MATH 3962 - RINGS, FIELDS AND GALOIS THEORY EXAM NOTES

ANDREW TULLOCH

1. Background Theory

Definition 1.1 (Monoids)**.** A monoid is a set S equipped with a single operation $\cdot$ obeying the following axioms

- **Closure** For all $a, b \in S$, $a \cdot b \in S$
- **Associativity** For all $a, b, c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Identity** There exists an element e in S such that $e \cdot a = a = a \cdot e$ for all $a \in S$.

Definition 1.2 (Groups)**.** A group is a set equipped with an operation $\cdot$ obeying the axioms of associativity, existence of inverses, and existence of an identity.

Definition 1.3 (Abelian Groups)**.** An abelian group is a group where the operation $\cdot$ is commutative.

Definition 1.4 (Cyclic Groups)**.** A cyclic group is a group that can be generated by a single element $\langle x \rangle = \{x^n \mid x \in \mathbb{Z}\}$

Definition 1.5 (Subgroup)**.** A subset H of a group G is a subgroup of G if and only if H is non-empty and for all $x, y \in G$

- If $x, y \in H$ then $x \cdot y \in H$
- If $x \in H$ then $x^{-1} \in H$.

Definition 1.6 (Normal Subgroup)**.** A subgroup K of a group G is said to be **normal** in G if $g^{-1}kg \in K$ for all $k \in K$ and $g \in G$. Equivalently, the subgroup K is normal in G if $g^{-1}Kg = K$, or $gK = Kg$ for all $g \in G$.

Definition 1.7 (Quotient Group)**.** If G is a group and H is a subgroup, we can form the **quotient group** G/H as follows. Defining the equivalence relation   as follows: for all $x, y \in G$,

$$x \sim y if x = yh$$

for some $h \in H$. The set

$$xH = \{xh \mid h \in H\}$$

is called the left coset containing x. These cosets partition G, and the number of cosets of H in G is denoted by $[G : H]$. By **Lagrange's Theorem**, we have

$$[G : H] = \frac{|G|}{|H|}$$

Now, letting K be a normal subgroup of G, we have the following. THe set of al cosets in G forms a group, with multiplication satisfying $(xK)(yK) = xyK$ for all $x, y \in G$.

Definition 1.8 (Solvable Groups)**.** A group G is **solvable** if there is a chain of subgroups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_s = G$$

where each G_i is normal in G_{i+1} and the quotient groups G_{i+1}/G_i is abelian for all i.

Corollary 1.9. The finite group G is solvable if and only if for every divisor n of $|G|$ with $\gcd(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n.

Corollary 1.10. Let N be normal in G. If N and G/N are solvable, then G is solvable.

Theorem 1.11 (Subgroups of Cyclic Groups)**.** *Let $G = \langle x \rangle$ be a cyclic group. Then we have the following.*

- *Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.*
- *If $|H| = \infty$, then if $a \neq b$, then $\langle x^a \rangle \neq \langle x^b \rangle$.*
- *If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \frac{n}{a}$. Furthermore, the subgroups of H correspond bijectively with the positive divisors of n.*

Definition 1.12 (Homomorphism of Groups)**.** A map $\varphi : G \to H$ is a homomorphism if and only if

- $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$

Definition 1.13 (Isomorphism of Groups)**.** A map $\varphi : G \to H$ is an isomorphism of groups if and only if

- φ is a homomorphism.
- φ is a bijection.

Definition 1.14 (Symmetric Groups)**.** The symmetric group of order n is the set of all permutations of the finite set $\{1, 2, \ldots, n\}$, with the operation being composition of permutations.

Proposition 1.15 (Properties of the Symmetric Groups)**.** *Let S_n be the symmetric group of order n. Then we have*

- $|S_n| = n!$

- *S_n is non-abelian for all $n \geq 3$.*

Definition 1.16 (Elementary Symmetric Functions)**.** Let $x_1, x_2, \ldots, x_n$ be indeterminates. Then the **elementary symmetric functions** $s_1, x_2, \ldots, s_n$ are defined by

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_2x_3 + x_2x_4 + \cdots x_{n-1}x_n \\ s_n &= x_1x_2 \cdots x_n \end{aligned}$$

Definition 1.17 (Symmetric functions)**.** A function $f(x_1, x_2, \ldots, x_n)$ is called **symmetric** if it is not changed by any permutation of the variables $x_1, x_2, \ldots, x_n$.

1.1. **Solving Polynomial Equations.** We have explicit solutions for solving polynomials of degrees two and three. Polynomials of degree two are solved using the quadratic equation. Polynomials of degree three are solvable using **Cardano's Method**

2. General Ring Theory

Definition 2.1 (Rings)**.** A **ring** R is a set equipped with two binary operations $+$ and $\times$ satisfying the following axioms

- (R,+) is an **abelian group -** impyling the existence of negatives, a zero element, and commutative addition.
- $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$
- Multiplication distributes over addition:

$$(a + b) \times c = (a \times c) + (b \times c) \qquad c \times (a + b) = (c \times a) + (c \times b)$$

A ring is **commutative** if multiplication is commutative.

A ring is said to contain an identity if there is an alement $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$.

Definition 2.2 (Zero divisors)**.** A non-zero element $a \in R$ is called a zero divisor if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

Definition 2.3 (Field)**.** A field can be defined in several ways.

- A field is a commutative ring F with identity $1 \neq 0$ such that every non-zero element $a \in F$ has a multiplicative inverse.
- A field is a commutative ring F with identiy $1 \neq 0$ in which every nonzero element is a unit, i.e. $F^\times = F - \{0\}$.

Definition 2.4 (Unit)**.** Assume a ring R has identity $1 \neq 0$. Then an element u of R is called a **unit** if there is some $v \in R$ such that $uv = vu = 1$. The set of units in R is denoted $R^\times$. Te set of units in R form a group under multiplication, denoted the **group of units** of R.

Definition 2.5 (Integral Domain)**.** An integral domain is a commutative ring with identity $1 \neq 0$ with no zero divisors.

Corollary 2.6 (Cancellation property)**.** Let R be an integral domain. Then for any $a, b, c \in R$, if $ab = ac$, then either $a = 0$ or $b = c$. ab = ac

Corollary 2.7. Any finite integral domain is a field.

Definition 2.8 (Subring)**.** A subring of a ring R is a subgroup of R that is closed under multiplication. Alternatively, a subset S of a ring R is a subring if the operations of addition and multiplication in R when restricted to S gives S the structure of a ring.

Corollary 2.9. To show a subset of a ring R is a subring it suffices to check that it is **nonempty** and **closed under subtraction and under multiplication**.

Definition 2.10 (Characteristic of a Ring)**.** The characteristic of a ring, $\mathrm{char}(R)$, is defined as the smallest positive number n such that $n \times 1 = 0$

Example 2.11 (Examples of Rings)**.** The set of all $n \times n$ matrices over a ring R is a ring, denoted by $\mathrm{Mat}_n(R)$.

Let x be indeterminate, and let R be a commutative ring with identity $1 \neq 0$. The set of all formal sums

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in R$ is the **polynomial ring** $R[x]$.

2.1. **Homomorphisms, kernels, images.** This section deals with maps between rings R and S.

Definition 2.12 (Homomorphisms of Rings)**.** Let $\varphi : R \to S$ be a map between two rings R and S. Then φ is a ring homomorphism if and only if

- $\varphi(a + b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $f(1) = 1$

Corollary 2.13. The image of a ring homomorphism φ is a subring of S.

Definition 2.14 (Kernel of a Homomorphism)**.** The kernel of a ring homomorphism φ, denoted $\ker \varphi$, is the set of elements R that maps to $0 \in S$, i.e. the set of all $a \in R$ such that $\varphi(a) = 0$.

Corollary 2.15. The kernel of a homomorphism φ is a subring of R. Furthermore, if $\alpha \in \ker \varphi$, then $r\alpha$ an $\alpha r \in \ker \varphi$ for all $r \in R$, i.e, $\ker \varphi$ is closed under multiplication by elements in R.

Example 2.16. Let R be a subring of a commutative ring T, and let $\alpha \in T$. Then the function $\mathrm{eval}_\alpha : R[x] \to T$ is a homomorphism.

2.2. **Ideals, Quotient Rings, and Isomorphisms.**

Definition 2.17 (Ideal of a Ring)**.** A subset I of a ring R is an ideal of R if and only if the following conditions all hold.

- I is nonempty
- $a+b \in I$ for al $a, b \in I$
- $-x \in I$ for all $x \in I$
- $ax, xa \in I$ for all $x \in I$ and $a \in R$.

Corollary 2.18. The kernel of a homomorphism φ is an ideal of R.

Proposition 2.19 (Cosets of an Ideal)**.** *Let I e an ideal in a ring R. The equivalence relation $\equiv$ defined by $a \equiv b$ if and only if $a - b \in I$ is an equivalence relation on the ring R, partioning the ring into a set of equivalence classes $r + I$ with $r \in R$ called the **cosets** of I in R*

Definition 2.20 (Quotient Ring)**.** Let R be a ring and let I be an ideal of R. Then the additive quotient group R/I is a ring under the binary operations:

- $(r+I)+(s+I) = (r+s)+I$
- $(r+I)\times(s+I) = (rs)+I$

The elements of R/I are precisely the cosets of I in R.

Theorem 2.21. *Let I be an ideal in the ring R. Then the mapping $\varphi : R \to R/I$ given by $\varphi(\alpha) = \alpha + I$ is a surjective homomorphism with kernel I.*

We can collect these results into the following theorem, known as the **First Isomorphism Theorem**.

Theorem 2.22 (First Isomorphism Theorem)**.** *Let R and S be rings, and $\varphi : R \to S$ a homomorphism of rings. Then the kernel of φ is an ideal of R, the image of φ is a subring of S, and there is an isomorphism $\psi : R/\ker\varphi \to \varphi(R)$ such that $\psi(r + \ker\varphi) = \varphi(r)$.*

Theorem 2.23 (Second Isomorphism Theorem)**.** *Let R be a ring. Let S be a subring and let I be an ideal of R. Then $S + I = \{s + i \,|\, s \in S, i \in I\}$ is a subring of R, $S \cap I$ is an ideal of S, and $(S+I)/I$ is isomorphic to $S/(S \cap I)$.*

Theorem 2.24 (Third Isomorphism Theorem)**.** *Let I and J be ideas of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I)$ is isomorphic to R/J.*

2.3. **Classification of Ideals.**

Proposition 2.25 (Sum, Product, Intersection of Ideals)**.** *Let I and J be ideals of R. Then*

- *The sum of I and J, $I+J$, is equal to $\{a+b \,|\, a \in I, b \in J\}$.*

- *The product of I and J, IJ, is equal to the set of all finite sums of elements of the form ab with $a \in I$, $b \in J$.*
- *The intersection of ideals, $I \cap J$, is defined simply as $I \cap J$.*

It can be shown that the sum $I + J$ of ideal I and J is the smallest ideal of r containing both I and J, and the product IJ is an ideal contained in $I \cap J$, but can be strictly smaller.

Corollary 2.26. Let $I = a\mathbb{Z}, J = b\mathbb{Z}$. Then we have $I + J = d\mathbb{Z}$, where $d = \mathrm{GCD}(a, b)$. We also have that $IJ = ab\mathbb{Z}$, and $I \cap J = \mathrm{LCM}(a, b)$

Definition 2.27 (Principal Ideal)**.** Let R be a commutative ring. An ideal that can be generated by a single element, of the form aR for some $a \in R$, is called a **principal ideal**.

Corollary 2.28. Every ideal in the ring $\mathbb{Z}$ is principal.

Proposition 2.29. *Let I be an ideal of a ring R. Then $I = R$ if and only if I contains a unit*

Proposition 2.30. *Let I be an ideal of a commutative ring R. Then R is a field if and only if its only ideals are* 0 *and R.*

Definition 2.31 (Maximal Ideal)**.** An ideal M in an arbitary ring S is called a **maximal ideal** if $M \neq S$ and the only ideals containing M are M and S.

Proposition 2.32. *Asume R is commutative. Then the idela M is a maximal ideal if and only if the quotient ring R/M is a field.*

Definition 2.33 (Prime Ideal)**.** Assume R is commutative. An ideal P is called a **prime ideal** if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

The definition is motivated by the following example. Let n be a nonnegative integer. Then $n\mathbb{Z}$ is a **prime** ideal provided $n \neq 1$ and every time the product ab of two integers is an element of $n\mathbb{Z}$, at least one of a, b is an element of $n\mathbb{Z}$. This is equivalent to stating that whenever n divides ab, n must divide a or divide b. Thus, n must be prime. Thus, **the prime ideals of $\mathbb{Z}$ are simply the ideal $p\mathbb{Z}$ of $\mathbb{Z}$ generated by prime numbers p together with the ideal 0.**

Proposition 2.34. *Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.*

Corollary 2.35. Assume R is commutative. Then every maximal ideal of R is a prime ideal.

Proof. If M is a maximal ideal then R/M is a field. As a field is an integral domain, we thus have that R/M is an integral domain, and thus M is a prime ideal. □

3. Integral Domains

Definition 3.1 (Field of Fractions)**.** Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors, and is closed under multiplication. Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit of Q. The ring Q has the following additional properties.

- Every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$, then Q is a field.
- The ring Q is the **smallest** ring containing R in which all element of D become units, in the following sense - Any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Definition 3.2 (Divisibility)**.** Let R is a commutative ring. Let $a, b \in R$. Then we say that a divides b if and only if $b = ca$ for some $c \in R$. We write $a|b$ if a divides b.

Definition 3.3 (Units, Irreducibles, Primes, Associates)**.** Let R be an integral domain - a commutative ring with $1 \neq 0$ with no zero divisors. Then we have the following.

- An element $a \in R$ is a **unit** in R is an element such that there exists $b \in R$ where $ab = ba = 1$.
- Suppose $r \in R$ is nonzero and is not a unit. Then r is called **irreducible** in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise, r is said to be **reducible.**
- The nonzero element $p \in R$ is called **prime** in R if the ideal (p) generated by p is a prime ideal. Alternatively, if R is a commutative ring, and $p \in R$. We say that p is **prime** if it is nonzero and not a unit, and the following condition holds: for all $a, b \in R$, if $p|ab$ then either $p|a$ or $p|b$.
- Two elements a and b differing by a unit are said to be **associate** in R (i.e., $a = ub$ for some unit u in R).

Proposition 3.4. *In an integral domain a prime element is always irreducible.*

Proof. Suppose (p) is a nonzero prime ideal and $p = ab$. Then $ab = p \in (p)$, so by the definition of prime ideal one of a or b, say a, is in (p). Thus $a = pr$ for some r. This implies $p = a = prb$, and so $rb = 1$. Thus b is a unit. This shows that p is irreducible. $\square$

Definition 3.5 (Principle Ideal Domains)**.** A **Principle Ideal Domains** (PID) is an integral domain in which every ideal is principal.

Definition 3.6 (Unique Factorisation Domains)**.** A **Unique Factorisation Domain** (UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

- r can be written as a finite product of irreducibles p_i of R (not necessarily distinct)
- The decomposition above is **unique up to associates**: if $r = q_1 q_2 \dots q_m$ is another factorisation of r into irreducibles, then $m = n$ and there is a renumbering of the factors so that p_i is associate to q_i.

Theorem 3.7. *Every principle ideal domain is a unique factorisation domain.*

3.1. Greatest Common Divisor, Euclidean Algorithm.

Definition 3.8 (Greatest common divisor)**.** Let R be a principal ideal domain and a, b nonzero elements of R. An element $d \in R$ is called a **greatest common divisor** of a and b if

(1) $d|a$ and $d|b$, and
(2) for all $e \in R$, if $e|a$ and $e|b$ then $e|d$.

Proposition 3.9 (Existence and properties of the GCD)**.** *Let R be a principal ideal domain, and $a, b \in R$ nonzero elements. Then*

- *There is an element $d \in R$ which is a greatest common divisor of a and b, and every associate of d is also a greatest common divisor of a and b.*
- *The greatest common divisor is unique up to associates.*
- *An element $d \in R$ is a greatest common divisor of a and b if and only if $d|a$, $d|b$ and there exist $r, s \in R$ such that $d = ar + bs$.*
- *An element $d \in R$ is a greatest common divisor of a and b if and only if $aR + bR = dR$.*

Definition 3.10 (Euclidean Algorithm)**.** This operation works in Euclidean Domains - domains where we can define a degree function measuring the size of each element. Given $a, b \in R$, calculates the GCD of a and b. Operates as follows:

While $b \neq 0$ - set $a, b = b, \mathrm{Rem}(a, b)$
where $\mathrm{Rem}(a, b)$ is the remainder of a upon division by b.

Theorem 3.11. *Every Principle Ideal Domain and Unique Factorisation Domain is a Euclidean Domain.*

Definition 3.12 (Gaussian Integers)**.** The Gaussian Integers $\mathbb{G}$ are defined as $\mathbb{Z}[i]$, the set $\{a + bi \,|\, a, b \in Z\}$.

Let $\alpha = a + bi \in \mathbb{G}$. Define the norm $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$.
We have the following theorem, due to Fermat.

Theorem 3.13. *The prime p is the sum of two integer squares, $p = a^2 + b^2, a, b \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \bmod 4$. This representation is essentially unique up to signs and interchanging elements.*

Secondly, the irreducible element in in the Gaussian integers $\mathbb{G}$ are as follows.

- *1 + i (with norm 2)*
- *The primes $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$ (with norm p^2)*
- *$a + bi, a - bi$, the distinct irreducible factors of $p = a^2 + b^2$ for primes p with $p \equiv 1 \bmod 4$.*

Proof. COMPLETE THIS! □

3.2. **Polynomial Rings.**

Definition 3.14 (Polynomial Ring)**.** Let x be indeterminate, and let R be a commutative ring with identity $1 \neq 0$. The set of all formal sums

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in R$ is the **polynomial ring** $R[x]$.

Proposition 3.15. *Let R be an integral domain. Then*

- $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ *if $p(x), q(x)$ are non-zero.*
- *The units of $R[x]$ are the units of R.*
- *$R[x]$ is an integral domain.*

Proposition 3.16. *Let I be an ideal of the ring R, and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of all polynomials with coefficients in I). Then we have*

$$R[x]/(I) \simeq (R/I)[x]$$

Theorem 3.17. *Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are unique $q(x)$ and $r(x)$ in $F[x]$ such that*

$$a(x) = q(x)b(x) + r(x)$$

with $r(x) = 0$ or $\deg r(x) < \deg b(x)$.

Theorem 3.18. *If F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorisation Domain.*

Theorem 3.19 (Gauss's Lemma)**.** *Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$.*

Corollary 3.20. R is a UFD if and only if $R[x]$ is a UFD.

Proposition 3.21. *Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, i.e., there exists $\alpha \in F$ with $p(\alpha) = 0$.*

Corollary 3.22. A quadratic or cubic in $F[x]$ is reducible if and only if it has a root in F.

Our next theorem gives us conditions on the roots of polynomials with integer coefficients.

Theorem 3.23 (Rational Roots Theorem). *Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If $\frac{r}{s} \in \mathbb{Q}$ is a root of $p(x)$ and r, s are relatively prime, then $r|a_0$ and $s|a_n$. In particular, if $p(x)$ is* ***monic*** *and $p(d) = 0$ for all integers d dividing the constant term a_0 of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.*

The following theorem gives conditions on the reducibility of a polynomial modulo some proper ideal.

Theorem 3.24. *Let I be a proper ideal in the integral domain R and let $p(x)$ be a non-constant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.*

Example 3.25. Consider the polynomial $p(x) = x^2 + x + 1 \in \mathbb{Z}[x]$. Then, reducing modulo 2, we see that $p(x)$ is irreducible in $\mathbb{Z}[x]$.

Our next theorem, Eisenstein's Irreducibility Criterion, applied to the ring $\mathbb{Z}[x]$ is stated below.

Theorem 3.26 (Eisenstein's Criterion for $\mathbb{Z}$). *Let p be a prime in $\mathbb{Z}$ and let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Suppose p divides a_i for all $a_i, i \in \{0, 1, \ldots, n-1\}$, p does not divide a_n, and p^2 does not divide a_0. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

4. Fields

Definition 4.1 (Field Extension). If K is a field containing the subfield F, then K is said to be an **extension field**, or simply and **extension**, of F, denoted K/F.

Definition 4.2 (Degree of an Extension). The degree of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F. The extension is said to be finite if $[K : F]$ is finite, and **infinite** otherwise

Theorem 4.3. *Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.*

Proof. Consider the quotient

$$K = F[x]/(p(x))$$

of the polynomial ring $F[x]$ by the ideal generated by $p(x)$. As $p(x)$ is irreducible in the PID $F[x]$, the ideal generated by $p(x)$ is a **maximal** ideal. Thus, the quotient $F[x]/(p(x))$ is a field. The projection π of $F[x]$ to the quotient $F[x]/(p(x))$ restricted to $F \subset F[x]$ gives a homomorphism $\varphi = \pi|_F : F \to K$ which is not identically zero, and hence $\varphi(F) \simeq F$.

If $\overline{x} = \pi(x)$ denotes the image of x in the quotient K, then we have

$$\begin{aligned} p(\overline{x}) &= \overline{p(x)} && \text{(since } \pi \text{ is a homomorphism)} \\ &= p(x) \bmod p(x) && \text{in } F[x]/(p(x)) \\ &= 0 \end{aligned}$$

Thus K contains a root of the polynomial $p(x)$. Hence, K is an extension of F in which the polynomial $p(x)$ has a root. □

Our next theorem allows us to understand the field $K = F[x]/(p(x))$ more fully, by having a simple representation for the elements of this field. Since F is a subfield of K, we might ask in particular for a basis for K as a vector space over F.

Theorem 4.4. *Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F, and let K be the field $F[x]/(p(x))$. Let $\theta = x \bmod (p(x)) \in K$. Then the elements*

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $[K : F] = n$. Hence,

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_i \in F\}$$

consists of all polynomials of degree less than or equal to n in θ.

Proof. Let $a(x) \in F[x]$ be any polynomial with coefficients in F. Since $F[x]$ is a Euclidean Domain, we may divide $a(x)$ by $p(x)$:

$$a(x) = q(x)p(x) + r(x)$$

It thus follows that $a(x) \equiv r(x) \bmod (p(x))$, which shows that every residue class in $F[x]/(p(x))$ is represented by a polynomial of degree less than n. Hence the images $1, \theta, \theta^2, \ldots, \theta^{n-1}$ of $1, x, x^2, \ldots$ in the quotient **span** the quotient as a vector space over F. We now show these elements are linearly independent, and so form a basis for the quotient over F. If the elements $1, \theta, \theta^2, \ldots, \theta^{n-1}$ were not linearly independent in K, then there would be a linear combination

$$b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1} = 0$$

in K, with $b_i \in F$ not all equal to zero. This is equivalent to

$$b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1} \equiv 0 \bmod (p(x))$$

i.e., $p(x)$ divides the above polynomial in x. But $\deg p(x) > \deg \sum^{n-1} b_i x^i$, and so by contradiction we have the above elements are a basis for K over F. Thus $\deg KF = n$. □

Proposition 4.5. *The above theorem gives us a formula for elements of the field K. Let K be an extension of F, and $a(\theta), b(\theta) \in K$. Then addition is defined as usual, and multiplication in K is* *defined as*

$$a(\theta)b(\theta) = r(\theta)$$

where $r(x)$ is the remainder obtained upon dividing the polynomial $a(x)b(x)$ by $p(x)$ in $F[x]$

Definition 4.6 (Simple Extension)**.** If the field K is generated by a single element α over F, then $K = F(\alpha)$, then K is said to be a **simple** extension of F and the element α is called a **primitive element** for the extension.

Theorem 4.7. *Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$, thus $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then*

$$F(\alpha) \simeq F[x]/(p(x))$$

Proof. Consider the natural homomorphism

$$\begin{aligned} \varphi : \quad & F[x] \to F(\alpha) \subseteq K \\ & a(x) \mapsto a(\alpha) \end{aligned}$$

Since $p(\alpha) = 0$ by assumption, we have that the element $p(x)$ is in the kernel of φ, and so we obtain an induced homomorphism

$$\varphi : F[x]/(p(x)) \to F(\alpha)$$

Since $p(x)$ is irreducible, we have that the quotient ring is a field, and as φ is not identically zero, we must have φ is an isomorphism. □

We now prove a theorem regarding the different roots of an irreducible polynomial. Consider the equation $p(x) = x^3 - 2$. Adjoining any of the three roots produces the same field extension (up to isomorphism). This is known as the **Isomorphism Extension Theorem**.

Theorem 4.8 (Isomorphism Extension Theorem)**.** *Let $\varphi : F \mapsto F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be irreducible and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F), and let β be a root of $p'(x)$ in some extension of F'. Then, there is an isomorphism*

$$\begin{aligned} \sigma : \quad & F(\alpha) \to F'(\beta) \\ & \alpha \mapsto \beta \end{aligned}$$

mapping α to β and extending φ, i.e., such that σ restricted to F is the isomorphism φ.

Proof. The isomorphism φ induces a natural isomorphism from $F[x]$ to $F'[x]$ which maps the maximal ideal $(p(x))$ to the maximal ideal $(p'(x))$. Taking quotients by these ideals, we have the following isomorphism of fields

$$F[x]/(p(x)) \to F'[x]/(p'(x))$$

and as the above fields are isomorphic to $F(\alpha)$ and $F'(\beta)$, respectively. $\square$

In the following, let K be an extension of F.

Definition 4.9 (Algebraic Elements and Algebraic Extensions)**.** An element α in K is said to be **algebraic** over K if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic then it is **transcendental** over F. The extension K/F is said to be **algebraic** if every element of K is algebraic over F.

Proposition 4.10 (Minimal polynomials)**.** *Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.*

Proof. Let $g(x) \in F[x]$ be a polynomial of minimal degree having α as a root. Multiplying $g(x)$ by a constant, we have $g(x)$ is monic. Supposing the $g(x)$ were reducible in $F[x]$, then

$$g(x) = a(x)b(x)$$

with $a(x), b(x)$ having degrees less than $\deg g(x)$. Yet as $g(\alpha) = 0$, then either $a(\alpha)$ or $b(\alpha)$ are zero, contradicting the minimal degree of $g(x)$.

Suppose now that $f(x) \in F[x]$ is a polynomial having α as a root. By the Euclidean Algorithm in $F[x]$, there are polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

with $\deg r(x) < \deg g(x)$. Then $f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = 0$, and thus $r(x) = 0$ by minimality of $g(x)$. Thus, any polynomial $f(x) \in F[x]$ with root α is divisible by $g(x)$. This proves that $m_{\alpha,F}(x) = g(x)$, completing the proof. $\square$

Corollary 4.11. If L/F is an extension of fields and α is algebraic over both F and L, then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

Proposition 4.12. *Let α be algebraic over F, and let $F(\alpha)$ be the field generated by α over F. Then*

$$F(\alpha) \simeq F[x]/(m_{\alpha,F}(x))$$

so that in particular,

$$[F(\alpha) : F] = \deg m_{\alpha,F}(x) = \deg \alpha$$

Theorem 4.13 (Tower Theorem)**.** *Let $F \subseteq K \subseteq L$ be fields. Then*

$$[L : F] = [L : K][K : F]$$

Proof. The proof proceeds as follows. Let (α_i) be a basis for L over K, and let (β_i) be a basis for K over F. The elements of L are of the form $\sum a_i \alpha_i$, with $a_i \in K$. Similarly, the elements a_i are of the form $\sum b_i\beta_i$ with $b_i \in F$. Thus, elements of L are of the form $\sum c_{ij}\alpha_i\beta_j$ - thus $\alpha_i\beta_j$ span L. Now, consider the linear relation $\sum c_{ij}\alpha_i\beta_j = 0$. As the elements β_j and α_i are both basis, it can be shown that $c_{ij} = 0$, thus elements $\alpha_i\beta_j$ are a basis for L over F, and the theorem follows. □

Definition 4.14 (Splitting Field)**.** Let F be a field. The extension field K of F is called splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (or **splits completely**) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Theorem 4.15. *For any field F, if $f(x) \in F[x]$, then there exists and extension K of F which is a splitting field for $f(x)$.*

Proposition 4.16. *The splitting field for a polynomial of degree n over F is of degree at most $n!$ over F.*

Proposition 4.17 (Uniqueness of splitting fields)**.** *Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.*

Proof. Take φ to be the identity mapping from F to itself and E, E' in the isomorphism extension theorem to be the two spitting fields for $f(x)$.

The proof proceeds by inducting on n, the degree of the extension of the splitting field. □

Definition 4.18 (Separable Polynomial)**.** A polynomial over F is called **separable** if it has no multiple roots. A polynomial which is not separable is inseparable.

Corollary 4.19. Every irreducible polynomial over a field of characteristic 0 (e.g. $\mathbb{Q}, \mathbb{Z}, \mathbb{Q}$) is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.

4.1. **Finite Fields.** A finite field $\mathbb{F}$ is a field with a finite number of elements. A finite field has characteristic p for some prime p, and so is a finite dimensional vector space over $\mathbb{F}_p$. If the dimension of the extension $[\mathbb{F}_p : \mathbb{F}] = n$, then the finite field has p^n elements.

Proposition 4.20. *Let F be a field of characteristic p. Then for any $a, b \in F$,*

$$(a+b)^p = a^p + b^p \quad \textit{and} \quad (ab)^p = a^p b^p$$

Alternatively, the map $\varphi(a) = a^p$ is an injective field homomorphism from F to F

Proof. Use the binomial theorem, and note that $\binom{p}{i}, i = 1, 2, \ldots, p-1$ is zero in characteristic p. □

Definition 4.21. The map $\varphi(a) = a^p$ is called the **Frobenius endomorphism** of F.

Corollary 4.22. If $\mathbb{F}$ is finite of characteristic p, then every element of $\mathbb{F}$ is a p^{th} power in $\mathbb{F}$ - notationally, $\mathbb{F} = \mathbb{F}^p$

Proof. This follows from the injectivity of the Frobenius endomorphism - as $\mathbb{F}$ is finite, an injective function is surjective. $\square$

The field K is said to be **separable** over F if eery element of K is the root of a separable polynomial over F. Equivalently, the minimal polynomial over F of every element of K is separable.

4.2. **Cyclotomic Extensions.**

Definition 4.23 (Cyclotomic Extensions)**.** The extension $\mathbb{Q}(\zeta_n)/Q$ generated by the n^{th} roots of unit over $\mathbb{Q}$ is called a cyclotomic extension.

Definition 4.24 (Cyclotomic Polynomial)**.** The n^{th} cyclotomic polynomial $\varphi_n(x)$ is defined as the polynomial whose roots are the primitive n^{th} roots of unity, which is of degree $\varphi(n)$.

Example 4.25. For p prime, the p^{th} cyclotomic polynomial $\Phi_p(x)$ is given by

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}$$

For example, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

Corollary 4.26. We have that

$$\Phi_n(x) = \frac{x^n - 1}{\Pi_{d|n}\Phi_d(x)}$$

Theorem 4.27. *The cyclotomic polynomial $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.*

Proof. If $\Phi_n(x)$ is reducible, there exist $f(x), g(x) \in \mathbb{Z}[x]$ such that

$$\Phi_n(x) = f(x)g(x)$$

where we take $f(x)$ to be an irreducible factor of $\Phi_n(x)$. Let ζ be a primitive n^{th} root of 1 which is a root of $f(x)$ (so that $f(x)$ is the minimal polynomial of ζ over $\mathbb{Q}$) and let p denote **any** prime not dividing n. Then ζ^p is also a primitive n^{th} root of 1, and hence is a root of either $f(x)$ or $g(x)$.

Suppose $g(\zeta^p) = 0$. Then ζ is a root of $g(x^p)$, and since $f(x)$ is the minimal polynomial for ζ, $f(x)$ must divide $g(x^p)$ in $\mathbb{Z}[x]$, say

$$g(x^p) = f(x)h(x)$$

Reducing modulo p gives

$$\overline{g}(x^p) = \overline{f}(x^p)\overline{h}(x^p)$$

in $\mathbb{F}_p[x]$.

By the remarks of polynomials over finite fields, we have

$$\overline{g}(x^p) = (\overline{g}(x))^p$$

so we have the equation

$$(\overline{g}(x))^p = \overline{f}(x)\overline{h}(x)$$

in the UFD $\mathbb{F}_p[x]$. it follows that $\overline{f}(x)$ and $\overline{g}(x)$ have a factor in common in $\mathbb{F}_p[x]$.

Now, from $\Phi_n(x) = f(x)g(x)$ we see by reducing modulo p that $\overline{\Phi_n}(x) = \overline{f}(x)\overline{g}(x)$, and so we have that $\overline{\Phi_n}(x)$ has a multiple root. But then also $x^n - 1$ would have a multiple root over $\mathbb{F}_p$ since it has $\overline{\Phi_n}(x)$ as a factor. This is a contradiction since we have that $x^n - 1$ has n distinct roots over any field of characteristic not dividing n.

Hence ζ^p must be a root of $f(x)$. Since this applies to every root ζ of $f(x)$, we must have that ζ^a is a root of $f(x)$ for every integer a relatively prime to n. This means that **every** primitive n^{th} root of unity is a root of $f(x)$, and thus $f(x) = \Phi_n(x)$, showing the $\Phi_n(x)$ is irreducible. □

4.3. **Constructible Numbers.** We now explore the set of numbers that can be constructed by a ruler and compass. Constructible numbers are completely classified by the following theorem.

Proposition 4.28. *If the element $\alpha \in \mathbb{Q}$ is obtained from a field $F \subset \mathbb{Q}$ by a series of compass and straightedge constructions then $[F(\alpha) : F] = 2^k$ for some integer $k \geq 0$.*

Proof. If a number is constructible, then there is a chain of subfields $\mathbb{Q} \subset F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$ such that each field F_i is constructed by adjoining the square root of an element $a_{i-1} \in F_{i-1}$, i.e. $F_i = F_{i-1}(\sqrt{a_{i-1}})$. This is an extension of degree one (if a_{i-1} is a square in F_{i-1}) or of degree two. Thus, by the Tower Theorem, we have that the overall extension degree is a power of two, and the proposition follows. □

5. Galois Theory

Definition 5.1 (Automorphism)**.** Let K be a field.

- An isomorphism σ of K with itself is called an **automorphism** of K. The collection of automorphisms of K is denoted $\mathrm{Aut}(K)$.
- An automorphism $\sigma \in \mathrm{Aut}(K)$ is said to **fix** an element $\alpha \in K$ if $\sigma(\alpha) = \alpha$. If F is a subset of K, then an automorphism σ is said to **fix** F if it fixes all the elements of F.

Definition 5.2. Let K/F be an extension of fields. Let $\mathrm{Aut}(K/F)$ be the collection of automorphisms of K which fix F.

Proposition 5.3. *Aut(K) is a group under composition and Aut(K/F) is a subgroup.*

Proposition 5.4. *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in$ Aut(K/F), $\sigma(\alpha)$ is a root of the minimal polynomial for α over F, i.e., Aut(K/F) permutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficients in F with α as a roots has $\sigma(\alpha)$ as a root.*

Proof. The proof is simple by noting that σ is a homomorphism fixing F. □

Proposition 5.5. *Let $H \leq Aut(K)$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.*

Proposition 5.6. *Let E be splitting field over F of the polynomial $f(x) \in F[x]$. Then*

$$|Aut(E/F)| \leq [E : F]$$

with equality if $f(x)$ is separable over F.

Definition 5.7 (Galois Extension)**.** Let K/F be a finite extension. Then K is said to be **Galois** over F and K/F is a **Galois** extension if $|\mathrm{Aut}(K/F)| = [K : F]$. If K/F is Galois, then the group of automorphism $\mathrm{Aut}(K/F)$ is called the **Galois group of** K/F, denoted $\mathrm{Gal}(K/F)$

Proposition 5.8. *If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.*

Corollary 5.9. The splitting field of any polynomial over $\mathbb{Q}$ is Galois, since the splitting field of $f(x)$ is clearly the same as the splitting field of the product of the irreducible factors of $f(x)$.

Definition 5.10 (Galois group of a polynomial)**.** If $f(x)$ is a separable polynomial over F, then the **Galois group of** $f(x)$ **over** F is the Galois group of the splitting field of $f(x)$ over F.

We now prove a fundamental relation between the orders of subgroups of the automorphism group of a field$K$ and the degrees of the extensions over their fixed fields.

Theorem 5.11. *Let G be a subgroup of the automorphisms of a field K and let F be the fixed field. Then*

$$[K : F] = |G|$$

Proposition 5.12. *Let K/F be any finite extension. Then*

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

with equality if and only if F is the fixed field of $Aut(K/F)$. Alternatively, K/F is Galois if and only if F is the fixed field of $Aut(K/F)$.

Theorem 5.13. *The extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. Furthermore, if this is the case then every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K.*

Theorem 5.14 (Fundamental Theorem of Galois Theory)**.** *Let K/F be a Galois extension and set $G = Gal(K/F)$. Then there is a bijection from (subfields E of K containing F) and (subgroups H of G), given by the correspondences (the field E mapping to the elements of G fixing E) and (H mapping to the fixed field of H) which are inverse to each other.*

Let $F \subseteq E \subseteq K$ and $1 \leq H \leq G = Gal(K/F)$, where E is the fixed field of H. Under this correspondence,

- *$[K:E] = |H|$ and $[E:F] = |G:H|$, the index of H in G.*
- *K/E is always Galois, with Galois group $Gal(K/E) = H$.*
- *E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group*

$$Gal(E/F) \simeq G/H$$

Definition 5.15 (Cyclic Extensions)**.** An extension K/F is said to be **cyclic** if it is Galois with a cyclic Galois group.

Proposition 5.16. *Let F be a field of characteristic not dividing n which contains the n^{th} roots of unity. Then the extension $F(\sqrt[n]{a})$ for $a \in F$ is cyclic over F of degree dividing n.*

Proof. The extension is Galois over F if F contains the n^{th} roots of unity since it is the splitting field for $x^n - a$. For any $\sigma \in \text{Gal}(K/F)$, $\sigma(\sqrt[n]{a})$ is another root of this polynomial, hence $\sigma(\sqrt[n]{(a)}) = \zeta_\sigma \sqrt[n]{a}$ for some root of unity ζ_σ. This gives a map

$$\begin{aligned} \varphi : \quad \text{Gal}(K/F) &\to \mu_n \\ \sigma &\mapsto \zeta_\sigma \end{aligned}$$

where μ_n denotes the group of n^{th} roots of unity. Since F contains μ_n, every n^{th} root of unity is fixed by every element of $\text{Gal}(K/F)$. Hence

$$\begin{aligned} \sigma\tau(\sqrt[n]{a}) &= \sigma(\zeta_\tau \sqrt[n]{a}) \\ &= \zeta_\tau \sigma(\sqrt[n]{a}) \\ &= \zeta_\tau \zeta_\sigma \sqrt[n]{a} \\ &= \zeta_\sigma \zeta_\tau \sqrt[n]{a} \end{aligned}$$

which shows that $\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau$, so the map above is a homomorphism. The kernel consists of precisely of the automorphism which fix $\sqrt[n]{a}$, namely the identity. This gives an injection of $\text{Gal}(K/F)$ into the cyclic group μ_n of order n, which proves the proposition. $\square$

Theorem 5.17. *Any cyclic extension of degree n over a field F of characteristic not dividing n which contains the n^{th} roots of unity is of the form $F(\sqrt[n]{a})$ for some $a \in F$.*

Definition 5.18 (Solvable by radicals)**.** An element α which is algebraic over F can be **expressed by radicals** or **solved for in terms of radicals** if α is an element of a field K which can be obtained by a succession of simple radical extensions

$$F = K_0 \subset K_1 \subset \cdots \subset K$$

where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, and $\sqrt[n_i]{a_i}$ is some root of the polynomial $x^{n_i} - a_i$. Such a field K is a **root extension** of F.

A polynomial $f(x) \in F[x]$ can be **solved by radicals** if all its roots can be solved for in terms of radicals.

Definition 5.19 (Solvable Groups)**.** A group G is **solvable** if there is a chain of subgroups

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_s = G$$

where each G_i is normal in G_{i+1} and the quotient groups G_{i+1}/G_i is abelian for all i.

Corollary 5.20. The finite group G is solvable if and only if for every divisor n of $|G|$ with $\gcd(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n.

Corollary 5.21. Let N be normal in G. If N and G/N are solvable, then G is solvable.

Theorem 5.22 (Solvability of a polynomial by radicals)**.** *A polynomial $f(x)$ is solvable by radicals if and only if its Galois group is a solvable group.*

Proof. IMPORTANT PROOF □

Corollary 5.23. The general equation of degree n cannot be solved by radicals for $n \geq 5$. For $n \geq 5$ the group S_n is not solvable.