis for L such that $W \subseteq L$
- $[L : F] = [L : K][K : F]$

3.10 Simple Extensions

Let K/F be a field extension and let S be a subset of K. Then $F(S)$ is the intersection of all subfields of K that contain F and S

- Let $u_1, ..., u_n$ be elements of K. Then $F(u_1, ..., u_n)$ is the intersection of all subfields of K that contain $u_1, ..., u_n$
  - $F(u_1, ..., u_n) = (F(u_1, ..., u_{n-1}))(u_n)$
- $F(S)$ is the smallest subfield of K that contains F and all elements of S
- If S is a finite set, then $F(S)$ is a finitely generated extension of F
- If $|S| = 1$, then $F(S)$ is a simple extension of F
- If $S \subseteq F$, then $F = F(S)$

3.11 Algebraic and Transcendental Elements

Let K/F be a field extension and let u be an element in K. Let $\varphi_u : F[x] \to K$ be the F-homomorphism defined as $\varphi(x) = i$

- If u is the root of some non-zero polynomial in $F[x]$, then u is algebraic over F
  - Alternately, if φ_u is injective, then u is algebraic over F
- If u is not the root of any non-zero polynomial in $F[x]$, then u is transcendental over F
  - Alternately, if φ_u is not injective, then u is transcendental over F

If u is transcendental over F, then there exists an F-isomorphism $\varphi : F(x) \to F(u)$ defined as $\varphi(x) = u$

3.12 Algebraic Extensions

Let K/F be a field extension where every element of K is algebraic over F. Then K/F is an algebraic extension

- All finite extensions are algebraic extensions
- If $F(u_1, ..., u_n)$ is a finitely generated extension field of F and each u_i is algebraic over F, then $F(u_1, ..., u_n)$ is a finite-dimensional algebraic extension of F
- Let K/F be a field extension and let $E \subseteq K$ be the subset of elements of K that are algebraic over F. Then E is an algebraic extension of F
- Let $F \subseteq K \subseteq L$ be field extensions. If L/K and K/F are algebraic extensions, then L/F is an algebraic extension

3.13 Algebraic Closure

A field extension K/F is an algebraic closure of F if

- K/F is an algebraic extension
- K is algebraically closed such that every non-constant polynomial $f(x) \in K[x]$ has a root in K

For any field F, the following existence and uniqueness properties hold

- There exists an algebraic closure K/F of F
- Given two algebraic closures K_1/F and K_2/F of F, there exists an F-isomorphism $K_1 \cong K_2$

3.14 Minimal Polynomial

Let K/F be a field extension and let $u \in K$ be algebraic over F. Since $F[x]$ is a PID, there exists a unique monic polynomial

$$m_{u,F} \in F[x]$$

such that $\ker(\varphi_u) = (m_{u,F})$ are ideals of $F[x]$. This is the minimal polynomial of u over F

- The minimal polynomial of an element $u \in F$ is the monic polynomial $p(x)$ over a field F such that $p(u) = 0$
  - If u is a root of $g(x) \in F[x]$, then $p(x)$ divides $g(x)$
- Let K/F be a field extension and let $u \in K$ be algebraic over F with minimal polynomial $m_{u,F} \in F[x]$. Then
  - There exists an F-isomorphism $F[x]/(m_{u,F}) \cong F(u)$
  - The set $\{1, u, ..., u^{\deg(m_{u,F})-1}\}$ is an F-basis of $F(u)$
  - $[F(u) : F] = \deg(m_{u,F})$
- If u and v have the same minimal polynomial $p(x)$ in $F[x]$, then $F(u)$ is isomorphic to $F(v)$
- Let $F_1 \subseteq F_2 \subseteq K$ be field extensions and let $u \in K$ be algebraic over F_1. Then u is also algebraic over F_2 and $m_{u,F_2} \mid m_{u,F_1}$ in $F_2[x]$
  - $\deg(m_{u,F_2}) \leq \deg(m_{u,F_1})$
- The degree of u over F is given by $\deg(m_{u,F})$

3.15 Computing $[K : F]$

Given an extension K/F, the degree $[K : F]$ can be computed as $[K : F(u)][F(u) : F]$ as follows

1. Find some monic polynomial $f(x) \in F[x]$ such that $f(u) = 0$
   - Then u is algebraic over F
2. Prove that $f(x)$ is irreducible
   - Then $m_{u,F} = f(x)$ such that $[F(u) : F] = \deg(f(x))$

We can show that a monic polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible as follows

1. Check for roots using the rational roots theorem
   - This shows that $f(x)$ is irreducible only when $\deg(f(x)) = 2$ or 3
2. Use Eisenstein's criterion
   - This may require a change of coordinates, where $f(x)$ is replaced by $f(x+n)$ for some $n \in \mathbb{Z}$
3. Consider the image $\bar{f}(x) \in \mathbb{F}_p[x]$ for a carefully chosen p
   - If $\bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$
4. Brute force
   - This may be reasonable if many of the coefficients of $f(x)$ are 0

3.16 Additional Theorems

- Let K/F be a field extension and let $u_1, ..., u_n \in K$ be algebraic over F. Then

$$\begin{aligned}[F(u_1, ..., u_n) : F] &= [F(u_1, ..., u_n) : F(u_1, ..., u_{n-1})]...[F(u_1, u_2) : F(u_1)][F(u_1) : F] \\ &= \deg(m_{u_n, F(u_1, ..., u_{n-1})}) \cdot ... \cdot \deg(m_{u_2, F(u_1)}) \cdot \deg(m_{u_1, F})\end{aligned}$$

- Let F be a field with $\mathrm{char}(F) \neq 2$ and let $a, b \in F$ be elements such that a, b, ab are not squares in F. For any K/F containing $\sqrt{a}, \sqrt{b}, \sqrt{ab}$, the set $\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$ is linearly independent over F such that $[F(\sqrt{a}, \sqrt{b}) : F] = 4$
- Let K/F be a field extension and let $u_1, u_2 \in K$ be algebraic over F. Let $d_1 = \deg(m_{u_1,F})$ and $d_2 = \deg(m_{u_2,F})$. Then $[F(u_1, u_2) : F] = d_1 d_2$ if $\gcd(d_1, d_2) = 1$

3.17 Splitting Functions

Let K/F be a field extension and let $f(x) \in F[x]$ be a monic polynomial. Then $f(x)$ splits over the field K if there exists elements $u_1, ..., u_n \in K$ such that $f(x) = (x - u_1)...(x - u_n)$ in $K[x]$

3.18 Splitting Fields

Let F be a field and let $f(x) \in F[x]$ be a polynomial. Then a splitting field of $f(x)$ over F is an extension K/F such that

- $f(x)$ splits over K
- $K = F(u_1, ..., u_n)$
- If $F \subseteq E \subseteq K$ and $f(x)$ splits over E, then $E = K$

K is the smallest extension field that contains all the roots of $f(x)$

- Let F be a field and let $f(x) \in F[x]$ be a non-constant polynomial with $\deg(f(x)) = n$. Then there exists a splitting field K of $f(x)$ over F such that $[K : F] \leq n!$
- Let F be a field, let $f(x) \in F[x]$ be a polynomial, and let K/F be a splitting field of $f(x)$ over K. For any extension $F \subseteq E \subseteq K$, the extension K/E is a splitting field of $f(x)$ over E
- Let F be a field and $p(x)$ be an irreducible polynomial in $F[x]$. Then $F[x]/p(x)$ is an extension field of F that contains a root $\alpha = [x]$ of $p(x)$

3.19 Extension Lemma

Let $\phi : F_1 \to F_2$ be an isomorphism of fields. For $i = 1, 2$, let K_i/F_i be a field extension and let $u_i \in K_i$ be algebraic over F_i with minimal polynomial $m_{u_i,F_i} \in F_i[x]$. If $\phi(m_{u_1,F_1}) = m_{u_2,F_2}$, then there exists a unique isomorphism $\phi' : F_1(u_1) \to F_2(u_2)$ such that $\phi'(u_1) = u_2$ and ϕ' extends ϕ

- Any two splitting fields of a polynomial in $F[x]$ are isomorphic

3.20 Normal Extensions

An algebraic extension K/F is a normal extension if whenever an irreducible polynomial $f(x) \in F[x]$ has a root in K, then it splits over K

- K/F is a normal extension if the minimal polynomial $m_{u,F} \in F[x]$ splits over K for every $u \in K$
- Let K/F be a finite extension. Then the following are equivalent
  - The extension K/F is a splitting field for some polynomial $f(x) \in F[x]$
  - The extension K/F is a normal extension

3.21 Derivatives

Let F be a field and let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial in $F[x]$. Then $f'(x) = \sum_{i=1}^{n} i \cdot a_i x^{i-1}$ is the derivative of $f(x)$

- If $c \in F$ and $f(x) \in F[x]$, then $(c \cdot f(x))' = c \cdot f'(x)$
- If $f(x), g(x) \in F[x]$, then $(f(x) + g(x))' = f'(x) + g'(x)$
- If $f(x), g(x) \in F[x]$, then $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

3.22 Separable Polynomials

Let F be a field and let $f(x)$ be a polynomial in $F[x]$ of degree n. Then $f(x)$ is separable if there exists an extension K/F such that $f(x)$ splits over K and $f(x)$ has n distinct roots

- Let $f'(x) \in F[x]$ be the derivative of $f(x)$. Then $f(x)$ is separable if and only if $\gcd(f(x), f'(x)) = 1$
- Let $f(x) \in F[x]$ be a monic irreducible polynomial. Then $f(x)$ is separable if and only if $f'(x)$ is non-zero

3.23 Separable Elements

Let K/F be a field extension and let $u \in K$ be algebraic over F. Then u is a separable element over F if its minimal polynomial $m_{u,F} \in F[x]$ is a separable polynomial

- An algebraic extension K/F is a separable extension if every element $u \in K$ is separable over F
- Let F be a field of $\mathrm{char}(F) = 0$. Then
  - Every irreducible polynomial $f(x) \in F[x]$ is separable
  - Every algebraic extension K/F is a separable extension

3.24 Primitive Element Theorem

Let K/F be a finite separable extension. Then there exists some $u \in K$ such that $K = F(u)$

- Let K/F be an extension of finite fields. Then there exists some $u \in K$ such that $K = F(u)$
- Given $K = F(v, w)$

    Let $m_{v,F} \in F[x]$ and $m_{v,F} \in F[x]$ be the minimal polynomials of v and w respectively
    Let $v_1, ..., v_m$ be the roots of $m_{v,F}$ and let $w_1, ..., w_n$ be the roots of $m_{w,F}$

  Then $F(v, w) = F(u)$ for some $u = v + cw$ with $c \notin \left\{ \frac{v_i - v_1}{w_1 - w_j} \,\middle|\, 1 \le i \le m,\ 1 < j \le n \right\}$

  - It is usually the case that we can choose $c = 1$ such that $F(u) = F(v + w)$

3.25 Finite Fields

Let F be a field. Then F is finite if F contains a finite number of elements

- If F is a finite field, then $\operatorname{char}(F) = p$ for some prime p
- If F is a finite field, then $|F| = p^n$ where $p = \operatorname{char}(F)$ and $n = [F : \mathbb{F}_p]$
- Let F be a field of $\operatorname{char}(F) = p$. For any positive integer n, the subset

  $$F' = \{u \in F \mid u^{(p^n)} = u\}$$

  is a subfield of F
- Let p be a prime and let n be a positive integer. Then there exists a field F of order p^n
  - If F_1, F_2 are both fields of order p^n, then $F_1 \cong F_2$
- Let F be a finite field where $p = \operatorname{char}(F)$ and let $n \in \mathbb{Z}^+$. Then $(a+b)^{(p^n)} = a^{(p^n)} + b^{(p^n)}$
- Let K/F be an extension of finite fields. Then the extension K/F is normal and separable
- Let K be a field and let $G \subseteq K^\times$ be a finite subgroup. Then G is cyclic

3.26 Magic Polynomials Over Finite Fields

- Let p be a prime. Then the polynomial $x^{(p^n)} - x \in \mathbb{F}_p[x]$ is separable
  - If $m \mid n$, then $\left(x^{(p^m)} - x\right) \,\Big|\, \left(x^{(p^n)} - x\right)$
- Let F be a finite field where $p = \operatorname{char}(F)$. Then the following are equivalent
  - $|F| = p^n$
  - The extension $F/\mathbb{F}_p$ is a splitting field of $x^{(p^n)} - x$ over $\mathbb{F}_p$
  - The extension $F/\mathbb{F}_p$ is exactly the set of roots of $x^{(p^n)} - x$
- Let p be a prime. For any positive integer n, there exists a monic irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $\deg(f(x)) = n$
- Let p be a prime. Then for any positive integer n the following holds

  $$x^{(p^n)} - x = \prod_{d \mid n,\ f(x) \in M_d} f(x)$$

  in $\mathbb{F}_p[x]$, where M_d is the set of monic irreducible polynomials of degree d in $\mathbb{F}_p[x]$

3.27 Prime Power Order Fields

The field $\mathbb{F}_{p^n}$ of order p^n is unique up to isomorphism

- If $|F| = p^n$, then $F \cong \mathbb{F}_{p^n}$
- $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$

4 Galois Theory

4.1 Automorphism Groups

Let K be a field. Then the set of field automorphisms $\varphi : K \to K$ is denoted $\mathrm{Aut}(K)$

- $\mathrm{Aut}(K)$ is a group under function composition
- Let K/F be a field extension. Then an automorphism $\varphi \in \mathrm{Aut}(K)$ is an F-automorphism if $\varphi(a) = a$ for all $a \in F$
- Let K/F be a field extension. Then

  $$\mathrm{Aut}(K/F) = \{\varphi \in \mathrm{Aut}(K) \mid \varphi(a) = a \text{ for all } a \in F\}$$

  is the set of F-automorphisms of K

  - $\mathrm{Aut}(K/F)$ is a subgroup of $\mathrm{Aut}(K)$
- Let K/F be a field extension and let $\varphi \in \mathrm{Aut}(K/F)$. If $u \in K$ is a root of $f(x) \in F[x]$, then $\varphi(u) \in K$ is also a root of $f(x)$
- Let $f(x) \in F[x]$ be monic irreducible over F and let K/F be the splitting field of $f(x)$ over F. If $u, v \in K$ are two roots of $f(x)$, then there exists some $\varphi \in \mathrm{Aut}(K/F)$ such that $\varphi(u) = v$
- Let K/F be a field extension with $K = F(u_1, ..., u_n)$ for some $u_1, ..., u_n \in K$ and let $\varphi_1, \varphi_2 \in \mathrm{Aut}(K/F)$. If $\varphi_1(u_i) = \varphi_2(u_i)$ for all $i = 1, ..., n$, then $\varphi_1 = \varphi_2$
- If K/F is a finite extension, then $\mathrm{Aut}(K/F)$ is a finite group
- Let F be a field, let $f(x) \in F[x]$ be a polynomial, and let K/F be a splitting field of $f(x)$ over F. If there are n distinct roots of $f(x)$ in K, then there is an injective group homomorphism

  $$\mathrm{Aut}(K/F) \to S_n$$

  where S_n is the symmetric group of degree n

  - $|\mathrm{Aut}(K/F)| \leq n!$
- Let F be a field, let $f(x) \in F[x]$ be a polynomial, and let K/F be a splitting field of $f(x)$ over F. Then

  $$|\mathrm{Aut}(K/F)| \leq [K : F]$$

  - If $f(x)$ is separable, then $|\mathrm{Aut}(K/F)| = [K : F]$
- Let K be a field and let $\varphi_1, ..., \varphi_n \in \mathrm{Aut}(K)$ be distinct automorphisms of K. Then $\{\varphi_1, ..., \varphi_n\}$ is linearly independent over K
- Let K be a field, let $\varphi_1, ..., \varphi_n \in \mathrm{Aut}(K)$ be automorphisms, and let $G \subseteq \mathrm{Aut}(K)$ be the subgroup generated by the φ_i. Then

  $$K^G = \{a \in K \mid \varphi_i(a) = a \text{ for all } i = 1, ..., n\}$$

  is a subfield of K

4.2 Fixed Fields

Let K be a field and let $G \subseteq \mathrm{Aut}(K)$ be a subgroup. Then the fixed field of G is given by

$$K^G = \{a \in K \mid \varphi(a) = a \text{ for all } \varphi \in G\}$$

- K^G is a subfield of K
- Let K be a field and let G be a finite subgroup of $\mathrm{Aut}(K)$. Then
  - The extension K/K^G is a finite extension and its degree is $[K : K^G] = |G|$
  - The extension K/K^G is separable and normal

4.3 Galois Correspondence

Let K be a field. Then there exists functions

$$f : \{\text{subgroups of } \mathrm{Aut}(K)\} \to \{\text{subfields of } K\} \text{ defined by } f(G) = K^G$$
$$g : \{\text{subfields of } K\} \to \{\text{subgroups of } \mathrm{Aut}(K)\} \text{ defined by } g(F) = \mathrm{Aut}(K/F)$$

where G is a subfield of $\mathrm{Aut}(K)$ and F is a subfield of K

- If $G_1 \subseteq G_2$ are two subgroups of $\mathrm{Aut}(K)$, then $K^{G_2} \subseteq K^{G_1}$
- If $F_1 \subseteq F_2$ are two subgroups of K, then $\mathrm{Aut}(K/F_2) \subseteq \mathrm{Aut}(K/F_1)$
- Let F be a subfield of a field K. Then $F \subseteq (f \circ g)(F)$ such that $F \subseteq K^{\mathrm{Aut}(K/F)}$
- Let G be a subgroup of $\mathrm{Aut}(K)$. Then $G \subseteq (g \circ f)(G)$ such that $G \subseteq \mathrm{Aut}(K/K^G)$
- If K/F is a finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$
- If $G \subseteq \mathrm{Aut}(K)$ is a finite subgroup, then $G = \mathrm{Aut}(K)$

4.4 Galois Extension

Let K/F is a finite extension. Then the following are equivalent

- K/F is separable and normal
- K is the splitting field of a separable polynomial $f(x) \in F[x]$
- $|\mathrm{Aut}(K/F)| = [K : F]$
- $F = K^{\mathrm{Aut}(K/F)}$

K/F is a Galois extension if it satisfies the above conditions

4.5 Fundamental Theorem of Galois Theory

Let K/F be a Galois extension. Then the following properties hold

- The Galois correspondence functions f, g satisfy $f \circ g = g \circ f = Id$
- A subgroup $G \subseteq \mathrm{Aut}(K/F)$ is a normal subgroup if and only if K^G/F is a normal extension
- If $F \subseteq E \subseteq K$ are field extensions and E/F is normal, then

  $$\mathrm{Aut}(K/F) \big/ \mathrm{Aut}(K/E) \cong \mathrm{Aut}(E/F)$$

  where $\mathrm{Aut}(K/F) \big/ \mathrm{Aut}(K/E)$ is a quotient group
- There exists a bijection between the set of all intermediate fields of K/F and the set of all subgroups of $\mathrm{Aut}(K/F)$
- An intermediate field E is a normal extension of F if and only if $\mathrm{Aut}(K/E)$ is a normal subgroup of $\mathrm{Aut}(K/F)$

4.6 Inverse Galois Conjecture

For every finite group G, there exists a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Aut}(K/\mathbb{Q}) \cong G$

5 Solvability

5.1 Radical Extensions

Let K/F be a finite extension. Then K/F is a radical extension if there exists a chain of fields

$$F = F_0 \subseteq F_1 \subseteq ... \subseteq F_t = K$$

such that there exists some $u_i \in F_i$ where $F_i = F_{i-1}(u_i)$ and some positive power of u_i is in F_{i-1} for all $i = 1, ..., t$

- If $F_1 \subseteq F_2 \subseteq F_3$ are field extensions such that F_3/F_2 and F_2/F_1 are radical, then F_3/F_1 is radical
- If K/F is a field extension such that $K = F(u_1, ..., u_t)$ for some $u_1, ..., u_t \in K$ and some positive power of u_i is in F for all $1 \leq i \leq t$, then K/F is radical

5.2 Solvability By Radicals

Let $f(x) \in F[x]$. Then $f(x)$ is solvable by radicals if there exists a radical extension K/F such that $f(x)$ splits over K

5.3 Roots of Unity Group

Let F be a field and let $\mu_n(F) = \{\xi \in F \mid \xi^n = 1_F\}$ be the set of all n^{th} roots of unity in F. Then $\mu_n(F)$ is a subgroup of $F^\times$ of order at most n

- If $|\mu_n(F)| = n$, then $n \neq 0$ in F such that either $\operatorname{char}(F) = 0$ or $\operatorname{char}(F) \nmid n$
- If $n \neq 0$ in F, then there exists an extension K/F such that $|\mu_n(K)| = n$

5.4 Primitive Roots of Unity

Let $\xi \in \mu_n(F)$ be an n^{th} root of unity. Then ξ is a primitive root of unity if $|\xi| = n$

- $|\xi| = n$ if and only if $\xi^n = 1_F$ and $\xi^i \neq 1_F$ for all $1 \leq i < n$
- If F is a field and K/F is an extension containing a primitive n^{th} root of unity $u \in K$, then $F(u)/F$ is a Galois radical extension of F and $\operatorname{Aut}(F(u)/F)$ is an abelian group
  - K/F is not necessarily a field extension
- If F is a field containing a primitive n^{th} root of unity and K/F is a field extension such that $K = F(u)$ for some $u \in K$ with $u^n \in F$, then K/F is a Galois radical extension and $\operatorname{Aut}(K/F)$ is an abelian group
- If F is a field of $\operatorname{char}(F) = 0$ and K/F is a radical extension, then there exists an extension L/K such that L/F is a Galois radical extension

5.5 Solvable Groups

Let G be a finite group. Then G is a solvable group if there exists a chain of subgroups

$$\{e\} = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

such that the group G_{i-1} is a normal subgroup of G_i and the quotient G_i/G_{i-1} is abelian for all $i = 1, ..., n$

- If G is a solvable group, then any subgroup of G is a solvable group
- If G is a solvable group and $f : G \to H$ is a group homomorphism, then $f(G)$ is a solvable group
- If G is a finite simple non-abelian group, then G is not solvable
- For any $n \geq 5$, the symmetric group S_n is not solvable
- If F is a field of $\mathrm{char}(F) = 0$ and K/F is a Galois radical extension, then $\mathrm{Aut}(K/F)$ is a solvable group

5.6 Galois Groups

Let $f(x) \in F[x]$ be a polynomial and let K/F be a splitting field of $f(x)$ over F. Then the automorphism group $\mathrm{Aut}(K/F)$ is the Galois group of $f(x)$

5.7 Galois' Criterion

Let F be a field of $\mathrm{char}(F) = 0$ and let $f(x) \in F[x]$ be a polynomial. Then $f(x)$ is solvable by radicals if and only if the Galois group of $f(x)$ is a solvable group

- Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of $\deg(f(x)) = n$ for some $n \geq 5$. If the Galois group of $f(x)$ is S_n, then $f(x)$ is not solvable by radicals

5.8 Additional Theorems

- Let G be a subgroup of S_n that contains an n-cycle and a 2-cycle. Then $G = S_n$