MATH 457 Honours Algebra 4*

Notes by

Marcel K. Goh

23 April 2020

Note. These notes form a large subset of the content covered by the lectures/notes given over the semester. Some proofs are either skipped or distilled to their main ideas. Note that because of the coronavirus outbreak, some concepts that are normally covered in Algebra 4 were omitted this year, e.g. solvability by radicals. I take responsibility for any errors that may be present.

1. Rings

A *ring* R is a set with operations $+$ and $\cdot$ such that

i) $(R,+)$ is an abelian group;

ii) $(R,\cdot)$ is a semigroup;

iii) $\cdot$ distributes over $+$ on both sides:

$$a\cdot(b+c)=a\cdot b+a\cdot c \quad \text{and} \quad (a+b)\cdot c=a\cdot c+b\cdot c$$

A *semiring is the same as a ring* except that condition (i) above becomes

i') $(R,+)$ is a monoid with absorbing identity 0.

A ring is *unital* if $(R,\cdot)$ has a unit 1. We always assume that $1\neq 0$, since if $1=0$ then $R=\{0\}$. Observe that in a unital ring, $(R,+)$ is necessarily abelian. A ring is said to be *commutative* if $(R,\cdot)$ is.

Even for commutative rings, there are many possible ring structures for $(R,+)=\mathbf{Z}^2$. For example we can take the *Gaussian integers* $\mathbf{Z}[i]=\{a+bi : a,b\in\mathbf{Z}\}$ or the *Eisenstein integers* $\mathbf{Z}[\omega]=\{a+b\omega : a,b\in\mathbf{Z}\}$ where

$$\omega=-\frac{1+i\sqrt{3}}{2}.$$

In both cases the second binary operation is complex multiplication. Since i and ω are both solutions to equations of the form $x^2+Bx+C=0$, they are called *quadratic integers* and $\mathbf{Z}[i]$ and $\mathbf{Z}[\omega]$ are called *quadratic rings*.

The definition of a ring is meant to describe a class of $\mathbf{Z}$-like objects, but many rings have properties different from the integers. For example, the ring $\mathbf{Z}[\sqrt{-5}]$ does not have Euclidean division. There are also many non-commutative rings such as the *Lipschitz quaternions*

$$\{a+bi+cj+dk : a,b,c,d\in\mathbf{Z}\}$$

or the *Hurwitz quaternions*

$$\left\{a+bi+cj+dk : a,b,c,d\in\mathbf{Z} \text{ or } a,b,c,d\in\mathbf{Z}+\frac{1}{2}\right\}.$$

If R is a ring, then a subgroup of $(R,+)$ that is closed under multiplication is called a *subring*. If a ring is unital, then any unital subring will have the same unit. A *homomorphism* between two rings R and S is a map $f:R\to S$ that preserves both operations:

$$f(a+b)=f(a)+f(b) \qquad \text{and} \qquad f(a\cdot b)=f(a)\cdot f(b)$$

* Course given by Prof. Mikaël Pichot at McGill University

A homomorphism that preserves the units is called *unital.*

An *ideal* in a ring R is a subgroup $(I,+)$ such that

i) $ab \in I$ for all $a \in R$, $b \in I$;

ii) $ab \in I$ for all $b \in I$, $a \in R$.

If (i) holds, I is called a *left ideal* and if (ii) holds, I is called a right ideal. Let $I \subseteq R$ be an ideal. One defines the *quotient ring* R/I as follows. Since $(I,+)$ is a normal subgroup of $(R,+)$, R/I is an abelian group. We associate $r \sim r'$ if $r - r' \in I$. Then we can define multiplication in R/I as $(a+I)(b+I) = ab+I$. This is well-defined because I is an ideal and distributivity holds.

The isomorphism theorems for groups extend to rings as well. Their proofs are analogous to the ones in group theory.

Theorem A (*First isomorphism theorem*). *Let $f : R \twoheadrightarrow S$ be a surjective ring homomorphism. Then f descends to a a ring homomorphism $f' : R/I \to S$ that takes $a+I$ to $f(a)$, where I is the kernel of f.* ▮

Theorem B (*Second isomorphism theorem*). *Let S be a subring and I and ideal in a ring R. Then $S+I$ is a subring of R, I is an ideal in $S+I$, and the map $S \twoheadrightarrow (S+I)/I$ is a surjective ring homomorphism with kernel $S \cap I$.* ▮

Theorem C (*Third isomorphism theorem*). *Let R be a ring and $I \subseteq J \subseteq R$ be ideals. Then $R/I \twoheadrightarrow R/J$ is a surjective ring homomorphism with kernel J/I.* ▮

Theorem D (*Fourth isomorphism theorem*). *Let $f : R \twoheadrightarrow S$ be a surjective ring homomorphism. There is a bijection between the ideals in R containing* $\ker f$ *and the set of all ideals in S.* ▮

Note that the correspondence in Theorem D works with subrings as well, not just ideals.

An element r in a unital ring R is said to be *invertible* if there exists $s \in R$ such that $rs = sr = 1$. The set of invertible elements is denoted $R^\times$ and this is a group under $\times$, called the *group of units.* A *field* is a ring in which every nonzero element is a unit. Non-commutative fields are called *division rings* or *skew fields* (the quaternions are an example of a skew field).

Let K be a field. The set $K[x]$ of polynomials with coefficients in K is a ring. Then the set

$$K(x) = \{f/g : f, g \in K[x], g \neq 0\}$$

is a field, called the *field of rational functions.* The set $K[[x]]$ is called the *ring of formal series*: possibly infinite sums $\sum_{n\geq 0} a_n x^n$. Addition is done pointwise and multiplication is convolution of power series. The map $K[x] \to K[[x]]$ is a homomorphism and some elements become invertible. For example, $1-x$ becomes invertible, since $1/(1-x) = \sum_{n\geq 0} x^n$. Not every element in $K[[x]]$ is invertible, but one can invert the elements to get a new field $K((x))$: the set of sequences $K^{\mathbf{Z}}$ that are eventually zero when going to the left.

A *zero-divisor* is an element $r \in R$, $r \neq 0$ for which there exists $s \in R$ such that $rs = 0$. A ring is *cancellative* if $rs = rs'$ implies that $s = s'$. Then we define an *integral domain* to be a unital, commutative, cancellative ring. Every integral domain embeds into a field, called the *field of fractions.* The construction is analogous to building the rational numbers from the integers.

Proposition Z. *If R is a ring with unity, there exists a unique unital homomorphism $f : \mathbf{Z} \to R$.* ▮

Proof. Since $f(1) = 1$, we have $f(n) = 1 + 1 + \cdots + 1 \in R$. ▮

The nonnegative integer n which generates $\ker f$ is called the *characteristic* of R. The image of f is called the *characteristic subring.* For example $\mathbf{Z}/n\mathbf{Z}$ has characteristic n.

Proposition P. *The characteristic of an integral domain R is either* 0 *or a prime number.* ▮

An *algebra* over a commutative ring R is a ring A with a homomorphism $\eta : \mathbf{R} \to A$ whose image lies in the *centre* of A. Examples of algebras include rings of functions and matrices $M_n(R)$.

For a group G and a ring R, we can define the *group ring* $G[R]$ as the set of all finitely supported functions from G to R. This forms a ring with addition $(f+g)(s) = f(s) = g(s)$ and multiplication $(fg)(s) = \sum_{uv=s} f(u)g(u)$.

2. Ideals

Every element r in a unital ring R generates a *principal* ideal (r). More generally any subset $S \subseteq R$ does. The ideal (S) is the intersection of all ideals that contain S. If R is commutative, then $(r) = rR = Rr$. In $\mathbf{Z}$, the ideals are the of the form $(n) = n\mathbf{Z}$. Then $(n) \subseteq (m)$ if and only if $m \setminus n$ (this is true in any commutative ring). A ring R in which every ideal is principal is called a *principal ring* and if R is also an integral domain, we call it a *principal ideal domain* or PID.

Principal ideals determine their generators up to unit. If $(r) = (s)$, then $s = ar$ and $r = bs$ together imply that both a and b are units. Elements r and s of a ring R are called *associate* if there exists a unit a such that $r = as$.

We can define three operations on ideals. Let $I, J \subseteq R$ be ideals.

i) $I \cap J$ is an ideal.
ii) $I + J = \{a + b : a \in I, b \in J\} = (I \cup J)$ is an ideal.
iii) $IJ = \{ab : a \in I, b \in J\}$ is an ideal.

Lemma P. *Let R be a commutative ring. Let $I = (S)$ and $J = (T)$ be two ideals. Then $IJ = (ST)$.* ▮

In the ring of integers $\mathbf{Z}$, we have $(m)(n) = (mn)$, $(m)\cap(n) = \big(\operatorname{lcm}(m, n)\big)$, and $(m)+(n) = \big(\gcd(m, n)\big)$. When $I \subseteq J$ is an inclusion of ideals, one may think of it as a kind of divisibility $J \setminus I$. For example, $\gcd(m, n) \setminus \operatorname{lcm}(m, n) \setminus mn$.

Lemma D. *If $I, J \subseteq R$ are ideals, then*

$$IJ \subseteq I \cap J \subseteq I + J. \quad ▮$$

The set of ideals forms a semiring where the two operations are $I + J$ and IJ. The semiring in $\mathbf{Z}$ is $\mathbf{N}$ with the addition $m + n = \gcd(m, n)$ and ordinary multiplication.

For an ideal $I \subseteq R$, we define the *radical* of I to be the set

$$\sqrt{I} = \{a \in R : a^n \in I \text{ for some } n \in \mathbf{N}\}.$$

This is an ideal and it has the property that $\sqrt{\sqrt{I}} = \sqrt{I}$. Furthermore, if $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.

An ideal $I \subseteq R$ is called *maximal* if it is proper and whenever $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

Lemma M. *Let R be a unital ring. Then every proper ideal is included in a maximal ideal.*

Proof. This is an application of Zorn's Lemma. Let I be a proper ideal and let X be the set of all proper ideals containing I, ordered by inclusion. Then this set is inductive (increasing union of ideals is an ideal) so there is a maximal element M. ▮

Lemma F. *Let R be unital and commutative. Then an ideal $I \subseteq R$ is maximal if and only if R/I is a field.*

Proof. This follows from the fourth isomorphism theorem. ▮

Let R be a unital ring. An ideal I of R is *prime* if it is proper and for any ideals A, B of R, $AB \subseteq I$ implies that $A \subseteq I$ or $B \subseteq I$. The *spectrum* of R is the set of all prime ideals and it is denoted $\operatorname{Spec}(R)$. The *maximal spectrum* of R, denoted $\operatorname{Spec}_{\max}(R)$, is the set of all maximal ideals of R.

Maximal ideals are always prime (so $\operatorname{Spec}_{\max}(R) \subseteq \operatorname{Spec}(R)$), but not all prime ideals are maximal. For example, (0) is prime in $\mathbf{Z}$ but certainly not maximal. A ring is called *local* if it has a unique maximal ideal. A ring R is local if and only if $R \setminus R^\times$ is an ideal.

Lemma C. *Let R be a unital commutative ring. Let $I \subseteq R$ be a proper ideal. Then I is prime if and only if $ab \in I$ implies that $a \in I$ or $b \in I$.* ▮

Lemma I. *Let R be a unital commutative ring. Then $I \subseteq R$ is a prime ideal if and only if R/I is an integral domain.* ▮

Since all fields are integral domains, this proves that all maximal ideals are prime. We also have that a commutative ring R is an integral domain if and only if (0) is a prime ideal in R (if R is not commutative, then we say it is a *prime ring*). If R is a PID, then every nonzero prime ideal is maximal.

We can view elements in a commutative unital ring R as "functions" on the set $\operatorname{Spec}(R)$ of prime ideals. To $r \in R$ we identify a function f_r such that $f_r(P) = r \bmod P \in R/P$. We have a bundle at every $P \in \operatorname{Spec}(R)$ and a fibre R/P which is an integral domain. The *total space* $B(R)$ is the union of R/P over all prime ideals P. A *section* is a map $s : \operatorname{Spec}(R) \to B(R)$ such that $s(P) \in R/P$. $\Gamma(R)$ is the set of all sections and $\Gamma_{\max}(R)$ is its restriction to $\operatorname{Spec}_{\max}(R)$. Let $\pi : R \to \Gamma(R)$ map $r \mapsto f_r$ and $\pi_{\max} : R \to \Gamma_{\max}(R)$ take r to f_r, restricted to $\operatorname{Spec}_{\max}(R)$. We want to know when π and $\pi_{\max}$ are faithful.

Proposition K. *The kernel of π is the intersection of all prime ideals and the kernel of $\pi_{\max}$ is the intersection of all maximal ideals.* ∎

For a unital commutative ring R, we define the *nilradical* of R to be the intersection $\operatorname{Nil}(R) = \bigcap P$ of all prime ideals P. The *Jacobean radical* is the intersection $\operatorname{Jac}(R) = \bigcap M$ of all maximal ideals M. Since $\operatorname{Spec}_{\max}(R) \subseteq \operatorname{Spec}(R)$, $\operatorname{Jac}(R) \supseteq \operatorname{Nil}(R)$. An element $r \neq 0$ in a ring R is called *nilpotent* if $r^n = 0$ for some n. It turns out that there is a connection between nilpotency and prime ideals.

Proposition N. *Let R be unital and commutative. Then $\operatorname{Nil}(R)$ is the set of all nilpotent elements, i.e.*

$$\sqrt{(0)} = \{r \in R : r^n = 0 \text{ for some } n \in \mathbf{N}\} = \bigcap_{P \in \operatorname{Spec}(R)} P.$$

Proof. To show that a nilpotent element r belongs to every prime ideal P, note that $r^n \in P$, so $r \cdot r^{n-1} \in P$ and we can iterate this until we get that $r \in P$. Conversely, if r is not nilpotent, we can let X be the set of ideals I such that r^n is not in I for any n. X is nonempty and inductive, so by Zorn's Lemma there is a maximal element and it can be shown that this ideal is prime. ∎

Let R be a commutative ring and let $p \in R$ be a nonzero non-unit. Then p is said to be

i) *prime* if $p \setminus ab$ implies that $p \setminus a$ or $p \setminus b$;

ii) *irreducible* if $p = ab$ implies a is a unit or b is a unit.

To find irreducible elements in a ring, may attempt the "bisection process". Let $r \in R$. If r is irreducible, we stop. If r is not irreducible, then $r = r_1 r_2$. If neither is irreducible, we continue by splitting r_1 and r_2 in the same way. This process may not terminate.

Proposition I. *Let R be an integral domain. If an element $p \in R$ is prime, then it is irreducible.*

Proof. . Let $p \in R$ be a prime element. Assume that $p = ab$. This implies that $p \setminus a$ or $p \setminus b$. Say $a = pc$ for some $c \in R$. Then $p = ab = pcb$ and $cb = 1$. So b is a unit. ∎

Note that the converse does not hold. For example, in the ring $\mathbf{Z}[\sqrt{-3}]$, we have $4 = (1+\sqrt{-3})(1-\sqrt{-3})$. The element 2 is irreducible, but it is not prime because 2 divides 4 but does not divide either of $(1+\sqrt{-3})$ and $(1-\sqrt{-3})$.

Proposition A. *Let R be an integral domain. Let p be a nonzero element in R. Then p is prime if and only if (p) is prime and p is irreducible if and only if (p) is maximal among principal ideals.* ∎

This proposition implies that in a PID, irreducible elements are prime.

A ring R is a *unique factorisation domain* if every $r \in R$ can be expressed as a product $r = p_1 \cdots p_n$ of irreducible elements, which is unique up to the order of the p_i. The rings $\mathbf{Z}$, $K[x]$, and $K[x, y]$ are all examples of UFDs. Every PID is a UFD and in a UFD, all irreducible elements are prime.

Lemma S. *In a PID, every chain of ideals stabilises.*

Proof. $I = \bigcup_{n \geq 1} I_n$ is an ideal. Since R is a PID, $I = (x)$ for some x and $x \in I_n$ for some n. This implies that $I = I_n$. ∎

Lemma N. *Let R be a unital ring. Then every increasing chain of ideals stabilises if and only if every ideal is finitely generated.*

Proof. If $I = (x_1, x_2, \ldots)$ is not finitely generated, then $I_n = (x_1, \ldots, x_n)$ is an increasing chain of ideals that does not stabilise. Conversely, if every ideal is finitely generated, then let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals and let $I = \bigcup_{n \geq 1} I_n$. There exist $(x_1, \ldots, x_n)$ that generate I, so there exists a k such $x_i \in I_k$ for all i and we find that $I = I_k$. ▮

A ring is called *Noetherian* if it the equivalent conditions from Lemma N hold.

For elements r and s of a ring, a *greatest common divisor* or gcd is an element d dividing both r and s such that if any d' divides both r and s, then d' divides d. An integral domain R is called a *Bézout domain* if $(r) + (s)$ is principal for every $r, s \in R$ (of course, every PID is a Bézout domain) and it is called a *GCD domain* if any two $r, s \in R$ have a gcd. Every UFD is a GCD domain.

Lemma B. *The following statements regarding Bézout domains are true.*

i) A ring R is Bézout if and only if every finitely generated ideal is principal.

ii) A Bézout domain is a GCD.

iii) If a ring is both Noetherian and a Bézout domain, then it is a PID. ▮

3. Gaussian Integers

Recall from Section 1 that the Gaussian integers are the ring

$$\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}.$$

We write N for the complex modulus, squared. So $N(z) = z\overline{z} = a^2 + b^2$. This is called the *norm* and it is a group homomorphism $\mathbf{C}^\times \to \mathbf{R}^\times$, since $N(zz') = N(z)N(z')$. $N(z) = 0$ implies that $z = 0$. The norm n takes $\mathbf{Z}[i]$ to $\mathbf{N}$. The kernel of N on $\mathbf{C}^\times$ is the unit circle $\{z \in \mathbf{C} : |z| = 1\}$. Let $\ker N$ denote the kernel of N restricted to $\mathbf{Z}[i]$, i.e. $\{\pm 1, \pm i\}$. These are the units of $\mathbf{Z}[i]$.

The image of N is

$$\mathrm{Im}(N) = \{n \in \mathbf{N} : n = a^2 + b^2 \text{ for some } a, b \in \mathbf{Z}\}.$$

This set is stable under product, since if $n = N(z)$ and $n' = N(z')$, then $nn' = N(zz')$. Gauss was interested in studying the number of integer numbers less than a given n that can be expressed as a sum of two squares. We will return to this point later.

We say that a prime number *splits* if it is no longer prime in $\mathbf{Z}[i]$ and we say that it is *inert* otherwise.

Lemma S. *Let p be a prime. Then p is a sum of two squares if and only if it splits in $\mathbf{Z}[i]$.*

Proof. If $p = a^2 + b^2$ then $p = (a + ib)(a - ib)$ and $N(a + ib)N(a - ib) = p^2$ implies that neither of these factors are units. So p is not prime in $\mathbf{Z}[i]$. Conversely, if $p = \alpha\beta$ in $\mathbf{Z}[i]$, then $N(\alpha) = N(\beta) = p$ means that p is the sum of two squares. ▮

Lemma I. *A prime p splits if and only if $p \equiv 1 \pmod 4$.*

Proof. If p splits, then by the previous lemma, $p = a^2 + b^2$ and the sum of two squares is never 3 modulo 4. So if p is an odd prime it is congruent to 1 modulo 4. Conversely, assume that $p \equiv 1 \pmod 4$. Then $p = 1 + 4n$ for some n and there exists $x \in \mathbf{Z}$ such that $x^2 \equiv 1 \pmod p$. (In fact, $x = (2n)!$ works.) Then p divides $x^2 + 1 = (x + i)(x - i)$. So p divides $(x + 1)$ or $(x - i)$, so p divides i and is not inert. ▮

All this talk of divisibility leads nicely into a discussion of Euclidean division. In $\mathbf{Z}$, the goal of Euclidean division for integers a and b is to find a $q \in \mathbf{Z}$ such that $a - bq$ is small, in some sense. The following proves a similar result in $\mathbf{Z}[i]$.

Proposition E. *There is a Euclidean division in $\mathbf{Z}[i]$.*

Proof. . Let $a, b \in \mathbf{Z}[i]$, $b \neq 0$. We can divide them in $\mathbf{C}$ to get $z = a/b$. Then there is a (not necessarily unique) $q \in \mathbf{Z}[i]$ that is of minimal distance to z. We have $|z - q| < 1$; in fact $|z - q| \leq \sqrt{2}/2 < 1$. So $|a - bq| < |b|$. ▮

Let us now define this generally. An integral domain R is a *Euclidean domain* if there exists a function $N : R \to \mathbf{N}$ called the *norm* such that $N(0) = 0$ and for all $a, b \in R$, $b \neq 0$, either b divides a or there exists $q \in R$ such that $N(a - bq) < N(b)$. Proposition E showed that $Z[i]$ is a Euclidean domain with the complex norm, and other familiar examples include $\mathbf{Z}$ with the absolute value function and $K[x]$ with the degree of a polynomial as its norm. In general, the Euclidean division algorithm does not give a unique answer. Even in $\mathbf{Z}$, we can end up with q or $-q$ as a quotient.

Proposition T. $\mathbf{Z}[\sqrt{-2}]$ *is a Euclidean domain.*

Proof. We repeat the same proof as for $\mathbf{Z}[i]$ except for the computation of $|z-q|$, which is now $\leq \sqrt{3}/2$. ∎

Recall that $\mathbf{Z}[\sqrt{-3}]$ is not a Euclidean domain. It is not even a UFD, since $4 = 2{\cdot}2 = (1+\sqrt{-3})(1-\sqrt{-3})$. But $\mathbf{Z}[\sqrt{-3}] \subseteq \mathbf{Z}[\omega]$ and this is a Euclidean domain, with norm $N(a+b\omega) = a^2 - ab + b^2$. The units in $\mathbf{Z}[\omega]$ are the elements of norm 1: $\{\pm 1, \pm\omega, \pm\omega^2\}$ and we have unique factorisation up to units.

Proposition P. *Every Euclidean domain is a PID (and consequently a UFD).*

Proof. Let R be a Euclidean domain and $I \subseteq R$ an ideal. Let $b \neq 0$ be an element of I of minimal norm. If $a \in I$ then b divides a. Otherwise, there exists $q \in R$ such that $N(a-bq) < N(b)$, contradicting the minimality of b's norm. So I is principal. ∎

A corollary of this fact is that every ideal in $\mathbf{Z}[i]$ is principal.

4. Modules

For any set X, the set of symmetries $\mathrm{Sym}(X)$ is a group and an action of a group G on X is a group homomorphism $G \to \mathrm{Sym}(X)$. If X is a group, we can define the *ring of endomorphisms* $\mathrm{End}(X)$ as the set of group homomorphisms from X to X.

Lemma M. *Let M be an abelian group. Then* $\mathrm{End}(M)$ *is a ring.*

Proof. Addition is pointwise addition from M and multiplication is composition of maps. ∎

Let R be a a unital commutative ring. A *module* M over R is a ring homomorphism $R \to \mathrm{End}(M)$. Explicitly, the list of axioms of a module are very similar to those of a vector space (in fact, if R is a field, then a module is a vector space). For $r, s \in R$ and $m, n \in M$, we have

i) $r(m+n) = rm + rn$;
ii) $(r+s)m) = rm + sm$;
iii) $(rs)m = r(sm)$;
iv) $1m = m$.

These axioms also work if R is not commutative; in this case, we call M a *left R-module.* The kernel of $R \to \mathrm{End}(M)$ is called the *annihilator* of M:

$$\mathrm{Ann}(M) = \{r \in R : rm = 0 \text{ for all } m \in M\}$$

A module is said to be *faithful* if $\mathrm{Ann}(M)$ is trivial. If M is an R-module, then M is a faithful S-module where $S = R/\mathrm{Ann}(M)$.

Proposition I. *Any ideal I in a ring R is a module over R.*

Proof. For $a \in I$ and $r \in R$, we have $ra \in I$. The rest of the axioms follow. ∎

Quotients R/I are also modules. When $R = \mathbf{Z}$, the action is determined by the group structure in M. For example,

$$2m = (1+1)m = 1m + 1m = m + m.$$

When $R = K[x]$ for some field K, we have the following interesting lemma.

Lemma V. *$K[x]$-modules are operators on vector spaces and vice versa.*

Proof. Let M be a $K[x]$-module. The restriction of the $K[x]$ action to K gives a K-module structure on M. This is a vector space. Furthermore, the indeterminate x also acts on M by taking $m \mapsto xm$. This gives a map $x : M \to M$ such that $x(m+n) = x(m)$ and $x(rm) = (xr)m = (rx)m = r \cdot x(m)$. So x is a linear map.

Conversely, if V is a K-vector space, and $T : V \to V$ is a linear map, then V is a $K[x]$-module, because for any $p \in K[x]$, $p(T)$ is a linear map on V. ∎

Note that the module is not faithful, because $K[x]$ has infinite dimension but $\mathrm{End}(V)$ has finite dimension when V has finite dimension. If G is a group, $K[G]$ is the group ring and a $K[G]$-module is a linear representation of G.

A *submodule* M' of M is a subgroup that is stable under the action of the ring, i.e. for all $m, n \in M'$ and $r \in R$, $m + rn \in M'$. For example, ideals are submodules of R and if M' is a submodule, we can define the *quotient module* M/M' with the action of R:

$$r(m + M') = rm + M'$$

If M and M' are modules, then $M \times M'$ is a module. If a module has no proper nontrivial submodules, then it is called *simple*.

An R-module map is a group homomorphism $f : M \to M'$ such that $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$. The kernel $\ker f$ is a submodule of M and the image of f is a submodule of M'. The isomorphism theorems for modules are exactly analogous to the ones given for rings in Section 1.

Lemma S (*Schur's lemma*). *Let M be a simple module. Then $\mathrm{End}_R(M)$ is a skew field.*

Proof. Let $f : M \to M'$ be a module map that is not identically zero. The kernel of f is a submodule of M, so since $f \neq 0$, $\ker f = \{0\}$. Then the image of f is a submodule of M' since $f \neq 0$, $\mathrm{Im}\, f = M'$. Hence f is an isomorphism. ▮

If M is an R-module and $I \subseteq R$ is an ideal, then

$$IM = \left\{ \sum r_i m_i : r_i \in I, m_i \in M \right\} \subseteq M$$

is a submodule.

Theorem C (*Chinese remainder theorem*). *Let I, J be ideals in a ring R. Let M be an R-module. Then the map*

$$M \to M/IM \times M/JM$$

has kernel $IM \cap JM$. ▮

If $I + J = R$ then the map is surjective and $(I \cap J)M = IJM$. With n ideals such that $I_k + I_l = R$ for $k \neq l$, we have

$$M/(I_1 \cdots I_n)M \cong M/I_1M \times \cdots \times M/I_nM.$$

Let M be an R-module. If $A \subseteq M$, then

$$(A) = \left\{ \sum r_i a_i : r_i \in R, a_i \in A \right\}$$

is the submodule of M *generated* by A. A module is *finitely generated* if it admits a finite generating set and *cyclic* (or *singly generated*) if it is generated by one element. If $M = (a)$ is cyclic, then the map $R \to M$ that sends $r \mapsto ra$ is surjective with kernel $\mathrm{Ann}(M)$.

Lemma P. *Let R be an integral domain. Then the nonzero principal ideals are isomorphic to R.*

Proof. Let $I = (a)$ be an ideal (so it is an R-module). If $r \in \mathrm{Ann}(I)$ then r is a zero divisor. So $R \to I$ is an isomorphism. ▮

A finitely generated R-module M is called *free* if it is isomorphic to R^n for some n. For example, if R is a field, every module (finite-dimensional vector space) is free. Equivalently, an R-module is free if there exists a basis, that is, a generating set A such that any $m \in M$ can be written in a unique way as a finite sum

$$m = \sum_{a \in A} r_a a.$$

The set A is called a *free generating set* and the cardinality of A is called the *rank* of M.

In a PID, every ideal is a free module (isomorphic to the ring itself). For any set A and ring R, we can let F_A be the set of all functions from A to R with finite support. This is a group under pointwise addition and r acts on F_A: $(rf)(a) = r \cdot f(a)$. A basis for F_A is the set $(\delta_a)_{a \in A}$ of delta functions, where $\delta_a(b) = 1$ if $b = a$ and 0 otherwise.

Proposition U (*Universal property of free modules*). *Let ϕ be a map from a set A to an R-module M. Then there is a unique extension of ϕ to a module map $\overline{\phi} : F_A \to M$.*

Proof. Take any element $f \in F_A$ and express it as

$$f = \sum_{a \in A} r_a \delta_a$$

for some $r_a \in R$. Then let $\overline{\phi}$ be given by

$$\overline{\phi}(f) = \sum_{a \in A} r_a \phi(a). \quad \blacksquare$$

Proposition S. *Let $N \hookrightarrow M \twoheadrightarrow F$ be a short exact sequence of modules (so $F \cong N/M$), where F is a free module. Then the sequence splits, i.e. $M \cong N \oplus F$.*

Proof. We need to construct the section s of $\pi : M \twoheadrightarrow F$. Let A be a basis of F. Since π is surjective, for any $a \in A$ we can find $m_a \in M$ such that $\pi(m_a) = m$. This gives a map $s_* : A \to M$ and by the universal property there is a unique extension $s : F_A \to M$. We have $\pi \circ s = \mathrm{Id}$ on the basis and therefore everywhere on F. So s is a section of π. Let $F' = \mathrm{Im}(s) \subseteq M$. So $F' \cong F$ as R-modules. We claim that $M = N \oplus F'$ (viewing N as a submodule of M).

Firstly, $N \cap F' = \{0\}$, since if $m \in N \cap F'$, then $\pi(m) = 0$ and there exists $f \in F$ such that $s(f) = m$. But this implies that $f = \pi\big(s(f)\big) = \pi(m) = 0$, so $m = 0$. And $M = N + F'$ because any $m \in M$ can be expressed as the sum of $\big(m - s \circ \pi(m)\big) + s \circ \pi(m)$. $\blacksquare$

The following theorem shows that the rank of a free module is well-defined.

Theorem R. *If $R^n \cong R^m$ as R-modules, then $n = m$.*

Proof. Since R is unital and commutative, it contains a maximal ideal M. Let $K = R/M$ and consider the submodule $MR^n = \big\{s(x_1, \cdots, x_n) \in R^n : s \in M, x_i \in R\big\}$. The quotient module is $K^n = (R/M)^n$ and a module isomorphism $R^n \cong R^m$ descends to a R-module isomorphism $K^n \cong K^m$. This map has kernel M and is a K-vector space isomorphism. So the dimension of the two vector spaces are the same and thus $n = m$. $\blacksquare$

Let M be a module over an integral domain R. The set of *torsion elements*

$$\mathrm{Tor}(M) = \{m \in M : rm = 0 \text{ for some } r \neq 0\}$$

is a submodule of M. A module is called *torsion* if $\mathrm{Tor}(M) = M$ and *torsion-free* if $\mathrm{Tor}(M) = \{0\}$. Note that R^n is torsion-free, since it has a basis $\{e_n\}$ and if $am = ra_1e_1 + \cdots + ra_ne_n = 0$, then $ra_i = 0$ for all i and $m = 0$.

Proposition T. *For any module M over an integral domain R, $M/Tor(M)$ is torsion-free.*

Proof. Let $N = M/\mathrm{Tor}(M)$ and let $\overline{m} \in N$. Suppose there exists $r \neq 0$ such that $r\overline{m} = 0$. So $\overline{rm} = 0$ and $rm \in \mathrm{Tor}(M)$. Thus there exists $s \neq 0$ such that $(rs)\overline{m} = 0$. But $\overline{rs} \neq 0$ so m must be 0. Hence $\mathrm{Tor}(N) = \{0\}$. $\blacksquare$

Lemma G. *A module M over an integral domain R is torsion if and only if it is generated by torsion elements.*

Proof. The forward direction is clear. Conversely, suppose $M = (A)$ and every element in A is torsion. Let $m = s_1a_1 + \cdots + s_na_n \in M$ for some $s_i \in R$ and $a_i \in A$. Each a_i is a torsion element so there is r_i such that $r_ia_i = 0$. Let $r = r_1 \cdots r_n$. Then $rm = 0$. $\blacksquare$

Proposition F. *Let M be a finitely generated module over an integral domain R. There exists a free module $F \subseteq M$ such that M/F is torsion.*

Proof. Let $M = (A)$ where A is finite. Let $B \subseteq A$ be a maximal basis which generates a free module F of rank $n = |B|$. Let N be the quotient M/F. For every $a \in A \setminus B$, the module $(B \cup \{a\})$ is not free. So there exists $r \in R, r_b \in R$, not all zero, such that

$$ra + \sum_{b \in B} r_b b = 0.$$

Note that $r \neq 0$, otherwise B would not be a basis. But $ra = 0 \bmod F$, so N is generated by torsion elements and by the previous lemma, N is torsion. ∎

5. Modules Over PIDs

An R-module has properties very much like a vector space when R is a PID.

Proposition F. *Let R be a PID. Then every submodule of a free module R^n is free of rank $k \leq n$.*

Proof. We proceed by induction. When $n = 1$, every ideal $I \subseteq R$ is free, isomorphic to R. Now assume the proposition is true for R^n. Let M be a submodule of R^{n+1}. Let $\pi : R^{n+1} \twoheadrightarrow R^n$ be the projection map on to the first n coordinates. So we have a short exact sequence

$$\ker(\pi_{|M}) \hookrightarrow M \twoheadrightarrow \pi(M).$$

But $\pi(M)$ is a submodule of R^n so, by the induction hypothesis, it is free and the sequence splits. Thus $M \cong \ker(\pi_{|M}) \oplus \pi(M)$ is free. ∎

A module M over a unital ring R is called a *Noetherian module* if every submodule is finitely generated.

Proposition N. *Let M be a left R-module. The following are equivalent:*

i) M is Noetherian.

ii) M satisfies the ascending chain condition on left modules.

iii) If $\mathfrak{F}$ is a nonempty family of submodules, there exists a maximal element in $\mathfrak{F}$ with respect to inclusion.

Proof. To show that (i) implies (ii), we let $N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$ be an increasing sequence of modules. We need to know there is an upper bound. Let $N = \bigcup_{i \geq 1} N_i$. Since N is finitely generated, there will be a first index i such that all the generators of N belong to N_i. Thus $N = N_i$ for some i.

We show that (ii) implies (iii) by contraposition. If (iii) fails, then there exists a family $\mathfrak{F}$ of submodules for which there is no maximal element. Pick $N_1 \in \mathfrak{F}$. We can find N_2 such that N_1 is properly contained in N_2. Continuing in this way, we are left with an increasing chain that does not stabilise.

Lastly, assume that (i) does not hold; i.e. there is a submodule N that is not finitely generated. Let $\{n_1, n_2, \ldots\}$ be an infinite countable subset of N such that, for every k, $N_k = (n_1, \ldots, n_k)$ is properly contained in $N_{k+1} = (n_1, \ldots, n_{k+1})$. Now $\mathfrak{F} = \{N_k\}$ is a family of submodules without a maximal element, so (iii) fails. ∎

Proposition S. *Let $N \hookrightarrow P \twoheadrightarrow Q$ be an exact sequence of modules. Then N and Q are Noetherian if and only if P is Noetherian.*

Proof. Clearly N is Noetherian if P is. To show that Q is Noetherian, let $M \subseteq Q$ be a submodule. Then, by the fourth isomorphism theorem, M is the image of a submodule M' of P. Since M' is finitely generated, M is as well.

Conversely, assume that N and Q are Noetherian and let $M \subseteq P$ be a submodule. Let $\pi : P \twoheadrightarrow Q$ be the quotient map and consider the exact sequence $\ker(\pi_{|M}) \hookrightarrow M \twoheadrightarrow \pi(M)$. Let X be a finite generating set for $\ker(\pi_{|M})$ and Y be a finite set in M such that $\overline{Y} = \pi(Y)$ is a finite generating set of $\pi(M)$. Then for any $m \in M$, then there exist some r_x and r_y in R such that

$$m = \sum_{x \in X} r_x x + \sum_{y \in Y} r_y y$$

and $X \cup Y$ generates M. ∎

Theorem R. *The following are equivalent:*

i) R is a Noetherian ring.

ii) The free module R^n is Noetherian for every n.

iii) Every finitely generated R-module is Noetherian. ∎

A corollary of Theorem R is that every finitely generated module over a PID is Noetherian. For example, $R = K[x_1, \ldots, x_n]$ is Noetherian.

Lemma N. *If R is a PID and M a torsion-free R-module, then M is free.*

Proof. In general, we showed that there exists F free such that $F \hookrightarrow M \twoheadrightarrow T$, where T is torsion. Since M is Noetherian, we can choose a maximal F satisfying this property. We claim that $M = F$. Let $\pi : M \twoheadrightarrow T$ denote the quotient map and let $m \in M$. Since $\pi(m) \in T$ is a torsion element, there exists $r \in R$ such that $r\pi(m) = 0$. So $rm \in \ker \pi$ and $rm \in F$. Let $f_r : M \to M$ be the map that sends $m \mapsto rm$. This map is injective because M is torsion-free. Since $f_r(F) \subseteq F$ and $f_r(M) \subseteq F$, so the submodule $f_r(F, M)$ is contained in F. By Proposition F, $f_r(F, M)$ is free, so M is free. ∎

Theorem T. *Let M be a finitely generated module over a PID R. Then $M \cong R^n \oplus \mathrm{Tor}(M)$.*

Proof. Consider the exact sequence $\mathrm{Tor}(M) \hookrightarrow M \twoheadrightarrow N$ where N is torsion-free. Since R is a PID, N is free and the sequence splits, giving us the desired direct sum decomposition. ∎

The integer n given by Theorem T is called the *free rank* of a module. If two modules M and N are isomorphic, then their free ranks are equal and $\mathrm{Tor}(M) \cong \mathrm{Tor}(N)$. The following theorem is called the structure theorem for finitely generated modules over a PID.

Theorem S. *Let R be a PID and let $F \cong R^n$ be a finitely generated free module. Let M be a finitely generated submodule of F. Then there exists a basis $(e_1, \ldots, e_n)$ of F and elements $r_1, \ldots, r_m \in R$ such that $(r_1e_1, \ldots, r_me_m)$ forms a basis of M:*

$$F/M \cong R^{n-m} \oplus R/(r_1) \oplus \cdots \oplus R/(r_m)$$

The elements r_i are unique up to multiplication by a unit if we assume that r_i divides r_{i+1}. ∎

The elements r_i in Theorem S are called the *invariant factors* of the module.

6. Fields and Polynomials

Because the kernel of a homomorphism is an ideal, then any nontrivial homomorphism $f : K \to R$ is injective when K is a field. If $R = L$ is a field, then $K \subseteq L$ is a subfield and we call L an *extension* of K. We will often denote this by L/K. If L/K is a field extension then L is a vector space over K and the dimension $[L : k] = \dim_K L$ is called the *degree* of the extension. Every there is a basis (α_i) of L such that any element $l \in L$ can be expressed as $\lambda_1\alpha_1 + \cdots \lambda_n\alpha_n$ where $\lambda_i \in K$. If $K \subseteq L \subseteq M$ is a chain of extensions and (β_j) is a basis of M over L, then it can shown that $(\alpha_i\beta_j)$ is a basis of M over K. So $[M : K] = [M : L][L : K]$.

A field is *prime* if it contains no proper nontrivial subfields. Any field K is an extension of a prime field that contains 1, $1 + 1$, etc. as well as their inverses. If the characteristic of K is 0, then the prime field is $\mathbf{Q}$, and if the characteristic is a prime p, then the prime field is $\mathbf{F}_p$.

Lemma F. *Let K be a field of characteristic p. The Frobenius map $x \mapsto x^p$ is a field homomorphism (so it is injective).*

Proof. For any $x, y \in K$, we have $(x + y)^p = x^p + y^p$ (by the binomial theorem) and $(xy)^p = x^py^p$. ∎

Let L/K be an extension and $S \subseteq L$ be a set. Then $K(S)$ is the subfield of L generated by S. The extension field is finitely generated if S is finite. If S consists of a single element α, then $L = K(\alpha)$ is called a *simple* extension and α is a *primitive element*. For $\alpha_1, \ldots, \alpha_n$, the extensions $K(\alpha_1, \ldots, \alpha_n)$ and $K(\alpha_1) \cdots (\alpha_n)$ are the same and the order in which the elements are adjoined does not matter.

If K is a field then $K[x]$ is a PID. So for any irreducible polynomial $f \in K[x]$, (f) is maximal and $L = K[x]/(f)$ is a field extension. This is called the *Kronecker construction*.

Lemma R. *Every $f \in K[x]$ admits a root in a finite-degree extension.*

Proof. We may assume that f is irreducible. It is of finite degree so $L = K[x]/(f)$ is a finite degree extension and if $\alpha = x \bmod f$, then $f(\alpha) = 0$ in L. ∎

Kronecker's construction is universal in the following sense. Let L/K be an arbitrary extension and let $\alpha \in L$. Consider the map $\mathrm{Ev}_\alpha : K[\alpha] \to L$ that takes a polynomial f to $f(\alpha)$. Since $K[x]$ is a PID, the $\ker(\mathrm{Ev}_\alpha)$ is principal and equals (f_α) for some polynomial $f_a \in K[x]$. Because L is an integral domain, one of two things may happen. The first is that f_α is an irreducible polynomial, in which case we say that α is *algebraic*. The second is that the kernel is trivial and in this case we call α *transcendental*.

When α is algebraic, the unique monic irreducible polynomial f_α such that $f_\alpha(\alpha) = 0$ is called the *minimal polynomial* of α and $K(\alpha) \subseteq L$ is obtained by the Kronecker construction

$$K(\alpha) \cong K[x]/(f_\alpha).$$

If α is transcendental, $\mathrm{Ev}_\alpha : K[x] \hookrightarrow L$ is injective and it extends to the fraction field $K(x) \hookrightarrow L$ by taking $f/g \mapsto f(\alpha)/g(\alpha)$ (since $g(\alpha) \neq 0$ whenever $g \neq 0$). Liouville established the existence of transcendental numbers in 1844 by proving that

$$L = \sum_{n \geq 0} \frac{1}{10^{n!}}$$

is transcendental. We have $\mathbf{Q}(L) \cong \mathbf{Q}(x) \subseteq \mathbf{R}$. Other famous transcendental numbers are π and e.

An extension L/K is *algebraic* if every $\alpha \in L$ is algebraic over K and the following lemma proves some properties of algebraic extensions.

Lemma A. *Assume that an extension L is generated by $\alpha_1, \ldots, \alpha_n$ over K. The following are equivalent:*

i) The elements $\alpha_1, \ldots, \alpha_n$ are algebraic over K.

ii) The degree $[L : K]$ is finite.

iii) Every $\alpha \in L$ is algebraic over K.

Proof. Suppose (i) holds. We have

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq L,$$

and since each α_i is algebraic over K, it is algebraic over $K(\alpha_1, \ldots, \alpha_{i-1}$, whence

$$\big[K(\alpha_1, \ldots, \alpha_i) : K(\alpha, \ldots, \alpha_{i-1})\big] < \infty.$$

By the multiplicativity of the degree, $[L : K] \leq \infty$.

Suppose (iii) fails, i.e. some $\alpha \in L$ is not algebraic. Then $K(x) \cong K(\alpha) \hookrightarrow L$ is an injection into L, contradicting the fact that $[K(x) : K] < \infty$. Thus (ii) implies (iii).

That (iii) implies (i) is obvious, so we are done. ∎

To construct extensions of a field, we need to find irreducible polynomials. Over $\mathbf{Q}$, we can consider $x^n - p$ where p is a prime. Then $\mathbf{Q}(\sqrt[n]{p})$ is an extension of degree n over Q. A general check for irreducibility is given by the following criterion.

Theorem E (*Eisenstein's criterion*). *Let R be an integral domain and let $f \in R[x]$ be a monic polynomial of degree n. If there exists a prime ideal $\mathfrak{p}$ such that $f = x^n \bmod \mathfrak{p}$ and $f(0) \notin \mathfrak{p}^2$, then f is irreducible.*

Proof. Suppose, towards a contradiction, that $f = ab$ is reducible. Then, we have $x^n = \overline{a}\overline{b}$, where the bar indicates the polynomials modulo $\mathfrak{p}$. In particular, $\overline{a}\overline{b}$ has zero constant term. The ideal $\mathfrak{p}$ is prime, so $R/\mathfrak{p}$ is an integral domain, so both $\overline{a}$ and $\overline{b}$ have zero constant term modulo $\mathfrak{p}$, meaning that the constant terms of a and b both belong to $\mathfrak{p}$. This is a contradiction, since it is clear that the constant term of f belongs to $\mathfrak{p}^2$. ∎

We can use Eisenstein's criterion to show that cyclotomic polynomials of the form

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

for p prime are irreducible. The criterion does not immediately apply, but if we consider

$$\Phi_p(x + 1) = x^{p-1} + px^{p-2} + \frac{p(p-1)}{2}x + p,$$

we find that Eisenstein's criterion applies, so $\Phi_p(x+1)$ is irreducible and this implies that $\Phi_p(x)$ is irreducible, since any factorisation for $\Phi_p(x)$ would give a factorisation for $\Phi_p(x + 1)$ (replacing x with $x + 1$).

There are other many other criteria for reducibility/irreducibility; we give two more famous ones.

Theorem C (*Cohn's criterion*). *Suppose that p is prime and in some base b,*

$$p = a_n b^n + \cdots + a_1 b + a_0.$$

Then $f = a_n x^n + \cdots + a_1 x + a_0$ is irreducible in $\mathbf{Z}[x]$. ▮

Lemma G (*Gauss' lemma*). *Let R be a UFD with fraction field K and let $f \in R[x]$ be a polynomial of degree n such that $\gcd(a_n, \ldots, a_0) = 1$. If f is reducible in $K[x]$, then f is reducible in $R[x]$.* ▮

Gauss' lemma is often applied with $R = \mathbf{Z}$ and $K = \mathbf{Q}$. It says that it f is irreducible in $\mathbf{Z}[x]$, then it is irreducible in $\mathbf{Q}[x]$.

7. Splitting Fields

We begin with a lemma regarding the interchangeability of the roots of a polynomial.

Lemma I. *Let $f \in K[x]$ be a monic, irreducible polynomial and let L/K be an extension of the field K. If α, β are two roots of f in L, then there is a field isomorphism $K(\alpha) \cong K(\beta)$.*

Proof. This follows from the universality of the Kronecker construction: $K(\alpha) \cong K[x]/(f) \cong K(\beta)$. ▮

More generally, any field isomorphism $\phi : K \to L$ extends uniquely to a ring isomorphism $\overline{\phi} : K[x] \to L[x]$ defined by applying ϕ on the coefficients. Then $f \in K[x]$ is irreducible if and only if $\overline{\phi}(f)$ is irreducible. Let α be an arbitrary root of an irreducible polynomial $f \in K[x]$ and let β be an arbitrary root of $\overline{\phi}(f)$. Then there exists a unique field isomorphism $\phi^* : K(\alpha) \to L(\beta)$ that takes α to β and whose restriction to K is ϕ. A corollary of this fact is that if $f \in K[x]$ is irreducible, then all roots of f have the same multiplicity in an algebraic closure (this will be expanded on later).

A *splitting field* for a polynomial $f \in K[x]$ is an extension L/K such that

$$f = \prod_{i=1}^{n} (x - \alpha_i)$$

for $\alpha_i \in L$ and $L = K(\alpha_1, \ldots, \alpha_n)$.

Proposition S. *Every polynomial $f \in K[x]$ of degree n admits a splitting field of degree at most $n!$.*

Proof. Let α_1 be an abstract root of f in $K(\alpha_1)$ obtained by the Kronecker construction. Then $f = (x-\alpha_1)f_1$ for some $f_1 \in K(\alpha_1)$. Let α_2 be a root of an irreducible factor of f_1 and extend the field to $K(\alpha_1, \alpha_2)$. This process happens at most n times, by which time we will have found a splitting field L of f. We have

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq L,$$

and the degree of each f_i is $n - i$. So by multiplicity of the degrees we have $[L : K] \leq n!$. ▮

For example, the polynomial $f = x^4 - 1$ has roots $\pm 1, \pm i$. When $K = \mathbf{Q}$, the abstract bound for the degree of the splitting field is $4! = 24$, but in fact $\mathbf{Q}(i)$ is a splitting field for f, of degree 2. More generally, when $f = x^n - 1$, the roots are the nth roots of unity $1, \omega, \ldots, \omega^{n-1} \in \mathbf{C}$, where $\omega = e^{2ki\pi/n}$ for $i = 0, \ldots, n-1$. The roots form a group isomorphic to $\mathbf{Z}/n\mathbf{Z} = \langle \omega \rangle$ and $K(\omega)$ is the splitting field of $x^n - 1$, since if one root is added, all of its powers come along for the ride. If n is prime, then the degree of this splitting field is $n - 1$; in general, the degree is equal to $\varphi(n)$ where φ denotes Euler's totient function.

The following theorem shows that splitting fields are unique up to K-isomorphism.

Theorem K (*Kronecker*, 1887). *Let $f \in K[x]$ be an irreducible polynomial. Let α and α' be two roots of f in two splitting fields L/K and L'/K respectively. Assume the existence of a map $\theta_0 \in \mathrm{Aut}(K)$ that fixes coefficients of f. Then there exists an isomorphism $\theta : L \to L'$ such that $\theta_{|K} = \theta_0$ and $\theta(\alpha) = \alpha'$.*

Proof. The proof is by strong induction on $n = \deg f$. If f splits in $K[x]$, then $L = K = L'$. We can take $\theta = \theta_0$, finishing the case when $n = 1$ and when every irreducible factor of f has degree 1.

Now we assume that the theorem is proved for any field K, automorphism θ_0 and polynomial f of degree less than n. Now let $p \in K[x]$ be an irreducible factor of f of degree at least 2. If $\alpha \in L$ and $\alpha' \in L'$ are roots of p, then we can extend θ_0 to an isomorphism $\theta : K(\alpha) \to K(\alpha')$. Let $K_1 = K(\alpha)$ and ${K_1}' = K(\alpha')$ for short. We have $f = (x-\alpha)f_1$ in K_1 and $f = (x-\alpha'){f_1}'$ in ${K_1}'$ where f_1 and ${f_1}'$ have degree $n-1$. Now L is a splitting field for f_1 over K_1 and L' is a splitting field for ${f_1}'$ over ${K_1}'$. Since the degrees of f_1 and ${f_1}'$ are less than n, by the induction hypothesis there is an isomorphism $\theta^* : L \to L$ that extends the isomorphism $\theta : K_1 \to {K_1}'$. The restriction of θ^* to K_1 is θ, and the restriction of that onto K is θ_0. ∎

Let L/K and L'/K be field extensions. A K-*embedding* $L \hookrightarrow L$ is an injective homomorphism that fixes K. If $\theta : L \to L'$ is a bijection, we call it a K-*automorphism*. The *Galois group* of a polynomial $f \in K[x]$ is the group of K-automorphisms of a splitting field of K. If L is a splitting field, we denote this group by $\mathrm{Gal}(L/K)$ or $\mathrm{Aut}(L/K)$. For short, we may use the notation $\mathrm{Gal}(f)$ for a polynomial f, but this is only well-defined up to conjugacy. If L/K and L'/K are two splitting fields, then by Theorem K there exists a K-isomorphism $\theta : L \to L'$ and $\mathrm{Aut}(L/K) \cong \mathrm{Aut}(L'/K)$.

Lemma A. *Let R be the roots of a polynomial f. Then $\mathrm{Gal}(f)$ acts on R.*

Proof. If $\theta \in \mathrm{Gal}(f)$ and $f(\alpha) = 0$, we have

$$\alpha^n + \lambda_{n-1}\alpha^{n-1} + \cdots + \lambda_1\alpha + \lambda_0 = 0$$

and

$$\theta(\alpha)^n + \lambda_{n-1}\theta(\alpha)^{n-1} + \cdots + \lambda_1\theta(\alpha) + \lambda_0 = 0$$

so $\theta(\alpha) \in R$. This defines an action $\mathrm{Gal}(f) \to \mathrm{Sym}(R)$. ∎

Proposition F. *The action of $\mathrm{Gal}(f)$ on the set of roots R is faithful.*

Proof. Let $L = K(R) = K(\alpha_1, \ldots, \alpha_n)$ be a splitting field. Suppose that $\theta \in \mathrm{Gal}(f)$ acts trivially on R, i.e. $\theta(\alpha_i) = \alpha_i$ for all i. Since $\theta_{|K} = \mathrm{Id}$, $\theta = \mathrm{Id}$ as an automorphism of L. ∎

We have established that $\mathrm{Gal}(f) \hookrightarrow \mathrm{Sym}(R)$ is a group of permutations of the roots of f.

Proposition O. *Let $\mathrm{Gal}(f)$ act on the set R of roots of f. Then the orbit $\mathrm{Gal}(f)\alpha$ of $\alpha \in R$ is the set R_1 of roots of f_1 where f_1 is the irreducible factor of f such that $f_1(\alpha) = 0$.*

Proof. If $f_1(\alpha) = 0$, since $f_1 \in K[x]$. we have $f_1\big(\theta(\alpha)\big) = 0$ so $\theta(\alpha) \in R_1$ (the set of roots of f_1). Thus $\theta(R) \subseteq R_1$. Furthermore, since f_1 is irreducible, Kronecker's uniqueness theorem shows that for any two roots α and β of f_1, there exists some $\theta_i : L \to L$ such that $\theta_i(\alpha) = \beta$. So $\mathrm{Gal}(f)\alpha = R_1$. ∎

As a corollary, if f is already irreducible, then $\mathrm{Gal}(f)$ is transitive. In general, it is not tractable to classify all the transitive subgroups (up to conjugacy) of S_n. This has been done for small n, however; for example, when $n = 6$ there are 16 different possible subgroups.

Let us look at an example. Consider $f = (x^2-2)(x^2-3)$ over the field $K = \mathbf{Q}$. Then $R = \{\pm\alpha = \sqrt{2}, \pm\beta = \sqrt{3}\}$ and $L = \mathbf{Q}(\alpha, \beta)$. The Galois group cannot take $\sqrt{2}$ to $\sqrt{3}$ because such a permutation does not preserve the relations between the roots: If $\theta(\alpha) = \beta$, then $2 = \theta(\alpha^2) = \theta(\alpha)^2 = 3$, a contradiction. In this case, $\mathrm{Gal}(f)$ is the Klein four-group V. Let θ_2 be the permutation that switches $\pm\sqrt{2}$ and let θ_3 transpose $\pm\sqrt{3}$. Then the two commute and generate a group isomorphic to V.

As another example, consider $f = x^4 - 2$ over $K = \mathbf{Q}$. Eisenstein's criterion with $p = 2$ tells us that f is irreducible, and the set of roots turns out to be $R = \{\pm\alpha = \sqrt[4]{2}, \pm\beta = i\sqrt[4]{2}\}$. The splitting field is $L = \mathbf{Q}(\alpha, \beta)$. We can employ a useful trick, namely that *if the coefficients of f are real, then complex conjugation permutes the roots.* This gives us an element in $\mathrm{Gal}(f)$ of order 2: the permutation that fixes α and takes $\beta \mapsto -\beta$. In any case, we will employ a more general method to compute $\mathrm{Gal}(f)$. Let $\theta \in \mathrm{Gal}(f)$. Since $\alpha^2 + \beta^2 = 0$, we have

$$\theta(\alpha)^2 + \theta(\beta)^2 = 0.$$

Suppose that $\theta(\alpha) = \beta$. Then $\theta(\beta)^2 = -\beta^2$ and $\theta(\beta)$ is $\pm i\beta$. If $\theta(\beta) = -i\beta = \alpha$, then we have the order 2 automorphism

$$s = (\alpha \leftrightarrow \beta, -\alpha \leftrightarrow -\beta).$$

If, instead, we have $\theta(\beta) = i\beta = -\alpha$, then we have the order 4 automorphism

$$r = (\alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha).$$

We conclude that $\mathrm{Gal}(f) = \langle r, s\rangle = D_4$.

A field is *algebraically closed* if every $f \in K[x]$ admits a root in K. For example, $\mathbf{C}$ is algebraically closed. Every algebraically closed field is infinite. The Kronecker construction tells us that for any finite set $F \subseteq K[x]$, there is a finite extension L of K such that every polynomial $f \in F$ splits in L. We can extend our definition of a splitting field to (not necessarily finite) subsets of $K[x]$. Then an *algebraic closure* of F is a splitting field for $K[x]$.

The following theorem gives the existence and uniqueness (up to K-isomorphism) of the algebraic closure $\overline{K}$ for every field K. The construction is "universal" in the sense that if L/K is an algebraic extension, then there exists a K-embedding $L \hookrightarrow \overline{K}$.

Theorem S (*Steinitz*, 1910). *Let K be a field. There exists an algebraic closure $\overline{K}$ of K and this extension is unique up to K-isomorphism.*

Proof. First we show existence. Let $\mathfrak{A}$ be the set of all algebraic extensions of K, ordered by set inclusion. Observe that $\mathfrak{A}$ is inductive; indeed, if $L_1 \subseteq L_2 \subseteq \cdots$ is a chain, then $\bigcup_{i=1}^{\infty} L_i$ is in $\mathfrak{A}$. By Zorn's Lemma, there exists a maximal element of $\mathfrak{A}$, call it L. We claim that L is algebraically closed. Let $f \in L[x]$ be a polynomial. By the Kronecker construction, there is an extension $L(\alpha)$ of L. Then $L(\alpha)$ is algebraic and $L \subseteq L(\alpha)$. Since L is a maximal element in $\mathfrak{A}$, $L = L(\alpha)$ and f admits a root in L.

Next we show uniqueness of the algebraic closure. It is enough to show that if L is algebraic over K, then $L \hookrightarrow \overline{K}$ (if there were two algebraic closures, this would make them isomorphic). So fix an algebraic extension L/K. Consider the set of all intermediate extensions $K \subseteq L_\phi \subseteq L$ and for each L_ϕ there exists an embedding $\phi : L_\phi \to \overline{K}$. Let $\mathfrak{B}$ be the set of all such ϕ, partially ordered in the following manner: $\phi \leq \phi'$ if $L_\phi \subseteq L_{\phi'}$, i.e. ϕ' extends ϕ.

The poset $\mathfrak{B}$ is inductive, since if $\phi_1 \leq \phi_2 \leq \cdots$, then we can let

$$L_\phi = \bigcup_{i=1}^{\infty} L_{\phi_i}.$$

For any $\alpha \in L_\phi$, we have $\alpha \in L_{\phi_i}$ for some i and we can simply set $\phi(\alpha) = \phi_i(\alpha)$. (This does not depend on the choice of i since the functions extend one another.) By Zorn's Lemma, $\mathfrak{B}$ admits a maximal element $\phi : L_\phi \to \overline{K}$. We want to show that $L_\phi = L$. If not, then there exists $\alpha \in L \setminus L_\phi$. By the uniqueness of Kronecker, $\phi : L_\phi \to \overline{K}$ admits an extension $\overline{\phi} : L_\phi(\alpha) \to \overline{K}$. But since $\overline{\phi}$ is an extension of ϕ, by the maximality of ϕ we have $\phi = \overline{\phi}$ so $\alpha \in L_\phi$. ∎

As corollaries of Theorem S we have $\overline{K} = \overline{\overline{K}}$ and if $L/\overline{K}$ is algebraic, then $L = \overline{K}$.

Proposition R. *Let K be a field and $f \in K[x]$ monic and irreducible. Let $\alpha, \beta \in \overline{K}$ be roots of f. Then there exists $\theta \in \mathrm{Aut}_K(\overline{K})$ such that $\theta(\alpha) = \beta$. Conversely, if $\theta(\alpha) = \beta$ then α and β have the same minimal polynomial.*

Proof. Theorem K provides an isomorphism $\theta : K(\alpha) \to K(\beta)$ such that $\theta(\alpha) = \beta$. Then Theorem S extends θ (not uniquely) to a map in $\mathrm{Aut}_K(\overline{K})$. Conversely, if θ fixes K then it fixes the coefficients of the minimal polynomial of α and β. ∎

The group $\mathrm{Aut}_K(\overline{K})$ is called the *absolute Galois group* over K and it acts on $\overline{K}$ with finite orbits. The orbits are precisely the set of roots of irreducible polynomials in $K[x]$.

Theorem N. *Let $K \subseteq L \subseteq \overline{K}$ be an intermediate extension of K. The following are equivalent:*

i) L/K is a splitting field for a subset of polynomials over K.

ii) Every irreducible polynomial $f \in K[x]$ which admits a root in L splits in L.

iii) For all $\theta \in \mathrm{Aut}_K(\overline{K})$, $\theta(L) = L$.

Proof. Conditions (i) and (ii) are clearly equivalent. To show that (ii) implies (iii), let $\theta \in \mathrm{Aut}_K(\overline{K})$ and $\alpha \in L$. There exists $f \in K[x]$ irreducible such that $f(\alpha) = 0$. So $\theta(\alpha)$ is a root of f and $\theta(\alpha) \in L$. Lastly, suppose (iii) holds. Let $f \in K[x]$ be an irreducible polynomial and let $\alpha \in L$ be a root of f. If β is another root of f, by Proposition R there is a $\theta \in \mathrm{Aut}_K(\overline{K})$ that takes α to β, and by hypothesis, $\theta(L) = L$, so $\beta \in L$. ▮

Any intermediate extension satisfying the equivalent conditions of Theorem N is called a *normal* extension. For any normal extension L, and any $\theta \in \mathrm{Aut}_K(\overline{K})$, we can restrict θ to L. This gives a surjective group homomorphism from $\mathrm{Aut}_K(\overline{K})$ to $\mathrm{Aut}_K(L)$. The latter is denoted $\mathrm{Gal}(L/K)$ and is called the *Galois group* of L/K.

8. Separable Extensions

Besides normality, there is another important concept in the Galois theory called separability. Let $f \in K[x]$ be irreducible and $L = K[x]/(f) = K(\alpha)$ be the Kronecker extension, where α is the abstract root, and let $\overline{K}$ be an algebraic closure of K. How many K-embeddings $L \hookrightarrow \overline{K}$ are there? This number is called the *separable degree* of L/K and is denoted $[L : K]_{\mathrm{sep}}$. This is the degree of an intermediate subfield $L_{\mathrm{sep}} \subseteq L$, called the *separable closure* of K in L. Then

$$[L : K]_{\mathrm{sep}} = [L_{\mathrm{sep}} : K].$$

We define the *separable degree* $\deg_{\mathrm{sep}}(f)$ to be the number fo distinct roots of f in a splitting field. Thus if α is a root in an extension $K(\alpha)$ of K and f_α is its minimal polynomial, then

$$[K(\alpha) : K]_{\mathrm{sep}} = \deg_{\mathrm{sep}}(f_\alpha).$$

A polynomial f is called *separable* if its roots are all distinct, i.e. $\deg(f) = \deg_{\mathrm{sep}}(f)$. We can make similar definitions for an element α of an extension. Its *separable degree* is the separable degree of its minimal polynomial and it is *separable* if its minimal polynomial is separable. This is equivalent to $[K(\alpha) : K]_{\mathrm{sep}} = [K(\alpha) : K]$. An algebraic extension is *separable* if it contains only separable elements. The "universal property" in Theorem 7S gives us the multiplicativity formula

$$[M : K]_{\mathrm{sep}} = [M : L]_{\mathrm{sep}}[L : K]_{\mathrm{sep}}$$

whenever $K \subseteq L \subseteq M$ is a chain of algebraic extensions.

Proposition M. *Let $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be an algebraic extension. Then $[L : K]_{\mathrm{sep}} \le [L : K]$ and the following are equivalent:*

i) The elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ are separable over K.
ii) $[L : K]_{\mathrm{sep}} = [L : K]$.
iii) Every element of L is separable over K.

Proof. By invoking the multiplicativity of degrees, it is enough to prove the proposition for a primitive extension $K(\alpha)$. The equivalence of (i) and (ii) is discussed above and (iii) trivially implies (i). So we prove that (ii) implies (iii). If $\beta \in K(\alpha)$, then $K \subseteq K(\beta) \subseteq K(\alpha) = L$ and

$$[L : K] = [K(\alpha) : K(\beta)][K(\beta) : K].$$

If α is separable over K, then it is also separable over $K(\beta)$ so

$$[K(\alpha) : K(\beta)] = [K(\alpha) : K(\beta)]_{\mathrm{sep}}.$$

Thus if we assume that $[L : K]_{\mathrm{sep}} = [L : K]$, then we also have $[K(\beta) : K]_{\mathrm{sep}} = [K(\beta) : K]$ so β is separable over K. ▮

A *Galois extension* is an extension that is algebraic, normal, and separable.

Proposition G. *An extension is Galois if and only if it is the splitting field of a family of separable polynomials.*

Proof. If an extension is the splitting field of a family of separable polynomials then it is clearly normal and separablility comes from the fact that L/K is generated by the roots of separable polynomials. Conversely, if $\alpha \in L$, then the minimal polynomial of α splits into linear factors in L with no multiple roots, so the extension is both normal and separable. ∎

If $K \subseteq L \subseteq M$ is a tower of extensions, then M/K may not be Galois even though M/L and L/K are. In particular, the normality condition may fail. The standard example is

$$\mathbf{Q} \subseteq \mathbf{Q}[\sqrt{2}] \subseteq \mathbf{Q}[\sqrt[4]{2}].$$

The extension $\mathbf{Q}[\sqrt[4]{2}]$ is not normal, but the intermediate extensions are quadratic extensions and therefore Galois. However, it is true that M/K is separable if and only if M/L and L/K are separable.

Earlier, for an extension L/K we defined an intermediate subfield $L_{\text{sep}} \subseteq L$ called the separable closure of K in L. This is the set of elements in L which are separable over K. Since L_{sep}/K is separable, $[L_{\text{sep}} : K]$ is exactly the number of K-embeddings from $L_{\text{sep}} \hookrightarrow \overline{K}$. Since $\overline{K}$ contains the roots of every polynomial in $K[x]$, we can define the *separable closure* of K to be $K^{\text{sep}} = \overline{K}_{\text{sep}}$. A field is called *perfect* if every irreducible polynomial over it is separable. We will prove that $\overline{K}_{\text{sep}} = \overline{K}$ if and only if K is perfect.

For a polynomial $f \in K[x]$, we define its *derivative* $f' \in K[x]$ in the the usual way. If $f(x) = a_n x^n + \cdots + a_1 x + a_0$, then $f'(x) = n a_n x^{n-1} + \cdots + a_1$.

Lemma D. *Let K be a field. Then f is separable if and only if f and f' have no common root in $\overline{K}$, which is true if and only if* $\gcd(f, f') = 1$.

Proof. Observe that $\gcd(f, f') \neq 1$ if and only if f and f' have a common irreducible factor and this is equivalent to them having a common root in $\overline{K}$. If $\alpha \in \overline{K}$ is a root of f, then $f = (x-\alpha)g$ for some g and by the product rule, $f' = g + (x-\alpha)g'$ so if α is also a root of f', then $g(\alpha) = 0$ and $f = (x-\alpha)^2 h$ for some h. Conversely, if $f = (x-\alpha)^2 h$ for some h, then α is a root of both f and f'. ∎

If K is a field and f is irreducible, then f is separable if and only if $f' \neq 0$. If the characteristic is zero, then $\deg(f') = \deg(f) - 1$, so $f' \neq 0$ is equivalent to f being a nonconstant irreducible. Thus fields of characteristic zero are perfect. A field of characteristic p is perfect if the Frobenius map that takes $x \mapsto x^p$ is surjective.

9. Fixed Fields

Let G be a semigroup and L be a field. A *multiplicative character* is a map $\chi : G \to L$ which is multiplicative:

$$\chi(st) = \chi(s)\chi(t)$$

Lemma D (*Dedekind's lemma*). *Multiplicative characters on a semigroup are linearly independent, i.e. if $\chi_1, \ldots, \chi_n$ are distinct and there exist $\beta_i \in L$ such that*

$$\sum_{i=1}^{n} \beta_i \chi_i = 0,$$

then all β_i are 0.

Proof. The proof is by induction. If $n = 1$, then $\beta_1 \chi_1(s) = 0$ for all s implies that $\beta = 0$. Now assume the lemma holds for n and assume that $\sum_{i=1}^{n+1} \beta_i \chi_i = 0$. Then for any $s, t \in G$, we infer from multiplicativity that

$$\sum_{i=1}^{n+1} \beta_i \chi_i(s) \chi_i(t) = 0.$$

On the other hand,

$$\Big(\sum_{i=1}^{n+1}\beta_i\chi_i\Big)\chi_{n+1}(t)=0,$$

so by subtracting the two equations we get

$$\sum_{i=1}^{n}\Big(\beta_i\big(x_i(t)-\chi_{n+1}(t)\big)\Big)\chi_i(s)=0$$

for all $s\in G$. By the induction hypothesis, $\chi_1,\ldots,\chi_n$ are independent over L, so for $i=1,\ldots,n$

$$\beta_i\big(\chi_i(t)-\chi_{n+1}(t)\big)=0$$

for all $t\in G$. Now, $\chi_i\neq\chi_{n+1}$ if and only if there exists $t\in G$, $\chi_i(t)\neq\chi_{n+1}(t)$, so $\beta_i=0$ for all $i\leq n$. Then $\beta_{n+1}\chi_{n+1}=0$ so $\beta_{n+1}=0$. ∎

Dedekind's lemma tells us that if L/K is a field extension, then the set of homomorphisms from K to L is linearly independent. This provides an upper bound on the number of homomorphisms if the dimension of the extension is finite.

Let L be a field and $G\subseteq\mathrm{Aut}(L)$ be a subgroup. The *fixed field* of G is the field

$$L^G=\{\alpha\in L:\theta(\alpha)=\alpha\text{ for all }\theta\in G\}.$$

To give a simple proof of the main result of the section, we will require the primitive element theorem. The proof given is the treatment given by van der Waerden.

Theorem P (*Primitive element theorem*). *Let $L=K(\alpha_1,\ldots,\alpha_n)$ be a finite algebraic extension of K and suppose that $\alpha_2,\ldots,\alpha_n$ are separable (it is not required that α_1 be separable). Then there exists an element γ such that $L=K(\gamma)$.*

Proof. We can suppose that K is infinite, since otherwise we can let γ be a primitive root of unity that generates $K^\times$. Moreover, it suffices to show the theorem for two elements α and β, with β separable, since a simple induction will extend the result to arbitrary n. Let f and g be irreducible polynomials for which α and β are roots, respectively. Let $\alpha_1,\ldots,\alpha_r$ be the distinct roots of f and $\beta_1,\ldots,\beta_s$ be roots of g; let $\alpha=\alpha_1$ and $\beta=\beta_1$.

For $k\neq 1$ we have $\beta_k\neq\beta_1$ so the equation

$$\alpha_i+\beta_k x=\alpha_1+\beta_1 x$$

has at most one solution in K for every i and every $k\neq 1$. If we take $c\in K$ to be different from any of these solutions, we have

$$\alpha_i+c\beta_k\neq\alpha_1+c\beta_1$$

for every i and $k\neq 1$. Now we let

$$\gamma=\alpha_1+c\beta_1=\alpha+c\beta;$$

this is an element of $K(\alpha,\beta)$.

The element β satisfies

$$g(\beta)=0\qquad\text{and}\qquad f(\gamma-c\beta)=f(\alpha)=0,$$

with coefficients in $K(\gamma)$. The polynomials $g(x)$ and $f(\gamma-cx)$ only have the root β in common, since for $k\neq 1$, $i=1,\ldots,r$, $a_i\neq\theta-c\beta_k$ and $f(\gamma-c\beta_k)\neq 0$. Since β is separable, the polynomials $g(x)$ and $f(\gamma-cx)$ only have the factor $x-\beta$ in common and the coefficients of this factor must lie in $K(\gamma)$, so $\beta\in K(\gamma)$. The same thing can be shown for α from the identity $\alpha=\gamma-c\beta$. So $K(\gamma)=K(\alpha,\beta)$. ∎

The main theorem of this section links fixed fields to Galois extensions.

Theorem A (*Artin's fixed field theorem*). *Let L be a field and let G be a subgroup of* $\mathrm{Aut}(L)$.

i) If G acts with finite orbits, then L is a Galois extension of L^G.

ii) If $|G|$ is finite, then $[L : L^G] = |G|$ and G is the Galois group $\mathrm{Gal}(L/L^G)$.

Proof. Let $\alpha \in L \setminus L^G$ and let $\{\alpha_1, \ldots, \alpha_n\}$ be the orbit under the G-action. Then

$$p(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

is G-invariant and $p \in L^G[x]$ is separable. L is the splitting field of p so L is a Galois extension of L^G.

To prove (ii), suppose that G is finite and let $n = |G|$. Take $\alpha \in L \setminus L^G$ and since $|G\alpha| \leq n$ for any $\alpha \in L$, $[L^G(\alpha) : L^G] \leq n$. We use this in our proof that $[L : L^G] \leq n$. Take $\alpha \in L$ such that $[L^G(\alpha) : L^G]$ is maximal and let $\beta \in L$. Then $L^G(x, y)$ is a finite extension. By the primitive element theorem, $L^G(\alpha, \beta) = L^G(\gamma)$ for some $\gamma \in L$. But by the maximality of α, we have $[L^G(\alpha) : L^G] \geq L^G(\gamma) : L^G]$ so $L^G(\alpha) = L^G(\gamma)$. This means that $\beta \in L^G(\alpha)$ and since our choice of β was arbitrary, $L = L^G(\alpha)$. In particular, $[L : L^G] \leq n$.

Now if $[L : L^G] < n$, then L cannot have L automorphisms over L^G. But G is a subgroup of $\mathrm{Aut}(L/L^G)$ with n elements. So $[L : L^G] = n$ and $G = \mathrm{Aut}(L/L^G)$. ∎

This theorem tells us that finite groups give field extensions, in the following sense.

Corollary G. *If G is a finite group, then there exists an extension L/K with* $G = \mathrm{Aut}(L/L^G)$.

Proof. By the fixed field theorem, it suffices to represent G as a group of automorphisms over some field L. Let $\{x_s\}_{s \in G}$ be a set of $|G|$ indeterminate variables over some field F. Then $G = \{e, s, t, \ldots\}$ acts on the polynomial ring $F[x_e, x_s, x_t, \ldots]$ by acting on the variables:

$$sx_t = x_{st}$$

The action extends to monomials as well; for a subset $T \subseteq G$,

$$s\Big(\prod_{t \in T} x_t\Big) = \prod_{t \in T} x_{st}$$

and the action of G on $F[x_s : s \in G]$ is by ring automorphisms. We can extend the action to the fraction field $L = F(x_s : s \in G)$ and the result is a faithful action by field automorphisms. Thus $G \subseteq \mathrm{Aut}(L)$ and L has degree $|G|$ over L^G. ∎

A well-known open problem is the following: *Given a finite group G, is it possible to to find an extension $L/\mathbf{Q}$ such that $G = \mathrm{Aut}(L/\mathbf{Q})$ and $\mathbf{Q} = L^G$? Equivalently, is G the Galois group of a polynomial with rational coefficients?* For example, the group of quaternions Q_8 is the Galois group of the polynomial

$$f = x^8 - 72x^6 + 180x^4 - 144x^2 + 36$$

and the group $\mathrm{PSL}_2(7)$ of order 168 (the second non-abelian simple group) is the Galois group of

$$x^7 - 56x^6 + 609x^5 + 1190x^4 + 6536x^3 + 4536x^2 - 6804x - 5832 - tx^3(x + 1),$$

where the parameter t can be any integer $t \equiv 1 \pmod{31}$.

Proposition S. *If $f \in \mathbf{Q}[x]$ is irreducible of prime degree p with exactly two roots in $\mathbf{C} \setminus \mathbf{R}$, then the Galois group of f is S_p.*

Proof. Complex conjugation is a non-trivial Galois automorphism, which acts as a transposition since there are two non-real roots. We just need to show that there exists a p-cycle. But the number p of roots of f divides the order of the Galois group, so by Cauchy's theorem we have an element of order p. This must be a p-cycle and we have generated S_p. ∎

10. The Galois Correspondence

If L/K is a Galois extension, then $\alpha \in L \setminus K$ must be displaced by some automorphism. The converse is also true, giving us the following theorem.

Theorem F (*Galois' fixed field theorem*). *Let L/K be an algebraic extension with automorphism group $G = \mathrm{Aut}_K(L)$. Then L/K is a Galois extension if and only if $K = L^G$.*

Proof. For the forward direction, let $\alpha \in L^G$ have minimal polynomial f and splitting field M. Because M is normal, we assume that $M \subseteq L$. If $\beta \in M$ is another root of f, then we can find $\theta \in \mathrm{Aut}_K(M)$ such that $\theta(\alpha) = \beta$. Extend θ to an element in $\mathrm{Aut}_K(L)$. Since $\alpha \in L^G$, we have $\beta = \theta(\alpha) = \alpha$, i.e. f has only one root. Since L is separable, f has degree 1, so $\alpha \in K$.

For the converse, assume that $K = L^G$. Let $\alpha \in L$ have minimal polynomial f with set of roots $R \subseteq \overline{L}$, and let

$$g = \prod_{\beta \in R \cap L} (x - \beta).$$

Note that g is separable and invariant under every $\theta \in \mathrm{Aut}_K(L)$, since $\theta(R \cap L) = R \cap L$. This implies that the coefficients of g are fixed by $G = \mathrm{Aut}_K(L)$. Since $L^G = K$, $g \in K[x]$ and since $g(\alpha) = 0$, it divides the minimal polynomial. Thus $f = g$ and all the roots of f are in L, proving normality. Lastly, f is separable because g is. ∎

The Galois correspondence was used by Galois to compute Galois groups of polynomial equations. It comprises the following results:

i) Equations that are solvable by radicals have solvable Galois groups.

ii) Conversely, if $\mathrm{Gal}(f)$ is solvable, then the roots of f can be expressed as radicals.

iii) A_5 is the smallest group that is not solvable (so every equation of degree ≤ 4 can be solved by radicals).

iv) A_5 is the Galois group of a polynomial of degree 5 with rational coefficients, which is therefore not solvable by radicals.

If L/K is a Galois extension, then L/M is Galois for any intermediate extension $K \subseteq M \subseteq L$.

Theorem C (*Classical Galois correspondence*). *Let L/K be a finite Galois extension. Then there is a bijection ϕ from subgroups of $\mathrm{Gal}(L/K)$ and intermediate fields in L/K. This is explicitly given by $\phi(H) = L^H$ for $H \subseteq \mathrm{Gal}(L/K)$ and $\phi^{-1}(M) = \mathrm{Gal}(L/M)$ for an intermediate extension $K \subseteq M \subseteq L$.*

Proof. From Artin's fixed field theorem and Theorem F we know that $|G| = [L : K]$ and that the map ϕ is injective. Let M be an intermediate extension and let $H = \mathrm{Gal}(L/M)$. Observe that since L/M is Galois, Theorem F asserts that $M = L^H$. Thus ϕ^{-1} is injective and we have a bijection. ∎

The correspondence is order-reversing in that the bigger the subgroup H, the smaller the fixed field L^H. Another corollary is that a Galois extension can only have finitely many intermediate subfields and that the number of subfields is at most the number of subgroups in the Galois group.

Proposition N. *Let L/K be a Galois extension and M be an intermediate field. The following are equivalent:*

i) $\mathrm{Gal}(L/M)$ *is a normal subgroup of* $\mathrm{Gal}(L/K)$.

ii) If $s \in \mathrm{Gal}(L/K)$, then $s(M) = M$.

iii) M/K is a normal extension.

iv) $K = M^H$ where $H = \mathrm{Aut}_K(M)$.

v) If M/K is a finite extension, then $[M : K] = |\mathrm{Aut}_K(M)|$.

vi) The map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ that maps $s \mapsto s_{|M}$ is surjective with kernel $\mathrm{Gal}(L/M)$. ∎

Let L/K be a Galois extension. Let $K \subseteq M, N \subseteq L$ be intermediate subfields. The *compositum* MN of M and N is the subfield of L that they generate, i.e. the smallest subfield of L containing them. It can be shown that

$$MN = \left\{ \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_i \beta_j : \alpha_1, \ldots, \alpha_m \in M, \beta_1, \ldots, \beta_n \in N \right\}.$$

Proposition I. *If M/K and N/K are Galois, then so is the compositum MN.*

Proof. It suffices to show normality. Suppose that M and N are finite normal extensions. Write $M = K(R_1)$ and $N = K(R_2)$ as splitting fields of two polynomials f_1 and f_2 with respective root sets R_1 and R_2. Then the splitting field of the product $f = f_1 f_2$ is $K(R_1 \cup R_2)$, which is the compositum $MN = K(R_1)K(R_2)$. If M and N are infinite, we can reuse the argument by writing M and N as splitting fields of families F_1 and F_2 of polynomials. ▮

The Galois correspondence interchanges intersection and compositum, as shown by the following proposition.

Proposition S. *Let L/K be a finite Galois extension and let G and H be subgroups of* $\mathrm{Gal}(L/K)$*. Then*

i) $L^G \cap L^H = L^{\langle G,H\rangle}$;
ii) $L^G L^H = L^{G\cap H}$.

Proof. This is a corollary of Theorem C. Because $\langle G,H\rangle$ is the smallest subgroup containing both G and H, it corresponds to the largest subfield $L^G \cap L^H$ of both L^G and L^H. Likewise, the compositum $L^G L^H$ is the smallest subfield containing both L^G and L^H, so it corresponds to the largest subgroup $G \cap H$ of both G and H. ▮

If M and N are Galois then MN is Galois and we have a homomorphism

$$f : \mathrm{Gal}(MN/K) \to \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$$

that maps $\sigma \mapsto (\sigma_{|M}, \sigma_{|N})$. It can be shown that $\ker f = \{e\}$ and $\mathrm{Im}\, f$ consists of pairs (s,t) for which $s_{|M\cap N} = t_{|M\cap N}$. In terms of polynomials, if $f = f_1 f_2$, the Galois group of f is the subgroup of $\mathrm{Gal}(f_1) \times \mathrm{Gal}_(f_2)$ consisting of pairs of permutations that coincide on $K(R_1) \cap K(R_2)$, where R_1 and R_2 are the root sets of f_1 and f_2.

Thus, if L/K is a Galois extension such that $L = MN$ for normal extensions M/K and N/K, and furthermore $M \cap N = K$, then $\mathrm{Gal}(L/K)$ can be expresed as the direct product

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K).$$