Commutative Algebra for Algebraic Number Theory and Algebraic Geometry

David Rufino

June 5, 2020

Contents

Chapter 1

Algebra

1.1 Introduction

Follows largely a subset of Lang's algebra with some changes notably in Galois Theory, and some more explicit statements, proofs and cross referencing.

- Separable is defined in the obvious way and proved to be equivalent to Lang
- Work consistently with field extensions K/k as k-algebras, rather than simply subfields
- I believe the treatment of the "exchange lemma" is corrected

1.2 Structures

1.2.1 Categories

A (locally small) category $\mathcal{C}$ consists of

- a collection $\mathrm{ob}(\mathcal{C})$ of objects
- for every pair of objects $a, b \in \mathrm{ob}(\mathcal{C})$ a *set* of morphisms $\mathrm{Mor}(a, b)$
- for every three objects a, b, c a composition mapping

$$\begin{aligned} \mathrm{Mor}(a,b) \times \mathrm{Mor}(b,c) &\to \mathrm{Mor}(a,c) \\ (g, f) &\to g \circ f \end{aligned}$$

such that the following conditions hold

- $h \circ (g \circ f) = (h \circ g) \circ f$
- There exists $1_a \in \mathrm{Mor}(a, a)$ such that $1_a \circ f = f$ and $g \circ 1_a = g$.

Definition 1.2.1 (Isomorphism)
A morphism $\phi \in \mathrm{Mor}(a, b)$ is an isomorphism if there exists $\psi \in \mathrm{Mor}(b, a)$ such that $\phi \circ \psi = 1_b$ and $\psi \circ \phi = 1_a$.

Example 1.2.2
The category of sets is **Set** *with maps in the usual way. Note associativity is automatically satisfied. Most categories are subcategories of this one.*

Example 1.2.3 (Pointed category)
Given a category $\mathcal{C}$ where objects are sets, we may consider the pointed category $(\mathcal{C}, \star)$ consisting of pairs (A, a) where $A \in \mathrm{ob}(\mathcal{C})$ and $a \in A$. We consider only morphisms $f : (A, a) \to (B, b)$ such that $f(a) = b$.

Example 1.2.4 (Slice category)

Definition 1.2.5 (Functor)
A (covariant) functor $F : \mathcal{C} \to \mathcal{D}$ is a mapping

$$F : \mathrm{ob}(\mathcal{C}) \to \mathrm{ob}(\mathcal{D})$$

together with a mapping

$$F : \mathrm{Mor}(a, b) \to \mathrm{Mor}(F(a), F(b))$$

which satisfies

- $F(1_a) = 1_{F(a)}$
- $F(f \circ g) = F(f) \circ F(g)$

A contravariant functor is the same, except arrows are reversed.

A simple consequence of the definitions is as follows

Proposition 1.2.1
A functor preserves isomorphisms

Definition 1.2.6
For any objects $a, b, c \in \mathrm{ob}(\mathcal{C})$, there is a canonical covariant functor

$$\begin{aligned} \mathrm{Mor}(a, -) : \mathcal{C} &\longrightarrow \mathbf{Set} \\ b &\longrightarrow \mathrm{Mor}(a, b) \end{aligned}$$

which acts on morphisms $f : b \to c$ by

$$\begin{aligned} \mathrm{Mor}(a, -) : \mathrm{Mor}(a, b) &\to \mathrm{Mor}(a, c) \\ g &\to f \circ g \end{aligned}$$

It's a functor precisely because composition of functions is associative. Similarly there's a canonical contravariant functor $\mathrm{Mor}(-, b)$.

1.2.2 Groups

Definition 1.2.7 (Group)
A group is a set G together with a binary operation

$$G \times G \longrightarrow G$$
$$(g, h) \to gh$$

for which

- *there is an identity element $e \in G$ such that $eg = ge = g$ for all $g \in G$*
- *$f(gh) = (fg)h$*
- *for all $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$*

Definition 1.2.8 (Abelian Group)
A group G is abelian if the binary operation is commutative

$$gh = hg$$

Often in this case the binary operation is written additively

$$g + h$$

Definition 1.2.9
A subgroup $H \leq G$ is a subset which is closed under the group operation.

A subgroup H is defined to be normal if $gHg^{-1} = H$ for all $g \in G$. NB in an abelian group every subgroup is normal.

Example 1.2.10
$\mathbb{Z}$ is an abelian group under addition. The subgroups are of the form $n\mathbb{Z}$.

Definition 1.2.11
A mapping $\phi : G \to H$ is a homomorphism if

$$\phi(gh) = \phi(g)\phi(h)$$

Define

$$\mathrm{Im}(\phi) = \{\phi(g) \mid \phi(g)\}$$

a subgroup of H. Similarly define

$$\ker(\phi) := \{g \mid \phi(g) = e_H\}$$

This is a normal subgroup of G.

Definition 1.2.12 (n-fold product)
For $g \in G$ and $n \in \mathbb{Z}$ write g^n for the n-fold product, where $g^{-n} := (g^n)^{-1}$. In particular we see that

$$g^n g^m = g^{m+n}$$

and

$$(g^n)^m = g^{mn}$$

Definition 1.2.13 (Subgroup generated by an element)
The subgroup generated by g is $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$

Proposition 1.2.2 (Quotient Group)
Let H be a normal subgroup G. Define the quotient group

$$G/H := G/\sim$$

under the equivalence relation $g_1 \sim g_2 \iff g_2^{-1} g_1 \in H$. This is a group under the operation

$$[g][h] = [gh]\,.$$

There is a canonical surjective group homomorphism

$$G \longrightarrow G/H$$

with kernel H.

Proposition 1.2.3 (Isomorphism Theorem)
Let $\phi : G \to H$ be a homomorphism, then there is a canonical isomorphism

$$G/\ker(\phi) \longrightarrow \mathrm{Im}(\phi)$$

Example 1.2.14
The quotient group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the set of integers modulo n under addition.

Definition 1.2.15
For $g \in G$ define the order of g to be $o(g) := \inf\{n \geq 0 \mid g^n = e\}$

Proposition 1.2.4 (Lagrange's Theorem)
Let G be a finite group and H a subgroup. Then

$$\#H \mid \#G$$

Furthermore $o(g) \mid \#G$.

Definition 1.2.16
A group G is cyclic if $G = \langle g \rangle$ for some $g \in G$.

Proposition 1.2.5
Let G be a cyclic group

- *The subgroups are of the form $\langle g^r \rangle$ for $r \geq 0$.*
- *G is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$*

Proof. Let H be a subgroup and g^r be an element with minimal non-negative exponent r. By the division algorithm $H = \langle g^r \rangle$.
There is a canonical surjective homomorphism $\mathbb{Z} \to G$. It either has no kernel or the kernel is of the form $n\mathbb{Z}$. The result follows from the isomorphism theorem. □

We analyse the structure of finite cyclic groups in more detail

Proposition 1.2.6 (Finite cyclic groups)
Let G be a finite cyclic group of order n with a generator g. Then

- *The order of g^r is $n/(n,r)$*
- *For $d \mid n$ are precisely $\phi(d)$ elements of order d in particular there are $\phi(n)$ generators.*
- *For $m \mid n$ there is a unique cyclic subgroup of order m.*
- *There are exactly d elements of order dividing d*

Proof. Observe by definition g has order n. Let $h = g^r$, then $h^s = 1 \iff n \mid rs \iff \frac{n}{(n,r)} \mid \frac{r}{(n,r)}s \iff \frac{n}{(n,r)} \mid s$. Therefore h has the required order

Note g^r is a generator $\iff o(g^r) = n \iff (n, r) = 1$. Therefore there are precisely $\phi(n)$ generators.

Let $d \mid n$ then $o(g^{n/d}) = d$ because $g^{rn/d} \neq e$ for $r < d$. Let H be any subgroup and let $g^r \in H$ be an element with minimal exponent. By the division algorithm we see $H = \langle g^r \rangle$ and $r \mid n$. Therefore the unique subgroup of order d is $\langle g^{n/d} \rangle$.

Elements of order d are contained in the unique cyclic subgroup of order d therefore there are $\phi(d)$ of them.

Consider the unique subgroups H', H of order d' and d, with $d' \mid d$. By uniqueness $H' \leq H$ and any element of order d' is contained in H' and a-fortiori H. Therefore we can reduce to the case $d = n$, which is clear. □

Corollary 1.2.7
Let n be an integer then

$$n = \sum_{d|n} \phi(d)$$

Proof. Every element has order dividing n so the result follows from the previous proposition. □

For an abelian group let

$$G[d] = \{g \in G \mid g^d = e\}$$

we have shown for a cyclic group that $\#G[d] = d$ whenever $d \mid n$. We claim that this can be used to characterize cyclic groups. NB the following is adapted from this stackexchange answer

Proposition 1.2.8 (Characterization of cyclic group)
Let G be an abelian group such that $\#G[d] \leq d$ then G is cyclic.

Proof. Let $n = \#G$ and G_d be the elements of order exactly d. Then we wish to show that G_n is non-empty. We actually show that $\#G_d = \phi(d)$.

Note that $G_d \subseteq G[d]$. If it's non-empty then $\langle y \rangle$ is a subgroup of $G[d]$ of order d. Therefore $G[d] = \langle y \rangle$ and there are exactly $\phi(d)$ elements of order d by the previous Lemma.

Since G_d is either empty of order $\phi(d)$ we find that

$$n = \sum_{d|n} \#G_d \leq \sum_{d|n} \phi(d) = n$$

Therefore we must have equality everywhere and therefore $\#G_d = \phi(d)$ as required. □

1.2.3 Rings and Fields

Definition 1.2.17 (Ring)
A ring A is a set with a multiplicative and additive law of composition, $+$ and $\times$ such that

- *A is an additive group with respect to $+$, with identity 0*
- *$\times$ is associative with an identity element 1*
- *Satisfies distributive property*

$$x(y + z) = xy + xz$$
$$(x + y)z = xz + yz$$

We say that A is a zero-ring (or trivial) if $0 = 1 \iff A = \{0\}$.

A ring is commutative if in addition $xy = yx$.

Definition 1.2.18
A subset $B \subset A$ is a subring if it is closed under addition and multiplication. Then it is a ring in its own right.

NB we consider only commutative rings.

Remark 1.2.19
As is the modern convention we assume the existence of a multiplicative identity (see Poonen...)

Definition 1.2.20 (Field, Integral, Reduced)
We say a commutative ring A is

- *a Field if it is non-trivial and every non-zero element is invertible*
- *an Integral Domain (or integral) if $xy = 0 \implies x = 0$ or $y = 0$*
- *Reduced if $x^n = 0 \implies x = 0$.*

Note we have the implications

Proposition 1.2.9
Let A be a ring then we have the following implications

$$\textit{Field} \implies \textit{Integral} \implies \textit{Reduced}$$

Proof. Suppose A is a field and $xy = 0$. If $x \neq 0$ then $y = x^{-1}xy = x^{-1}0 = 0$ as required.

If A is an integral domain, then $x^n = 0 \implies x = 0$ or $x^{n-1} = 0$. It follows by induction on n that $x = 0$. □

Definition 1.2.21 (Unit)
An element $0 \neq a$ is called a unit *if it has a multiplicative inverse.*

For A not a zero-ring the set of units $A^\star$ forms an abelian group under multiplication.

1.2.4 Ring Homomorphisms

Definition 1.2.22 (Ring homomorphism)
A ring homomorphism $\phi : A \to B$ is a mapping which is both a multiplicative and additive homomorphism

- $\phi(0) = 0$
- $\phi(1) = 1$
- $\phi(x + y) = \phi(x) + \phi(y)$
- $\phi(xy) = \phi(x)\phi(y)$

The kernel of ϕ is given by

$$\ker(\phi) = \{a \mid \phi(a) = 0_B\}$$

The kernel is an example of an ideal

Definition 1.2.23
An ideal $\mathfrak{a} \triangleleft A$ is an additive subgroup of A for which $A\mathfrak{a} \subseteq \mathfrak{a}$

An ideal is proper *if $\mathfrak{a} \neq A$.*

Proposition 1.2.10
Let A be a ring and $\mathfrak{a}_i$ be a family of ideals. Then $\bigcap_i \mathfrak{a}_i$ is also an ideal of A.

Lemma 1.2.11 (Proper ideal)
An ideal $\mathfrak{a}$ is proper if and only if $1 \notin \mathfrak{a}$ if and only if $\mathfrak{a} \cap A^\star = \emptyset$.

Alternatively $\mathfrak{a} = A$ if and only if $1 \in \mathfrak{a}$ if and only if $\mathfrak{a} \cap A^\star \neq \emptyset$.

Definition 1.2.24 (Ideal generated by a set)
Given a subset X define the ideal $\langle X \rangle = AX$ to be the set of finite linear combinations

$$\langle X \rangle := \{\sum_i a_i x_i \mid a_i \in A \, x_i \in X\}$$

It is the smallest ideal containing X.

Definition 1.2.25 (Principal Ideal)
A principal ideal is an ideal generated by a single element

$$(a) = \langle \{a\} \rangle = Aa$$

Lemma 1.2.12
A principal ideal (a) is proper if and only if $a \notin A^\star$

Definition 1.2.26 (Coprime)
We say two elements x, y of a commutative ring A are coprime if $(x, y) = (1) \iff ax + by = 1$ for some $a, b \in A$

The proper ideals are precisely kernels of ring homomorphisms, as shown by the next two results.

Proposition 1.2.13
Let $\phi : A \to B$ be a ring homomorphism, then

- *The kernel $\ker(\phi)$ is an ideal of A*
- *The image $\phi(A)$ is a subring of B*
- *ϕ is injective if and only if $\ker(\phi) = \{0\}$*
- *$\mathfrak{a}$ is proper if and only if B is not a zero-ring.*

.

Proposition 1.2.14 (Quotient Ring)
Let A be a ring and $\mathfrak{a}$ an ideal. Then the set of equivalence classes

$$A/\mathfrak{a} := A/\sim \tag{1.1}$$
$$x \sim y \iff x - y \in \mathfrak{a} \tag{1.2}$$

forms a ring under the obvious multiplication and addition operations. Moreover there is a canonical surjective homomorphism

$$\pi : A \longrightarrow A/\mathfrak{a}$$

whose kernel is exactly $\mathfrak{a}$. Typically we write $\bar{x}$ for the image of x under π.

$A/\mathfrak{a}$ is a non-zero ring if and only if $\mathfrak{a}$ is proper.

Corollary 1.2.15 (Isomorphism Theorem)
Let $\phi : A \to B$ be a ring homomorphism. Then this induces a canonical isomorphism

$$A/\ker(\phi) \to \phi(A) \subset B$$

Definition 1.2.27 (Maximal, Prime, Radical)
A proper ideal $\mathfrak{a} \triangleleft A$ is

- *Maximal if it is not properly contained in another proper ideal*
- *Prime if $xy \in \mathfrak{a} \implies x \in \mathfrak{a}$ or $y \in \mathfrak{a}$*
- *Radical if $x^n \in \mathfrak{a} \implies x \in \mathfrak{a}$*

These correspond to properties of the quotient ring as follows

Proposition 1.2.16 (Criteria for Maximal, Prime and Reduced)
Let $\mathfrak{a} \triangleleft A$ then $\mathfrak{a}$ is

- *Maximal if and only if $A/\mathfrak{a}$ is a field*
- *Prime if and only if $A/\mathfrak{a}$ is an integral domain*
- *Radical if and only if $A/\mathfrak{a}$ is reduced*

Proof. We prove each in turn

- Suppose $\mathfrak{a}$ maximal. Consider $0 \neq \bar{x} \in \mathfrak{a}$ corresponding to $x \notin \mathfrak{a}$. Then $\mathfrak{a} + (x) = A$ by maximality. Therefore $ax \in 1 - \mathfrak{a}$ and $\bar{a}\bar{x} = \bar{1}$ as required. Suppse $A/\mathfrak{a}$ is a field, then by Proposition 1.2.14 $\mathfrak{a}$ is proper. Suppose $\mathfrak{a} \subsetneq \mathfrak{b}$ and consider $b \in \mathfrak{b} \setminus \mathfrak{a}$. By hypothesis $\bar{x}\bar{b} = 1$, then $xb = 1 + a$ for $a \in \mathfrak{a}$. Therefore $1 \in \mathfrak{b}$ and $A = \mathfrak{b}$ (Lemma 1.2.11).
- Suppose $\mathfrak{a}$ is prime and $\bar{x}\bar{y} = 0$. Then $\overline{xy} = 0$ and $xy \in \mathfrak{a}$. By hypothesis this implies $x \in \mathfrak{a} \vee y \in \mathfrak{a} \implies \bar{x} = 0 \vee \bar{y} = 0$. This shows that $A/\mathfrak{a}$ is an integral domain. The converse is very similar.
- This follows if one demonstrates $\bar{x}^n = \overline{x^n}$.

□

Proposition 1.2.17
Let $\mathfrak{a} \triangleleft A$ be a proper ideal, then the following implications hold

$$\textit{Maximal} \implies \textit{Prime} \implies \textit{Radical}$$

Proof. This follows from Proposition 1.2.9 and Proposition 1.2.16. For example $\mathfrak{a}$ maximal $\implies A/\mathfrak{a}$ is a field, which implies $A/\mathfrak{a}$ is an integral domain and $\mathfrak{a}$ is prime. □

Corollary 1.2.18
Let A be a ring. Then A is a field if and only if the only proper ideal is (0).

Proof. Let $\mathfrak{a} = (0)$ then $A \to A/(0)$ is an isomorphism. Then it follows by a previous Proposition. □

Corollary 1.2.19
Let $\phi : k \to B$ be a homomorphism from a field to a non-zero ring. Then ϕ is injective.

Proof. $\ker(\phi)$ is an ideal. Since the only ideals are (0) and k, the result follows. □

1.2.5 (Commutative) Algebra over a ring

Definition 1.2.28 ((Commutative) Algebra over a ring)
Let A be a ring. An algebra over A is a pair (i_B, B) where B is a commutative ring and $i_B : A \to B$ is a ring homomorphism.

We call i_B the structural morphism and write $a \cdot b := i_B(a)b$

If k is a field we may speak of a k-algebra. The morphisms consist of ring homomorphisms $\phi : B \to C$ such that $\phi \circ i_B = i_C$.

These objects form a category $\mathbf{Alg}_A$

Example 1.2.29 (Algebra over subring)
If $A \subset B$ is a subring, then B is naturally a A-algebra

The polynomial ring $A[X]$ is naturally an A-algebra

Definition 1.2.30 (Algebra generated by a set)
Let B be an A-algebra and $S \subset B$ a subset. We define $A[S]$ to be the smallest sub-A-algebra containing S.

A more explicit characterization when S is finite is given in Section 1.4.

1.2.6 Modules

Definition 1.2.31 (Module)
Let A be a ring. A (left) A-module M is an abelian group together with a multiplication by A

$$A \times M \to M$$

such that

$$(a+b)x = ax + bx$$
$$a(x+y) = ax + ay$$

Example 1.2.32 (Free Module)
The canonical example of an A-module is the free module A^I consisting of elements $(a_i)_{i \in I}$, for some indexing set I. If I is finite then we would denote this by A^n.

Definition 1.2.33 (Submodule)
Let M be an A-module. Then $N \subset M$ is a sub-module if it is an additive subgroup closed under multiplication by N.

Definition 1.2.34 (Internal sums of submodules)
Let M be an A-module, with submodules $\{M_i\}_{i \in I}$. We write

$$\sum_{i \in I} M_i$$

for the submodule of all finite linear combinations of elements in M_i. It is the smallest submodule containing all the M_i.

Definition 1.2.35 (Module homomorphism)
Let M, N be an A-module, then a module homomorphism is an additive group homomorphism $\phi : M \to N$ which is stable under A

$$\phi(am) = a\phi(m)$$

Example 1.2.36 (Trivial Examples)
A is a module over itself

An A-algebra is a-fortiori an A-module.

The ideals of A are exactly the A-submodules of A.

Definition 1.2.37 (Restriction of Scalars)
Let $\phi : A \to B$ a ring homomorphism and M a B-module. Then we may consider M as an A-module in the obvious way. Denote this by $[M]_\phi$.

Definition 1.2.38 (Faithful Module)
We say an A-module M is faithful if

$$am = 0 \quad \forall m \in M \implies a = 0$$

Definition 1.2.39 (Span of a set)
Let M be an A-module and $S \subset M$ a subset. Then define the span of S as

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} a_i s_i \mid a_i \in A \; s_i \in S \right\}$$

to be the submodule of finite linear combinations of S. It is the smallest submodule containing S.

Lemma 1.2.20
If $M \subseteq N$ then $M + N = N$.

Lemma 1.2.21
Let M be an A-module and $S, T \subset M$ two subsets. Then

$$\langle S \cup T \rangle = \langle S \rangle + \langle T \rangle .$$

Definition 1.2.40 (Linearly Independent, Spanning and Basis)
Let M be an A-module and $S \subset M$ a set. We say S is

- spanning *if $\langle S \rangle = M$*
- linearly independent *if for every finite subset $\{s_1, \ldots, s_n\} \subseteq S$ we have*

$$\sum_{i=1}^{n} a_i s_i = 0 \implies a_i = 0 \quad 1 \leq i \leq n$$

- *a* basis *if it is both spanning and linearly independent*

Definition 1.2.41 (Finite Module)
An A-module M is finite *if there exists a finite spanning set.*

Definition 1.2.42 (Free Module)
Let M be an A-module. We say that M is a free module over A if it has a basis.

Definition 1.2.43 (Vector space)
If k is a field and V a k-module, then we say V is a vector space over k.

Definition 1.2.44 (Endomorphism algebra)
For an A-module M, the set

$$\mathrm{End}_A(M) := \mathrm{Mor}_A(M, M)$$

is a ring under composition, and indeed an A-algebra with structural morphism

$$a \longrightarrow a1_M$$

1.3 Vector Spaces

Recall a vector space V over k is simply a k-module. We refer to k-submodules as subspaces. The theory is much simpler because all vector spaces are free modules.

Lemma 1.3.1
Let S be a linearly independent set. Then $S \cup \{x\}$ is linearly independent if and only if $x \notin \langle S \rangle$.

Proof. We only prove one direction. Suppose S is linearly independent and $S \cup \{x\}$ is linearly dependent. Then there exists dependence with not all coefficients equal to zero

$$0 = \lambda x + \sum_i \lambda_i s_i \quad s_i \in S$$

As S is linearly independent we have $\lambda \neq 0$ so

$$s = -\lambda^{-1} \left(\sum_i \lambda_i s_i \right) \in \langle S \rangle$$

as required. □

Theorem 1.3.2
Let Γ be a spanning set and S a linearly independent set such that $S \subseteq \Gamma$. Then there exists a basis $\mathcal{B}$ such that $S \subseteq \mathcal{B} \subseteq \Gamma$.

Proof. Let $\mathcal{I}$ be the set of subsets of Γ which contain S and are linearly independent. Then $\mathcal{I}$ is non-empty and inductively ordered. Let $\mathcal{B}$ be a maximal element of $\mathcal{I}$ then we claim $\langle \mathcal{B} \rangle = V$ so $\mathcal{B}$ is a basis.

Suppose not and choose $x \in V \setminus \langle \mathcal{B} \rangle$. Then by assumption

$$x = \sum_{i=1}^{n} \lambda_i \gamma_i$$

with all $\lambda_i \neq 0$ and $\gamma_i \in \Gamma$. If all $\gamma_i \in \langle \mathcal{B} \rangle$, then $x \in \langle \mathcal{B} \rangle$ a contradiction. Therefore at least one $\gamma_i \notin \mathcal{B}$ so by Lemma 1.3.1 $\mathcal{B} \cup \{\gamma_i\}$ is also a linearly independent subset of Γ, contradicting maximality. □

Corollary 1.3.3 (Vector Spaces are Free)
Every vector space has a basis.

Proof. Apply Theorem 1.3.2 with $S = \emptyset$ and $\Gamma = V$. □

Definition 1.3.1 (Finite dimensional)
We say that a vector space V is finite-dimensional if it is finite as a k-module.

Corollary 1.3.4 (Finite basis exists)
A finite-dimensional vector space has a finite basis.

Proof. Apply Theorem 1.3.2 with Γ any finite spanning set. □

NB I think Lang gets the following wrong by taking Γ to be a basis and the inductive step failing.

Lemma 1.3.5 (Exchange Lemma)
Let V be a vector space over k with a finite linearly-independent set S and a spanning set Γ.

Then there exists a subset T of Γ of order $\#S$ such that

$$\Gamma' := (\Gamma \setminus T) \cup S$$

is a spanning set. In particular

$$\#S \leq \#\Gamma$$

and $\#\Gamma < \infty \implies \#S < \infty$.

Proof. Proceed by induction on $\#S = n$. This is trivial when $n = 0$. Consider any $s \in S$ and $\hat{S} = S \setminus \{s\}$. By induction there is a set $\hat{T}$ of order $n - 1$ such that

$$\hat{\Gamma} := (\Gamma \setminus \hat{T}) \cup \hat{S}$$

spans V. In particular by Lemma 1.2.21

$$s = \hat{s} + \hat{w}$$

for $\hat{s} \in \langle \hat{S} \rangle$ and $\hat{w} \in \langle \Gamma \setminus \hat{T} \rangle$. We must have $\hat{w} \neq 0$, otherwise $s \in \langle \hat{S} \rangle$ which contradicts Lemma 1.3.1. Therefore

$$0 \neq \hat{w} = \sum_i \lambda_i w_i \quad w_i \in \Gamma \setminus \hat{T}$$

with not all λ_i zero. For such an element $w = w_i$ define $T = \hat{T} \cup \{w\}$. Define

$$\Gamma' := (\Gamma \setminus T) \cup S = (\hat{\Gamma} \setminus \{w\}) \cup \{s\}$$

We have

$$w = \lambda_i^{-1}\left(\hat{w} - \sum_{j\neq i}\lambda_j w_j\right) = \lambda_i^{-1}\left(s - \hat{s} - \sum_{j\neq i}\lambda_j w_j\right) \in \langle\Gamma'\rangle$$

Therefore $\langle w\rangle \subseteq \langle\Gamma'\rangle$ and

$$V = \langle\hat{\Gamma}\rangle \subseteq \langle\{w\}\cup\Gamma'\rangle \overset{1.2.21}{=} \langle w\rangle + \langle\Gamma'\rangle \overset{1.2.20}{=} \langle\Gamma'\rangle$$

as required.

□

Proposition 1.3.6 (Dimension is well-defined)
If V is finite-dimensional, then every basis is finite of the same order. We denote the order of any basis as $dim_k V < \infty$.

Proof. By Corollary 1.3.4 there exists a finite basis $\mathcal{B}$. Let $\mathcal{B}'$ be another basis. Then by Lemma 1.3.5 $\#\mathcal{B}' \leq \#\mathcal{B} < \infty$. Switching roles we find $\#\mathcal{B} \leq \#\mathcal{B}'$, whence $\#\mathcal{B} = \#\mathcal{B}'$ as required. □

Proposition 1.3.7
Let V be a finite-dimensional vector space then

- *S linearly independent $\implies \#S \leq \dim_k V$*
- *Γ spanning $\implies \#\Gamma \geq \dim_k V$*

Proof. If S is linearly independent, it can be extended to a basis by Theorem 1.3.2 so the inequality follows from Proposition 1.3.6. The other statement is similar. □

Proposition 1.3.8 (Basis criteria)
Let V be a finite-dimensional vector space. Let $\mathcal{B}$ be a subset, then the following are equivalent

1. *$\mathcal{B}$ is a basis*
2. *$\mathcal{B}$ is linearly-independent and $\#\mathcal{B} \geq \dim_k V$*
3. *$\mathcal{B}$ is spanning and $\#\mathcal{B} \leq \dim_k V$.*

Proof. Clearly $1 \implies 2,3$ by the first part.

$2 \implies 3)$ $\mathcal{B}$ is contained in a basis $\mathcal{B}'$ by Theorem 1.3.2. So using the inequality $\mathcal{B} = \mathcal{B}'$ is a basis.

$3 \implies 2)$ is similar. □

Corollary 1.3.9
Let $W_1 \subseteq W_2$ be two finite-dimensional vector subspaces then

$$\dim_k W_1 \leq \dim_k W_2$$

with equality if and only if $W_1 = W_2$.

Proof. Let $\mathcal{B}_1$ be a basis of W_1. By Theorem 1.3.2 there is a basis $\mathcal{B}_2$ of W_2 containing $\mathcal{B}_1$, whence the inequality follows.

If $\dim_k W_1 = \dim_k W_2$, then by counting we have $\mathcal{B}_1 = \mathcal{B}_2$ and $W_1 = W_2$ as required.

Conversely suppose $W_1 \subsetneq W_2$, then choose $w \in W_2 \setminus W_1$. As $w \notin \langle\mathcal{B}_1\rangle$, Lemma 1.3.1 shows that $S_2 := \mathcal{B}_1 \cup \{w\}$ is a linearly independent subset of W_2. Therefore $\dim_k W_1 = \#\mathcal{B}_1 \lneq \#S_2 \overset{1.3.7}{\leq} \dim_k W_2$ as required. □

1.4 Polynomial Rings

Definition 1.4.1
Let A be a ring. The polynomial ring $A[X]$ is an A-algebra consisting of formal sums

$$f(X) = \sum_{i=0}^{\infty} a_i X^i$$

such that only finitely many a_i are non-zero. Define degree in the obvious way

$$\deg(f) = \inf\{n \mid m > n \implies a_m = 0\} < \infty$$

and the leading coefficient to be $c(f) := a_{\deg(f)}$. By convention $\deg(0) = -\infty$. We say f is monic *if the leading coefficient is* 1.

Addition is defined in the obvious way and multiplication is defined by

$$f(X)g(X) = \sum_{d=0}^{\infty} \left(\sum_{i+j=d} a_i b_j \right) X^d$$

It's associative because

$$f(X)g(X)h(X) = \sum_{d=0}^{\infty} \left(\sum_{i+j+k=d} a_i b_j c_k \right) X^d$$

Lemma 1.4.1
If A is an integral domain then for elements $f, g \in A[X]$

$$\deg(fg) = \deg(f) + \deg(g)$$

$$c(fg) = c(f)c(g)$$

Proposition 1.4.2
The units of $A[X]$ are precisely the constant polynomials equal to units in A.

Polynomials of the form $(X - \alpha)$ are irreducible.

Proof. □

It satisfies the following universal property

Proposition 1.4.3 (Evaluation at a point)
Consider an A-algebra B and $b \in B$. Then there exists a unique A-algebra homomorphism

$$\mathrm{ev}_b : A[X] \to B$$

such that $\mathrm{ev}_b(X) = b$. We write $p(b) = \mathrm{ev}_b(p)$. It is given by

$$p(b) = \sum_{k=0}^{\deg(p)} i_B(a_k) b^k$$

The image of ev_p is equal to $A[b]$ the smallest sub-A-algebra generated by b.

Proposition 1.4.4 (Evaluation commutes with algebra homomorphism)
Let $\phi : B \to C$ be a homomorphism of A-algebras and $p \in A[X]$ then

$$\phi(p(b)) = p(\phi(b))$$

Definition 1.4.2 (Conjugate polynomial)
Let $\phi : A \to B$ be a homomorphism and $f \in A[X]$, then define

$$f^{\phi}(X) := \sum_{i=0}^{n} \phi(a_i) X^i$$

It induces a ring homomorphism

$$A[X] \to B[X]$$

and has the property that

$$f^{\phi}(\phi(a)) = \phi(f(a))$$

1.5 Finiteness

Definition 1.5.1 (Noetherian)
We say an A-module M is Noetherian if every submodule is finitely generated as an A-module

We say a ring A is Noetherian if every ideal is finitely generated as an A-module (i.e. A is Noetherian as an A-module)

The following is useful

Proposition 1.5.1 (Ascending chain condition (ACC))
Let M be an A-module. The following are equivalent

- *M is Noetherian*
- *Every ascending chain of submodules eventually terminates*

Proof. □

Proposition 1.5.2 (Restriction of Scalars preserves finiteness)
Let $\phi : A \to B$ be a finite A-algebra and M a finite B-module. Then $[M]_\phi$ is a finite A-module.

Proof. We suppose that M is generated by $m_1, \ldots, m_n$, and B is generated by $b_1, \ldots, b_m$. Then we claim that the elements $b_i m_j$ generate $[M]_\phi$. □

1.6 Unique Factorization

For this section we assume A is a commutative integral domain.

Definition 1.6.1 (Associates)
We say two non-zero elements x and y are associates if $x = uy$ for some $u \in A^\star$. We write $x \sim y$.

Lemma 1.6.1
The relation $x \sim y$ is an equivalence relation on $A \setminus \{0\}$.

Definition 1.6.2 (Irreducible element)
We say $0 \neq x$ is irreducible if $x = ab \implies a$ a unit or b a unit.

Definition 1.6.3 (Prime element)
We say $0 \neq p$ is prime if $p \mid ab \implies p \mid a$ or $p \mid b$.

Example 1.6.4
The units of $\mathbb{Z}$ are $\{-1, 1\}$ so each equivalence class is of the form $\{n, -n\}$.

Lemma 1.6.2
Suppose A is an integral domain. Then $x \mid y \wedge y \mid x \iff x \sim y$.

Proof. We have $y = ax = aby \implies y(1 - ab) = 0$. Since A is an integral domain $1 = ab$, i.e. a is a unit as required. The converse is clear. □

Example 1.6.5
A number $p \in \mathbb{Z}$ is prime in the traditional sense exactly when it is irreducible. It is of course also prime in the ring-theoretic sense but this requires proof (Bezout's Lemma).

The concept of associates is important to unique factorization, because we may only hope to have unique factorization upto multiplication by a unit.

Lemma 1.6.3
If $x \sim y$ are associates then x is irreducible iff y is

Proof. Suppose $x \sim y$ and x irreducible. If $y = ab$ then $x = abu \implies a$ a unit and bu a unit $\implies b$ a unit. Therefore y is irreducible as required. □

Example 1.6.6
The units of $\mathbb{Z}$ are $\{-1, 1\}$. Therefore n is irreducible (i.e. prime) iff $-n$ is.

Lemma 1.6.4 (Criterion for primality)
p is prime if and only if (p) is a prime ideal

Proof. Note $x \mid y \iff y \in (x)$. So in particular if p is prime then $xy \in (p) \implies p \mid xy \implies p \mid x$ or $p \mid y \implies x \in (p)$ or $y \in (p)$, whence (p) is prime.

Conversely if (p) is prime, then $p \mid xy \implies xy \in (p) \implies x \in (p)$ or $y \in p \implies p \mid x$ or $p \mid y$, so that p is prime. □

Lemma 1.6.5 (Criterion for irreducibility)
Let A be an integral domain. Then f is irreducible if and only if (f) is maximal amongst principal ideals.

Proof. Suppose f is irreducible and $(f) \subseteq (g)$. Then $f = ag$ with either a a unit or g a unit. If a is a unit then $(f) = (g)$, and if g is a unit $(g) = A$. So the result follows.

Conversely □

Proposition 1.6.6 (Primes are Irreducible)
Let A be an integral domain then p prime $\implies p$ irreducible

Proof. Suppose $b \mid p$ then $p = ab$ and $a \mid p$. By hypothesis $p \mid a$ or $p \mid b$. If $p \mid a$ (resp. b) then by Lemma 1.6.2 $p \sim a$ (resp. b) as required. □

Definition 1.6.7 (Unique Factorization Domain (UFD) or Factorial Ring)
We say an integral domain A is factorial (or a UFD) if every element $0 \neq a$ may be represented as

$$a = u \prod_{i=1}^{n} p_i$$

for u a unit and p_i irreducible, and moreover this is unique in the sense that given another factorization

$$a = u' \prod_{i=1}^{m} p'_i$$

we have $n = m$ and $p_i \sim p'_{\psi(i)}$, for ψ a permutation on $\{1, \ldots, n\}$.

Definition 1.6.8 (Atomic Ring)
We say that A is atomic if it has a (not necessarily unique) decomposition into irreducible elements.

Proposition 1.6.7
A Noetherian ring is atomic.
In fact we need only the weaker condition that any ascending chain of principal *ideals terminates (ACCP).*

Proof. □

We show a simple criterion for a ring to be a UFD.

Proposition 1.6.8 (Atomic + AP $\iff$ UFD)
The following are equivalent

- *A is a UFD*
- *A is integral, atomic and (p irreducible $\implies$ p prime)*

NB a ring satisfying irreducible $\implies$ prime is referred to as an AP-domain.

Proof. Suppose A is a UFD. Then by definition it is atomic. Suppose p is an irreducible element and $p \mid ab$, then by uniqueness it must appear in the irreducible factorization of either a or b, so we are done.

Conversely suppose A is integral and atomic. We wish to show uniqueness of factorization, that is if

$$\prod_{i=1}^{n} p_i \sim \prod_{j=1}^{m} p'_j$$

then $n = m$ and $p_i \sim p'_{\sigma(i)}$ for some permutation σ. By convention an empty product is 1 and by hypothesis all the elements are in fact prime. If $n = 0$, then since p'_j is irreducible, it is not a unit and hence $m = 0$. Otherwise consider p_1, then $p_1 \mid$ RHS , so by definition of prime we must have $p_1 \mid p'_j$ for some j. Since p'_j is irreducible and p_1 is not a unit, we have $p_1 \sim p'_j$. Since A is integral we may cancel these two to obtain an equivalence of smaller degree and we may proceed by induction. □

Furthermore it may be convenient in applications to count the multiplicities

Proposition 1.6.9 (Factorization with multiplicities)
Let A be a unique factorization domain, then for every element $0 \neq a \in A$ there is a factorization of the form

$$a = u \prod_{i=1}^{n} p_i^{r_i}$$

where $r_i > 0$ and none of the p_i are associate to each other. Furthermore this is essentially unique in the sense that given another such factorization we have $n = n'$, $r_i = r'_{\sigma(i)}$ and $p_i \sim p'_{\sigma(i)}$ for some permutation $\sigma \in S_n$.

Proof. Given a factorization into irreducible elements

$$a = u \prod_{i=1}^{n} p_i$$

Consider a representative set of irreducibles $q_1, \ldots, q_m$ (under the equivalence relation $x \sim y$). Then we have $p_i = q_{\sigma(i)} u_i$ for some units u_i. Let $r_j = \#\sigma^{-1}(j)$. Then we have that the set of irreducibles $\{p_1, \ldots, p_n\}$ is the *disjoint* union of the set of equivalence classes with representatives q_j. Therefore

$$a = u\prod_{j=1}^{m}\prod_{p\sim q_j} p = u\prod_{j=1}^{m}\prod_{i:\sigma(i)=j} u_i q_j = \left(u\prod_{j=1}^{m}\prod_{i:\sigma(i)=j} u_i\right)\prod_{j=1}^{m} q_j^{r_j}$$

as required. Suppose we have two factorizations

$$u\prod_{i=1}^{n} p_i^{r_i} = u'\prod_{i=1}^{m}(p_i')^{r_i'}$$

Let I be the indexing set of p_i and J the set of p_j'. By unique factorization there must be mappings $\sigma : I \to J$ such that $p_i \sim p'_{\sigma(i)}$, and $\tau : J \to I$ such that $p_j' \sim p_{\tau(j)}$. Which means that $p_i \sim p_{\tau(\sigma(i))}$ and $p_j' \sim p_{\sigma(\tau(i))}$. Since none are associate to each other we see that τ and σ are mutual inverses, whence $m = n$ and we may regard $\sigma \in S_n$. In the unique factorization p_i appears r_i times and $p'_{\sigma(i)}$ appears $r'_{\sigma(i)}$ times. Since p_i is associate to $p'_{\sigma(i)}$ it is not associate to any p_j' for $j \neq \sigma(i)$. Unique factorization shows that $r_i = r'_{\sigma(i)}$.

□

If we take a suitable fixed set of irreducible elements we can obtain completely unique factorization

Definition 1.6.9
Let A be a ring we say $\mathcal{P}$ is a representative set of irreducible elements if

- *No two elements $p, q \in \mathcal{P}$ are associate*
- *Every irreducible element $p \in A$ is associate to one in $\mathcal{P}$*

Example 1.6.10
For $\mathbb{Z}$ the positive *primes are a canonical set of irreducible elements.*

Corollary 1.6.10 (Canonical Factorization)
Let A be a UFD and let $\mathcal{P}$ be a set of representative irreducible elements, then we may define a valuation function

$$v_p : \mathcal{P} \times A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$$

such that for all $0 \neq a \in A$ we have

$$a = u\prod_{p\in\mathcal{P}} p^{v_p(a)}$$

This factorization is totally unique, and so v_p is additive in the sense that for a fixed irreducible $p \in \mathcal{P}$

$$v_p(ab) = v_p(a) + v_p(b)$$

Lemma 1.6.11 (Divisibility)
Suppose A is a UFD with a canonical factorization function v_p. Then $f \mid g$ iff $v_p(f) \leq v_p(g)\ \forall p$ iff $(g) \subseteq (f)$

1.7 Principal Ideal Domains

Definition 1.7.1
An integral domain A is a principal ideal domain (PID) if every ideal $\mathfrak{a}$ is principal.

Proposition 1.7.1
Let A be a PID. An element $a \in A$ is irreducible if and only if (a) is maximal.

Proof. This follows from the definition of a PID and Lemma 1.6.5. □

Proposition 1.7.2
A PID is a Noetherian UFD.

Furthermore irreducible $\iff$ prime and every prime ideal is maximal.

Proof. Suppose we have an ascending chain of ideals

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_n \ldots$$

Clearly the union is again an ideal, which is also principal of the form (a). We must have $a \in \mathfrak{a}_n$ for some n, whence it terminates after n. Therefore A is Noetherian by Proposition 1.5.1 and atomic by Proposition 1.6.7. By Proposition 1.6.8 it's enough to show that an irreducible element is prime.

Note that from previous results, and by hypothesis, we have

$$p \text{ irreducible} \overset{1.7.1}{\iff} (p) \text{ maximal} \overset{1.2.17}{\implies} (p) \text{ prime} \overset{1.6.4}{\iff} p \text{ is prime}$$

Finally p prime $\implies$ p irreducible by Proposition 1.6.6 to complete the equivalences.

Every prime ideal is principal of the form (p) and we've already shown it's maximal.

□

Proposition 1.7.3
$\mathbb{Z}$ is a PID.

In particular an integer m is irreducible $\iff$ it is prime and every prime ideal is maximal.

Proof. This follows from the well-ordering principle. Let $\mathfrak{a}$ be an ideal with minimal positive element d. We claim $\mathfrak{a} = (d)$. By the division algorithm (or apply well-ordering principle to the coset $x + (d)$), for every $x \in \mathfrak{a}$ there is $0 \leq r < d$ and $q \in \mathbb{Z}$ such that

$$x = qd + r\,.$$

Clearly $r \in \mathfrak{a}$, whence by minimality $r = 0$ as required. □

Example 1.7.2
Let k be a field, then the ring of polynomials $k[X]$ is a PID, as shown in later.

Lemma 1.7.4 (Co-prime elements in a PID)
Let A be a PID, then x, y are coprime if and only if they have no non-invertible common divisors.

Proof. First suppose $(x, y) = 1$, then $ax + by = 1$ and any common divisor d must divide 1 and therefore be invertible.

Conversely suppose $(x, y) \neq (1)$, since A is a PID it must equal (d) for some non-invertible d which is then a common divisor. □

1.8 Matrix Rings

Definition 1.8.1
Let A be a non-zero commutative ring. Define the set of matrices

$$\mathrm{Mat}_{m,n}(A) = \{(E_{ij})_{i=1\ldots n\, j=1\ldots m}\}$$

There is the standard multiplication operator

$$\mathrm{Mat}_{m,n}(A) \times \mathrm{Mat}_{n,p}(A) \to \mathrm{Mat}_{m,p}(A)$$

If $\phi : A \to B$ is a ring homomorphism, then there is a pointwise map

$$\begin{array}{rcl} \mathrm{Mat}_{m,n}(A) & \to & \mathrm{Mat}_{m,n}(B) \\ E & \to & E^{\phi} \end{array}$$

Matrices are concrete realisations of linear maps of finite free A-modules, as demonstrated in the next two Propositions.

Proposition 1.8.1 (Matrix by vector multiplication)
There is a canonical bijection of A-algebras

$$\begin{array}{rcl} \mathrm{Mat}_{m\times n}(A) & \longrightarrow & \mathrm{Mor}_A(A^n, A^m) \\ E & \longrightarrow & (v_j)_{j=1\ldots n} \to \left(\displaystyle\sum_{j=1}^{n} E_{ij} v_j\right)_{i=1\ldots m} \end{array}$$

under which matrix multiplication corresponds to composition of functions.

Typically we simply write this as $Ev \in A^m$ for $v \in A^n$, so

$$(EF)v = E(Fv)$$

Corollary 1.8.2 (Algebra of matrices)
The set of square matrices $\mathrm{Mat}_{n,n}(A)$ forms an A-algebra under multiplication.

Similarly

Proposition 1.8.3 (Matrix representation of a morphism)
Let M, N be two finite free A-modules with bases $\mathcal{B}$, $\mathcal{B}'$ of order m and n respectively. Let $\phi \in \mathrm{Mor}_A(M,N)$, then there is a unique matrix $[\phi]^{\mathcal{B}}_{\mathcal{B}'} \in \mathrm{Mat}_{n\times m}(A)$ such that

$$\phi(m)_{\mathcal{B}'} = [\phi]^{\mathcal{B}}_{\mathcal{B}'} m_{\mathcal{B}}\,.$$

Explicitly it is characterized by the relationship

$$\phi(m_i) = \sum_{j=1}^{q} [\phi]_{ji} n_j \quad i = 1 \dots p$$

where $\mathcal{B} = \{m_1, \dots, m_p\}$ and $\mathcal{B}' = \{n_1, \dots, n_q\}$.

In addition of L is a finite free A-module with basis $\mathcal{B}''$ and $\psi \in \mathrm{Mor}_A(N,L)$, then

$$[\psi \circ \phi]^{\mathcal{B}}_{\mathcal{B}''} = [\psi]^{\mathcal{B}'}_{\mathcal{B}''}[\phi]^{\mathcal{B}}_{\mathcal{B}'}$$

In particular we induce an A-algebra isomorphism

$$\mathrm{End}_A(M,N) \longrightarrow \mathrm{Mat}_{n\times m}(A)$$
$$\phi \longrightarrow [\phi]^{\mathcal{B}}_{\mathcal{B}'}$$

for every pair of bases and

$$[1_M]^{\mathcal{B}}_{\mathcal{B}} = I_n$$

is the identity matrix.

Corollary 1.8.4
Let M be a finite free A-module with bases $\mathcal{B}, \mathcal{B}'$ and $\phi \in \mathrm{End}_A(M)$. Then ϕ is an isomorphism if and only if $[\phi]^{\mathcal{B}}_{\mathcal{B}'}$ is invertible.

Corollary 1.8.5 (Change of basis)
Let M be a finite free A-module and $\mathcal{B}, \mathcal{B}'$ bases then

$$[1_M]^{\mathcal{B}}_{\mathcal{B}'} = \left([1_M]^{\mathcal{B}'}_{\mathcal{B}}\right)^{-1}$$

and

$$[\phi]^{\mathcal{B}'}_{\mathcal{B}'} = P[\phi]^{\mathcal{B}}_{\mathcal{B}}P^{-1}$$

where

$$P := [1_M]^{\mathcal{B}}_{\mathcal{B}'}$$

is invertible.

We may define determinants as follows

Definition 1.8.2 (Determinant of a Matrix)
Let A be a ring, then define the determinant of a square matrix $E \in \mathrm{Mat}_{n\times n}(A)$ as follows

$$\det(E) := \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} E_{i\sigma(i)}$$

Proposition 1.8.6
The determinant satisfies a number of properties

- $\det(EF) = \det(E)\det(F)$
- $\det(I_n) = 1$
- $\det(PEP^{-1}) = \det(E)$

Proof. Regard det as a function of the matrix columns, namely a mapping $(A^n)^n = A^n \times \ldots \times A^n \to A$. □

Proposition 1.8.7
Let $\phi : A \to B$ be a ring homomorphism and $E \in \mathrm{Mat}_{n,n}(A)$, then

$$\det(E^{\phi}) = \phi(\det(E))$$

Corollary 1.8.8
Let M be a finite free A-module and $\phi \in \mathrm{End}_A(M)$, then define

$$\det(\phi) := \det([\phi]_{\mathcal{B}})$$

This is independent of the basis $\mathcal{B}$.

Proposition 1.8.9 (Adjoint Matrix)
Let $E \in \mathrm{Mat}_n(A)$ then there exists an adjoint matrix E^{ad} such that

$$EE^{\mathrm{ad}} = E^{\mathrm{ad}}E = \det(E)I_n$$

Explicitly

$$E^{\mathrm{ad}}_{ij} = (-1)^{i+j}\det(E_{(ji)})$$

where $E_{(ij)}$ is formed from E by removing the i-th row and j-th column.

Corollary 1.8.10 (Existence of an Inverse)
Let $E \in \mathrm{Mat}_n(A)$ then E is invertible if and only if $\det(E) \neq 0$.

1.9 Polynomial ring over a field

Consider polynomials over a field k.

Proposition 1.9.1
Degree is multiplicative in the sense $0 \neq f, g$ we have

$$\deg(fg) = \deg(f) + \deg(g)$$

In particular $f \mid g \implies \deg(f) \leq \deg(g)$.

Proposition 1.9.2
The units of $k[X]$ are precisely the non-zero polynomials of degree 0.

Proposition 1.9.3 (Associate polynomials)
The following are equivalent for $0 \neq f, g$

- $f \sim g$
- $f = \lambda g$ *for* $\lambda \neq 0$
- $f \mid g$ *and* $g \mid f$

Proposition 1.9.4
A polynomial $f \in k[X]$ is associate to precisely one monic polynomial g. If f is irreducible so is g.

Proof. **TODO** □

Proposition 1.9.5 (Division Algorithm)
For k a field consider the polynomial ring $k[X]$. For every pair of polynomials $f(X)$, $g(X)$ there exists unique polynomials $q(X)$ and $r(X)$ such that

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

and $\deg(r) < \deg(g)$.

Proof. Suppose $\deg(f) < \deg(g)$ then we simply have $q = 0$ and $r = f$. So assume wlog that $\deg(f) \geq \deg(g)$. □

Proposition 1.9.6 (Polynomial ring is a PID)
Let k be a field, then $k[X]$ is a PID, and therefore a Noetherian UFD.

Proof. Let $(0) \neq \mathfrak{a}$ be an ideal and let $f \in \mathfrak{a}$ be a polynomial of minimal degree. We may assume it is monic. Any $g \in \mathfrak{a}$ may be represented as $f = qg + r$ by the division algorithm. Clearly $r \in \mathfrak{a}$, therefore by minimality $r = 0$, whence $g \in (f)$. □

Proposition 1.9.7 (Unique Factorization of Polynomials)
For the ring $k[X]$ the set of irreducible monic polynomials constitutes a representative set (Definition 1.6.9). Therefore we have a unique factorization

$$f = c(f) \prod_{p \text{ irreducible monic}} p^{v_p(f)}$$

such that

$$v_p(fg) = v_p(f) + v_p(g)$$

Proof. Proposition 1.9.4 shows that the irreducible monic polynomials constitute a representative set. Therefore the result follows from Corollary 1.6.10. Let u be the unit appearing in the factorization, it must be an element of k. Compare leading coefficients to see that $u = c(f)$. □

Lemma 1.9.8 (Roots and Multiplicity)
For $f \in k[X]$ a non-constant polynomial and $\alpha \in k$ we have

$$f(\alpha) = 0 \iff (X - \alpha) \mid f \iff v_{(X-\alpha)}(f) > 0$$

In this case $r := v_{(X-\alpha)}(f)$ is the multiplicity of the root α, and observe

$$f(X) = c(f)(X - a)^r g(X)$$

with $g(\alpha) \neq 0$ (equivalently $v_{(X-\alpha)}(g) = 0$).

Proof. The right to left implication is obvious. Conversely by the division algorithm we may write

$$f(X) = f(\alpha) + (X - \alpha)Q(X)$$

Then if $f(\alpha) = 0$ we clearly have $v_{(X-\alpha)}(f) > 0$. Finally we may construct

$$g(X) = \prod_{p \neq (X-\alpha)} p^{v_p(f)}$$

It's clear that for every p appearing in the product $p(\alpha) \neq 0$ because otherwise we would have $(X-\alpha) \mid p$ and by irreducibility $(X - \alpha) = p$. Therefore $g(\alpha) \neq 0$ as required. □

Definition 1.9.1 (Splitting Polynomial)
Let K/k be a field extension and $f \in k[X]$. We say a polynomial f splits completely in K if the irreducible factorization of f^i in $K[X]$ is

$$f^i(X) = c(f^i) \prod_{i=1}^{n} (X - \alpha_i)^{r_i}$$

where α_i are the distinct roots of $f(X)$ in K and $r_i := v_{(X-\alpha_i)}(f^i)$ are the multiplicities. Equivalently f splits in K if

$$p \in K[X] \text{ irreducible } \wedge \deg(p) > 1 \implies v_p(f^i) = 0 \tag{1.3}$$

Observe that the number of roots counting multiplicities is $\deg(f)$

$$\deg(f) = \sum_{i=1}^{n} v_{(X-\alpha_i)}(f^i)$$

Corollary 1.9.9
A polynomial f has at most $\deg(f)$ *roots*

1.9.1 Separable Polynomials

We are interested in characterizing polynomials $f \in k[X]$ which do not have multiple roots in any extension field K/k. These are exactly the separable polynomials, and it useful to consider the formal derivative $f'(X)$ as follows

Proposition 1.9.10 (Criteria for Multiple Roots)
Let $f(X) \in k[X]$ be a polynomial and either $char(k) = 0$ or $r < char(k)$. Then $\alpha \in k$ is a root of multiplicity r precisely when

$$f(\alpha) = f^{(1)}(\alpha) = \ldots = f^{(r-1)}(\alpha) = 0$$

and $f^{(r)}(\alpha) \neq 0$.
Therefore the multiple roots are precisely the common roots of $f(X)$ and $f'(X)$ (irrespective of the characteristic).

Proof. Note that by Lemma 1.9.8

$$f^{(1)}(X) = (X - \alpha)^{r-1}[rg(X) + (X - \alpha)g'(X)]$$

with $g(\alpha) \neq 0$ and r the multiplicity of the root. If $r = 1$, then $f^{(1)}(\alpha) = g(\alpha) \neq 0$ as required. If $r > 1$, then $f^{(1)}(X)$ has α as a root of multiplicity $r - 1$, so it follows by induction.
The second statement is simply the case $r = 1$. □

Definition 1.9.2 (Separable Polynomial)
A polynomial $f \in k[X]$ is separable if f and f' are coprime.

Proposition 1.9.11 (Separable Polynomial)
A separable polynomial $f \in k[X]$ has no multiple roots in any extension field K/k

Proof. Since $(f, f') = 1$ we have $af + bf' = 1$. Clearly f and f' have no common roots, and therefore f has no multiple roots by Proposition 1.9.10. □

Proposition 1.9.12
Suppose $f, g \in k[X]$, g is separable and $f \mid g$, then f is separable.

Proof. Suppose f is not separable then by Lemma 1.7.4 f and f' have a common divisor d such that $\deg(d) > 0$. Since $g = fh$, so $g' = f'h + fh'$. Therefore d is also a non-trivial common divisor of g and g' contradicting Lemma 1.7.4. □

We can provide a partial converse by working in a large enough extension field

Proposition 1.9.13 (Separability)
Let K/k be a field extension and $f \in k[X]$ a polynomial which splits completely in K. Then TFAE

1. *f is separable*
2. *f has no multiple roots in K*
3. *f has $\deg(f)$ distinct roots in K*

Proof. Using the formula

$$\deg(f) = \sum_{i=1}^{n} v_{(X-\alpha_i)}(f)$$

we see easily that $3 \iff 2$. The previous Proposition shows that $1 \implies 2$.

Conversely suppose f is not separable, then by Lemma 1.7.4 f and f' must have a non-trivial common divisor h. Using 1.6.11 and (1.3) we see that h splits in K. Any root of h is a common root of f and f' in K, which by Proposition 1.9.10 is a multiple root of f in K. □

1.10 Cayley-Hamilton Theorem

Definition 1.10.1 (Characteristic Polynomial of a Matrix)
For a matrix $E \in \mathrm{Mat}_n(A)$ define the characteristic polynomial by

$$P_E(X) := \det(X \cdot I_n - E^T)$$

working in $\mathrm{Mat}_n(A[X])$. This is a monic polynomial in $A[X]$.

Definition 1.10.2 (Characteristic Polynomial of an endomorphism of a free module)
Let M be a finite free A-module. Define the characteristic polynomial of $\phi \in \mathrm{End}_A(M)$ by

$$P_\phi(X) := P_{[\phi]}(X)$$

This is independent of the basis $\mathcal{B}$.

Adapted from Atiyah-Macdonald (...) but more explicit theorems

Theorem 1.10.1 (Cayley-Hamilton)
Let M be a finitely generated A-module and $\phi \in \mathrm{End}_A(M)$ then there exists a monic polynomial $P(X) \in A[X]$ such that

$$P(\phi) = 0$$

When M is a finite free A-module then P may be taken to be the characteristic polynomial $P_\phi(X)$.

Proof. First since $\mathrm{End}_A(M)$ is an A-algebra there is a canonical evaluation morphism

$$\mathrm{ev}_\phi : A[X] \to \mathrm{End}_A(M)$$

and the meaning of $P(\phi)$ is simply $\mathrm{ev}_\phi(P)$.

Let $\{m_1, \ldots, m_n\}$ be a generating set, then by definition

$$\phi(m_i) = \sum_j E_{ij} m_j$$

for some $E \in \mathrm{Mat}_n(A)$. Consider the matrix

$$B(X) = XI_n - E \in \mathrm{Mat}_n(A[X])$$

Then we may define $B(\phi) := B(X)^{\mathrm{ev}_\phi} \in \mathrm{Mat}_n(\mathrm{End}_A(M))$ pointwise, so given by

$$B(\phi)_{ij} = \delta_{ij}\phi - E_{ij}1_M\,.$$

By definition

$$\sum_j B(\phi)_{ij}m_j = \phi(m_i) - \sum_{ij} E_{ij}m_j = 0$$

Formally we have a group action

$$\mathrm{Mat}_n(\mathrm{End}_A(M)) \times M^n \to M^n$$

$$F \cdot (x_1, \ldots, x_n)^T \to \left(\sum_{ij} F_{ij}(x_j)\right)_i$$

such that $(EF)v = E(Fv)$ (check).
And we have shown that

$$B(\phi)\,(m_1, \ldots, m_n)^T = \mathbf{0}$$

Using Proposition 1.8.9, premultiply by the adjoint to show that

$$\det(B(\phi))I_n\,(m_1, \ldots, m_n)^T = \mathbf{0}$$

and $\det(B(\phi)) \in \mathrm{End}_A(M)$ annihilates $m_1, \ldots, m_n$ and therefore M.

Finally we claim that $P(X) := \det(B(X)) \in A[X]$ is a suitable monic polynomial. We see that

$$P(\phi) := \mathrm{ev}_\phi(\det(B(X))) \overset{1.8.7}{=} \det(B(X)^{\mathrm{ev}_\phi}) = \det(B(\phi)) = 0$$

When M is a finite free A-module then we may choose $\{m_1, \ldots, m_n\}$ to be a basis, and then the matrix E equals $[\phi]^T$ as required.

□

1.11 Finite-type Algebras

Definition 1.11.1 (Finite algebra)
An A-algebra B is finite *if it is finite as an A-module.*

Definition 1.11.2 (Finitely generated algebra)
An A-algebra B is finitely generated (or of finite type) if there exists an integer $n \in \mathbb{N}$ and a surjection of A-algebras

$$A[X_1, \ldots, X_n] \to B$$

the images of X_i are the generators.

1.12 Ring Ideal Structure

Proposition 1.12.1
Let A be a ring and $\mathfrak{a} \triangleleft A$ a proper ideal. Then it is contained in some maximal ideal $\mathfrak{m}$.

In particular there always exists a maximal ideal.

Proof. Simple application of Zorn's Lemma. □

The following definition will be useful

Definition 1.12.1 (Multiplicatively closed set)
A subset $S \subset A$ is said to be multiplicatively closed if

- $1 \in S$
- $x, y \in S \implies xy \in S$

Further it is said to be saturated *if in addition*

$$x, y \in S \iff xy \in S$$

Example 1.12.2
Let $\mathfrak{p} \triangleleft A$ be a prime ideal, then the set $A \setminus \mathfrak{p}$ is a saturated multiplicatively closed set.

Lemma 1.12.2
Let A be a ring, S a m.c. closed set and $\mathfrak{b} \triangleleft A$ such that $\mathfrak{b} \cap S = \emptyset$ then

$$\mathcal{I} = \{\mathfrak{a} \mid \mathfrak{b} \subseteq \mathfrak{a} \quad \mathfrak{a} \cap S = \emptyset\}$$

has a maximal element, which is prime.

Proof. Since $\mathfrak{b} \in \mathcal{I}$ it is non-empty. By Zorn's Lemma it has a maximal element, $\mathfrak{p}$. We claim it is prime, for suppose $xy \in \mathfrak{p}$ and $x, y \notin \mathfrak{p}$. Then by maximality $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ intersect S. Therefore S intersects $(\mathfrak{p} + (x))(\mathfrak{p} + (y)) \subseteq \mathfrak{p}$, a contradiction. □

It is possible to define the minimal radical ideal containing a given ideal.

Proposition 1.12.3 (Prime Nullstellensatz)
The set

$$\sqrt{\mathfrak{a}} = \{x \mid x^n \in \mathfrak{a}\}$$

is a radical ideal. Any radical ideal containing $\mathfrak{a}$ also contains $\sqrt{\mathfrak{a}}$. Furthermore it satisfies

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}$$

Proof. Suppose $x, y \in \sqrt{\mathfrak{a}}$, such that $x^n \in \mathfrak{a}$ and $y^m \in \mathfrak{a}$. Then

$$(x+y)^{m+n} = \sum_{j=0}^{r} (\ldots) x^r y^{m+n-r}$$

which is clearly in $\mathfrak{a}$, so that it is an additive group. Similarly $(ax)^n = a^n x^n \in \mathfrak{a}$, so that $\mathfrak{a}$ is an ideal. Suppose $y^n \in \sqrt{\mathfrak{a}}$, then $y^{mn} \in \mathfrak{a}$, which implies $y \in \sqrt{\mathfrak{a}}$. Therefore $\sqrt{\mathfrak{a}}$ is radical.

Suppose $x \in \sqrt{\mathfrak{a}}$ then $x^n \in \mathfrak{a}$. When $\mathfrak{a} \subseteq \mathfrak{p}$ then it's clear that $x^n \in \mathfrak{p} \implies x \in \mathfrak{p}$. Therefore x lies in the right hand side.

Conversely suppose $x \notin \sqrt{\mathfrak{a}}$ then $S := \{1, x, x^2, \ldots\}$ is a proper multiplicatively closed set such that $S \cap \mathfrak{a} = \emptyset$. By Lemma 1.12.2 there is a prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ which does not intersect S. Therefore $x \notin RHS$ as required. □

We say an element x to be nilpotent if $x^n = 0$. These form an ideal.

Definition 1.12.3 (Nilradical)
Define the nilradical to be the set of nilpotents

$$\mathfrak{N}(A) := \sqrt{(0)} \overset{1.12.3}{=} \bigcap_{\mathfrak{p}} \mathfrak{p}$$

Clearly A is reduced if and only if $\mathfrak{N}(A) = \{0\}$.

Remark 1.12.4
When working with rings of functions (with codomain a field), then we wouldn't expect there to be nilpotent elements.

We also make the following definition

Definition 1.12.5 (Irreducible)
Let A be a ring. We say A is irreducible if $\mathfrak{N}(A)$ is prime.

Lemma 1.12.4 (Integral Domain $\iff$ Reduced and Irreducible)
Let A be a ring. Then A is an integral domain if and only if it is reduced and irreducible

Proof. Suppose A is an integral domain. Since $\mathfrak{N}(A)$ is the intersection of all prime ideals and (0) is prime it must be equal to (0). Therefore A is reduced and irreducible.
The converse is clear. □

1.13 Integral Algebras

Definition 1.13.1 (Integral Element)
Let $\phi : A \to B$ be a ring homomorphism and $\alpha \in B$. Then we say α is integral over A if $m^{\phi}(\alpha) = 0$ for some monic *polynomial $m(X) \in A[X]$.*

Definition 1.13.2 (Ring Extensions)
Let $\phi : A \to B$ be a ring homomorphism. Then B is

- *finite over A if it is finite as an A-module*
- *finite-type over A if it is finitely generated as an A-algebra*
- *integral over A if every element is integral over A*

We note the trivial implication

$$\text{finite} \implies \text{finite type}$$

For example $k[X]$ is a ring of finite type over k, but certainly not finite.

Proposition 1.13.1
Let $\phi : A \to B$ be a ring map and $b \in B$. Then the following are equivalent

1. *b is integral over A*
2. *$\phi(A)[b]$ is a finitely generated A-module*
3. *$\phi(A)[b]$ is contained in a subring C of B which is finitely generated as an A-module.*
4. *There exists a $\phi(A)[b]$-module M which is faithful and finitely generated as a $\phi(A)$-module.*

Proof. Note C is a faithful module, so only non-trivial step is $4 \implies 1$. This is the usual "determinant trick". We apply Theorem 1.10.1 by considering $\psi_b \in \mathrm{End}_{\phi(A)}(M)$ to be multiplication by b. Then we have some monic polynomial $P(X) \in \phi(A)[X]$ such that $P(\psi_b) = 0$, whence $P(b)m = 0$ for all $m \in M$. Since M is faithful, then we have $P(b) = 0$ as required. □

Proposition 1.13.2 (Finite-type + integral $\implies$ finite)
Let B be integral over A and finitely generated as an A-algebra then B is finitely generated as an A-module.

Proof. Consider a tower

$$A \subset A[b_1] \subset \ldots \subset A[b_1, \ldots, b_n] = B$$

By the previous Proposition $A[b_1]$ is a finite A-module. We proceed inductively on n. Namely we assume that $A[b_1, \ldots, b_i]$ is a finite A-module. Then a-fortiori $A[b_1, \ldots, b_{i+1}]$ is integral over $A[b_1, \ldots, b_i]$ and finitely generated as an algebra. Therefore by the same proposition it is a finite $A[b_1, \ldots, b_i]$-module and therefore a finite A-module (by Proposition 1.5.2) □

1.14 Galois Theory

1.14.1 Algebraic Extensions

Definition 1.14.1 (Field Extension)
A field extension K/k is a k-algebra K which is also a field.. Every field K is an extension over its prime subfield.

We typical denote the structural morphism by $i_{kK} : k \to K$, and it is automatically injective (...). We may write (K, i_{kK}) if we need to stress the relevance of the structural morphism to the argument.

These objects form a category $\mathbf{Field}_k$ *in the obvious way. The morphisms may be called k-embeddings and we denote them by*

$$\mathrm{Mor}_k(K, L)$$

and the set of automorphisms by

$$\mathrm{Aut}(K/k)\,.$$

Observe every extension K/k may be viewed as a k-vector space so we define the degree of an extension field to be the vector space dimension

$$[K : k] := \dim_k K$$

Definition 1.14.2 (Finite field extension)
A field extension K/k is finite if $[K:k] < \infty$

Definition 1.14.3 (Tower of Field Extensions)
We may also consider a "tower" of extensions

$$K_n/\ldots/K_0 = k$$

with embeddings $i_{K_iK_{i+1}} : K_i \to K_{i+1}$, with the picture that these usually correspond to inclusions. We may consider an extension K_i/K_j for $j < i$. Typically if we have a family of morphisms

$$\sigma_i : K_i \to M$$

they would commute with these embeddings. In particular we may abuse notation by defining $\sigma_i|_{K_j} = \sigma_i \circ i_{K_{i-1}K_i} \circ \ldots \circ i_{K_jK_{j+1}}$.

Proposition 1.14.1
Let L/K and K/k be two finite extensions with basis $\{l_1,\ldots,l_n\}$ and $\{k_1,\ldots,k_m\}$. Then L/k has basis $\{l_ik_j\}_{i,j}$. In particular

$$[L:k] = [L:K][K:k]$$

Corollary 1.14.2
Let $K_n/\ldots/K_0 = k$ be a tower of finite extensions then

$$[K:k] = \prod_{i=1}^{n}[K_i:K_{i-1}]$$

Definition 1.14.4 (Evaluation homomorphism)
Let K/k be a field extension and $\alpha \in K$. There is a canonical homomorphism

$$\mathrm{ev}_\alpha : k[X] \to K$$
$$\sum_{i=0}^{n} a_iX^i \to \sum_{i=0}^{n} i_{kK}(a_i)\alpha^i$$

which we write as $f(\alpha)$. We say $\alpha \in K$ is a root of $f(X)$ if $f(\alpha) = 0$.

Proposition 1.14.3 (Morphisms commute with evaluation)
Let $\sigma : K/k \to L/k$ be a morphism of field extensions then

$$\sigma(p(\alpha)) = p(\sigma(\alpha))$$

for all $p \in k[X]$. In particular α is a root of $p \iff \sigma(\alpha)$ is a root of p.

Proof. This is just a specific case of Proposition 1.4.4, The last statement is obvious, modulo the fact σ is injective (...). □

Definition 1.14.5 (Subalgebra generated by a set)
Let K/k be a field extension and $S \subset K$ a finite subset. Recall $k[S]$ is the smallest sub-algebra containing S. When S consists of a single element we have the characterization from Proposition 1.4.3.

$$k[\alpha] := k[\{\alpha\}] = \mathrm{im}(\mathrm{ev}_\alpha) = \{p(\alpha) \mid p \in k[X]\}$$

Definition 1.14.6 (Subfield generated by a set)
Let K/k be a field extension and $S \subset K$ a subset. Define the subfield generated by S

$$k(S) := \left\{ \frac{p(s_1,\ldots,s_n)}{q(s_1,\ldots,s_n)} \mid p,q \in k[X_1,\ldots,X_n]\ s_1,\ldots,s_n \in S \right\}$$

It is the smallest subfield of K containing S.

Lemma 1.14.4
If $S \subset K$ and $k[S]$ is a field then $k[S] = k(S)$

Lemma 1.14.5 (Image of f.g. field extension)
Let K/k be a field extension and S a subset. If $\sigma : K/k \to L/k$ is a morphism them

$$\sigma(k(S)) = k(\sigma(S))$$

Proposition 1.14.6 (Uniqueness of morphisms on a generating set)
Let K/k be a field extension and $S \subset K$ a finite set. If $\sigma, \sigma' : k(S)/k \to L/k$ are morphisms of field extensions such that $\sigma|_S = \sigma'|_S$. Then $\sigma = \sigma'$.

Definition 1.14.7 (Simple Extension)
A field extension K/k is simple if $K = k(\{\alpha\}) =: k(\alpha)$ for some $\alpha \in K$.

Definition 1.14.8 (Algebraic Element)
We say an element $\alpha \in K/k$ is algebraic if it is a root of a polynomial $f \in k[X]$ (i.e. α is integral, since we can always ensure f is monic)
We say an extension K/k is algebraic if every element $\alpha \in K$ is algebraic.

Proposition 1.14.7 (Finite $\implies$ algebraic)
A finite extension K/k is algebraic.

Proof. Suppose $n = \dim_k K$. The set $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is linearly dependent by Proposition 1.3.7. Therefore there is a non-zero polynomial with α as a root. □

Proposition 1.14.8 (Endomorphisms are automorphisms)
Let $\sigma \in \mathrm{Mor}_k(K, K)$ be an endomorphism of an algebraic extension. Then it is an isomorphism.

Proof. As field morphisms are injective (...) we only need to show that σ is surjective. Given $\alpha \in K$ let T denote the set of roots of $m_\alpha \in k[X]$ in K. Note by Corollary 1.9.9 T is finite. Further by Proposition 1.14.3 σ maps T to itself. Since σ is injective it is also surjective. In particular α is in the image of σ as required. □

Proposition 1.14.9 (Minimal Polynomial)
If $\alpha \in K/k$ is algebraic then there is a unique monic, irreducible polynomial $m_{\alpha,k}(X) \in k[X]$ such that $m_{\alpha,k}(\alpha) = 0$. This is called the minimal polynomial of α over k and $(m_{\alpha,k}) = \ker(\mathrm{ev}_\alpha)$.

Proof. Let $\mathfrak{a} = \ker(\mathrm{ev}_\alpha)$. Since $k[X]$ is a PID it is of the form $(m_{\alpha,k})$. As α is algebraic it is non-zero. $m_{\alpha,k}(X)$ cannot be a constant, and therefore is not a unit.

We claim $m_{\alpha,k}$ is irreducible. If $m_{\alpha,k}(X) = p(X)q(X)$ then p, q are non-zero and either $p(\alpha) = 0$ or $q(\alpha) = 0$. If $p(\alpha) = 0$ then $m_{\alpha,k} \mid p$. As $p \mid m_{\alpha,k}$ by Proposition 1.9.3 $m_{\alpha,k} = \lambda p$. In particular $\deg(m_{\alpha,k}(X)) = \deg(p(X))$ so $\deg(q(X)) = 0$ and $q(X)$ is a unit 1.9.2. Therefore by definition $m_{\alpha,k}(X)$ is irreducible.

Dividing by the leading coefficient we may assume that this polynomial is monic. Suppose $m'(X)$ is another such irreducible monic polynomial. Then $m_\alpha \mid m'$. Since m_α is not a unit, by definition of irreducible $m' \sim m_\alpha$ whence $m' = \lambda m_\alpha$. Compare leading coefficients to find $\lambda = 1$ and $m' = m_\alpha$. □

Given an irreducible polynomial $f \in k[X]$ it's possible to construct an extension field K/k which has at least one root, as follows.

Proposition 1.14.10 (Construct simple extension)
Let $f \in k[X]$ be an irreducible polynomial. Then (f) is maximal and $K := k[X]/(f)$ is a field extension with canonical structural morphism. Define $\alpha := X + (f)$

- $f(\alpha) = 0$
- *$K = k(\alpha)$ is a simple field extension and $k(\alpha) = k[\alpha]$*
- *$m_\alpha = f/c(f)$ and $\deg(m_\alpha) = \deg(f) =: n$*
- *K is a finite-dimensional k-vector space with basis*

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

Example 1.14.9
Take $k = \mathbb{R}$, $f(X) = X^2 + 1$, then $\mathbb{C}/\mathbb{R} = \mathbb{R}[i] = \mathbb{R}[X]/(X^2 + 1)$.

Proof. Consider the structural morphism $i : k \to k[X]$ and canonical surjective homomorphism

$$\pi : k[X] \to k[X]/(f)$$

and $\alpha = X + (f) = \pi(X)$. As $k[X]$ is a PID, f irreducible implies (f) maximal by Lemma 1.7.1 so K is a field by Proposition 1.2.16. The composition $\pi \circ i$ makes K into a k-algebra and hence a field extension. Furthermore π is then by definition a k-algebra homomorphism.

Since π is surjective every $\beta \in K$ is represented as $\pi(p(X)) \overset{1.14.3}{=} p(\pi(X)) = p(\alpha)$. By Proposition 1.14.5 we see $K = k[\alpha]$. Since K is a field then $K = k[\alpha] = k(\alpha)$ is simple by Lemma 1.14.4.

Similarly $f(\alpha) = f(\pi(X)) \overset{1.14.3}{=} \pi(f(X)) = 0$, so α is a root of f. By Proposition 1.9.3 $f/c(f)$ is irreducible and by uniqueness in Proposition 1.14.9 we have $m_\alpha = f/c(f)$.

Given $\beta = p(\alpha)$, the division algorithm (...) yields

$$p(X) = q(X)f(X) + r(X)$$

with $\deg(r) < \deg(f) = n$. Therefore $\beta = r(\alpha)$ and the given set is spanning. A non-trivial linear dependence yields a non-zero polynomial $g(X)$ such that $g(\alpha) = 0$ and $\deg(g) < \deg(f)$. But by definition of the minimal polynomial $m_\alpha \mid g$ a contradiction by comparing degrees. Therefore the given set is linearly independent and hence a basis. □

Conversely any simple algebraic extension is obtained in this way, as follows

Proposition 1.14.11 (Simple extension)
Let $k(\alpha)/k$ be a simple extension. Then there is a canonical isomorphism of k-algebras

$$k[X]/(m_\alpha) \longrightarrow k(\alpha)$$

under which $X + (m_\alpha) \to \alpha$. Further $k(\alpha)$ is a finite-dimensional vector space with basis

$$\{1, \alpha, \ldots, \alpha^{n-1}\}$$

where $n = \deg(m_\alpha) = [k(\alpha) : k]$ and $k(\alpha) = k[\alpha]$.

Proof. By Proposition 1.14.9, Definition 1.14.5 and Corollary 1.2.15 there is a canonical isomorphism $k[X]/(m_\alpha) \to k[\alpha]$ of k-algebras induced by the evaluation homomorphism $\mathrm{ev}_\alpha : k[X] \to K$. Proposition 1.14.10 shows that the image of this isomorphism, $k[\alpha]$, is a field, whence $k[\alpha] = k(\alpha)$ by Lemma 1.14.4. Since a k-algebra isomorphism is a-fortiori a k-vector space isomorphism it maps a basis to a basis. The result follows from Proposition 1.14.10 as the basis thus defined is the image of the basis in the proposition under the specified isomorphism. □

We may show the following

Proposition 1.14.12 (Finitely generated by algebraic $\implies$ finite and algebraic)
Let $K = k(\alpha_1, \ldots, \alpha_n)/k$ be a field extension such that α_i is algebraic. Then K/k is a finite algebraic extension.

In particular a finitely-generated algebraic extension is finite.

Proof. We write $K_i = k(\alpha_1, \ldots, \alpha_i)$. Then we have a tower

$$K = K_n/\ldots/K_0 = k$$

such that $K_i = K_{i-1}(\alpha_i)$ is a simple algebraic extension. By Proposition 1.14.11 K_i/K_{i-1} is finite. Therefore by Corollary 1.14.2 K/k is finite. By Proposition 1.14.7 it's also algebraic. □

The following is useful for reducing to cases of finite extensions where counting arguments work.

Lemma 1.14.13 (Reduce to finite extensions)
Let K/k be a field extension and $E \subset K$ algebraic over k. For every $\alpha \in K$ algebraic over E, there is some subfield $E_0 \subset E$ such that

- *E_0/k is finite*
- *α is algebraic over E_0*
- *$m_{\alpha,E} = m_{\alpha,E_0}$*

Furthermore α is algebraic over k and $m_{\alpha,E_0} \mid m_{\alpha,k}^{i_{kK}}$.

Proof. Suppose

$$m_{\alpha,E}(X) = a_0 + a_1 X + \ldots a_n X^n$$

Then define $E_0 = k(a_0, \ldots, a_n)$. By Proposition 1.14.12 E_0/k is finite. Clearly α is algebraic over E_0 as it is a root of $m_{\alpha,E}$. By Proposition 1.14.9 $m_{\alpha,E_0} \mid m_{\alpha,E}$ as elements of $E_0[X]$ and $m_{\alpha,E} \mid m_{\alpha,E_0}$. Therefore $m_{\alpha,E_0} = m_{\alpha,E}$.

By Proposition 1.14.11 $E_0(\alpha)/E$ is finite, therefore $E_0(\alpha)/k$ is finite. By Proposition 1.14.7 $E_0(\alpha)/k$ is algebraic, whence α is algebraic over k. The last statement follows from Proposition 1.14.9 again. □

Corollary 1.14.14
K/E and E/k are both algebraic if and only if K/k is.

Proof. One direction is obvious. The converse follows from the previous result. □

We may prove the first lifting theorem

Proposition 1.14.15 (Lifting to simple extensions)
Let $k(\alpha)/k$ be a simple algebraic extension and L/k a field extension such that $m_{\alpha,k}$ has a root in L. Then there exists a morphism $\sigma : k(\alpha)/k \to L/k$.

More precisely there is a bijective mapping

$$\mathrm{Mor}_k(k(\alpha), L) \longrightarrow \{\beta \in L \mid m_{\alpha,k}(\beta) = 0\}$$

where

$$\sigma \to \sigma(\alpha)$$

and $\sigma(k(\alpha)) = k(\sigma(\alpha))$*. In particular if* $m_{\alpha,k}$ *is separable and splits completely in* L *then there are precisely* $\deg(m_\alpha) \overset{1.14.11}{=} [k(\alpha) : k]$ *such extensions.*

Proof. Observe $m_{\alpha,k}(\sigma(\alpha)) \overset{1.14.3}{=} \sigma(m_{\alpha,k}(\alpha)) = 0$. Therefore the mapping is well-defined. By Proposition 1.14.6 it is injective. We claim it is also surjective. By Proposition 1.14.11 there is a k-algebra isomorphism

$$k[X]/(m_{\alpha,k}) \longrightarrow k(\alpha)$$

Similarly for $\beta \in T$ there is a k-algebra isomorphism

$$k[X]/(m_{\beta,k}) \longrightarrow k(\beta)$$

We are done if $m_{\alpha,k} = m_{\beta,k}$. But $m_{\alpha,k}$ is monic, irreducible and has β as a root. So this follows from uniqueness of the minimal polynomial in Proposition 1.14.9. The final statement follows from Corollary 1.9.13 □

1.14.2 Galois Theory Summary

Definition 1.14.10 (Separable, Normal and Galois)
Let K/k *be an algebraic extension. We say that* K/k *is*

- Normal *if every minimal polynomial* $m_{\alpha,k} \in k[X]$ *splits completely in* K
- Separable *if every minimal polynomial* $m_{\alpha,k} \in k[X]$ *is separable.*
- Galois *if it is both normal and separable (iff* $m_{\alpha,k}$ *has* $\deg(m_{\alpha,k})$ *distinct roots in* K*, see Proposition 1.9.13).*

In the case of a Galois extension we denote the group of automorphisms by $\mathrm{Gal}(K/k)$.

To summarize the main results

1. The group of automorphism of a normal extension K/k acts transitively on the roots of a given irreducible polynomial.
2. For K/k finite we have $\#\operatorname{Aut}(K/k) \leq [K : k]$ with equality if and only if K/k is Galois.
3. An algebraic extension K/k is automatically separable whenever either $\mathrm{char}(k) = 0$ or k is finite.
4. When K/k is finite and Galois then we have an order-reversing bijection between subfields and subgroups

$$\begin{aligned} \{H \leq \mathrm{Gal}(K/k)\} &\longleftrightarrow \{F \subseteq K\} \\ \phi : H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \psi : \mathrm{Gal}(K/F) &\longleftarrow F \end{aligned}$$

We follow the approach in Lang72 and rephrase the concepts of "Normal" and "Separable" in terms of morphisms into an algebraic closure, i.e. the set $\mathrm{Mor}_k(K, \bar{k})$. The first requires some work to set up the algebraic closure $\bar{k}$.

1.14.3 Algebraic Closure

Proposition 1.14.16 (Algebraically Closed)
A field M *is algebraically closed if one of the following equivalent conditions holds*

- *Every algebraic extension* M'/M *is trivial*
- *Every non-constant polynomial in* $M[X]$ *has a root in* M
- *Every non-constant polynomial in* $M[X]$ *splits in* M

If M *is an extension field of* k*, then we say it is algebraically closed over* k.

Definition 1.14.11 (Algebraic Closure)
An algebraic closure $\bar{k}$ *of* k *is a field extension* $\bar{k}/k$ *which is algebraic and for which* $\bar{k}$ *is algebraically closed.*

Proposition 1.14.17 (Existence of Algebraic Closure)
Given a field k *there exists an algebraic closure* $\bar{k}/k$

Proposition 1.14.18 (Generic Lifting Theorem)
Let K/k *be a field extension. Suppose* L/K *is an algebraic extension and* $\sigma : K \to M$ *a* k*-embedding into an algebraically closed field. Then there exists an extension* $\tilde{\sigma} : L \to M$*. In other words there is a surjection*

$$\mathrm{Mor}_k(i_{KL}, M) : \mathrm{Mor}_k(L, M) \to \mathrm{Mor}_k(K, M)$$

Proof. Broadly speaking consider the poset of extensions to subfields of L ordered under consistency and take a maximal element by Zorn's Lemma. Apply Proposition 1.14.15 to show that this maximal element must be an extension to L.

If $[L : K] < \infty$, then we may simply proceed by induction on dimension. □

Corollary 1.14.19 (Unique up to isomorphism)
An algebraic closure $\bar{k}$ of k is unique up to (non-unique) isomorphism.

Remark 1.14.12
Note if K/k is an algebraic extension then the Proposition shows that we may consider construct an embedding $K \to \bar{k}$ commuting with $k \to \bar{k}$.

In general given a tower of algebraic extensions

$$K = k_n/\ldots/k_0 = k$$

we will assume the existence of compatible embeddings $i_{k_i} : k_i \to \bar{k}$ such that $i_{k_{i+1}} \circ i_{k_i,k_{i+1}} = i_{k_i}$.

1.14.4 Separability

We follow Lang and not only characterize separability but define a "separability degree" which equals the extension degree if and only if it's separable. The proofs are somewhat technical, especially in light of the fact most base fields will be perfect.

Definition 1.14.13 (Separable element)
We say $\alpha \in K/k$ is separable over k if $m_{\alpha,k}(X)$ is a separable polynomial.

We say K/k is separable if every $\alpha \in K$ is separable.

Lemma 1.14.20
$\alpha \in K/k$ is separable if and only if it is a root of a separable polynomial in $k[X]$.

In particular α separable over k implies it is separable over any subfield $E \subset K$.

Proof. One direction is obvious. Conversely suppose $f(\alpha) = 0$ with f separable. Then $m_{\alpha,k} \mid f$ so the result follows from Proposition 1.9.12. □

The main results of this section are the following

Proposition 1.14.21 (Separability Degree)
Let K/k be a finite extension and define the separability degree $[K : k]_s$ as

$$[K : k]_s = \#\operatorname{Mor}_k(K, \bar{k})$$

1. *It is independent of the choice of embedding into $\bar{k}$*
2. *It is multiplicative in the sense that*

$$[K : k]_s = [K : F]_s[F : k]_s$$

3. *$[K : k]_s \leq [K : k]$ with equality if and only if K/k is separable*

Proposition 1.14.22
Consider a tower of algebraic extensions $K/E/k$. Then K/E and E/k is separable iff K/k is.

Proof. K/k separable $\implies$ K/E and E/k separable follows from Lemma 1.14.20.

Conversely the finite case follows from Proposition 1.14.21 by multiplicativity. We delay the proof of the general case until later in the section, as we don't need it for subsequent results. □

Proposition 1.14.23
An algebraic extension $K = k(\alpha_1, \ldots, \alpha_n)/k$ is separable iff α_i are.

Proposition 1.14.24 (Equivalent definition of separability)
An algebraic extension K/k. TFAE

1. *K/k is separable*
2. *E/k is separable for every finite sub-extension*
3. *$[E : k]_s = [E : k]$ for every finite sub-extension*

NB 3) is Lang's definition of separability which makes it a lot easier to prove certain results.
First we prove a key lemma regarding simple extension

Lemma 1.14.25 (Separability degree of simple extension)
If $k(\alpha)/k$ is a simple extension then

$$[k(\alpha):k]_s = \#\{ \text{ roots of } m_\alpha \text{ in } \bar{k}\} \leq \deg(m_\alpha) = [k(\alpha):k]$$

Furthermore equality holds iff α is separable over k.

Proof. The first equality follows from 1.14.15, the final equality from Proposition 1.14.11. The inequality follows from Corollary 1.9.9. The final statement follows from Corollary 1.9.13. □

Proof. Proof of 1.14.21
Note that any two algebraic closures $\bar{k}/k$ and $\bar{k}'/k$ are k-isomorphic by (...). Since $\mathrm{Mor}(K,-)$ is a covariant functor (1.2.6) we see that implies $\mathrm{Mor}(K,\bar{k})$ is isomorphic to $\mathrm{Mor}(K,\bar{k}')$ as a set by 1.2.1. This shows that $[K:k]_s$ is well-defined.

For a tower $K/F/k$ consider the restriction map

$$\psi := \mathrm{Mor}_k(i_{FK},\bar{k}) : \mathrm{Mor}_k(K,\bar{k}) \to \mathrm{Mor}_k(F,\bar{k})$$

It is surjective by Proposition 1.14.18. Consider $\sigma \in \mathrm{Mor}_k(F,\bar{k})$ then the fibre $\psi^{-1}(\sigma)$ is equal to $\mathrm{Mor}_F(K,(\bar{k},\sigma))$. As we've noted already the order does not depend on the embedding σ and $\#\psi^{-1}(\sigma) = [K:F]_s$ for all σ. As $\mathrm{Mor}_k(K,\bar{k})$ is equal to the disjoint union of all the fibres, then the multiplicativity result follows.

It's possible to decompose K/k as a tower of simple extensions

$$K = K_n/\ldots/K_0 = k$$

with $K_i = K_{i-1}(\alpha_i)$. By Lemma 1.14.25 we have

$$[K_i:K_{i-1}]_s \leq [K_i:K_{i-1}]$$

with equality iff α_i separable over K_{i-1}. By multiplicativity the inequality follows.

If K/k is separable then by Lemma 1.14.20 α_i is separable over K_{i-1} and we have $[K_i:K_{i-1}]_s = [K_i:K_{i-1}]$ and $[K:k]_s = [K:k]$ by multiplicativity. Conversely if $[K:k]_s = [K:k]$ then $[K_i:K_{i-1}]_s = [K_i:K_{i-1}]$ and α_i is separable over K_{i-1}. Since the choice of α_1 was arbitrary we see that K/k is separable. □

Proof. Proof of 1.14.23
Let $K = k(\alpha_1,\ldots,\alpha_n)$. Then we may construct a tower of finite (simple) extensions

$$K = K_n/\ldots/K_0 = k$$

with $K_i = k(\alpha_1,\ldots,\alpha_i)$ and $K_i = K_{i-1}(\alpha_i)$. By Lemma 1.14.20 α_i is separable over K_{i-1}. Therefore $[K_i:K_{i-1}]_s = [K_i:K_{i-1}]$ by Lemma 1.14.25 and $[K:k]_s = [K:k]$ by multiplicativity. Proposition 1.14.21 shows that K/k is separable. □

Proof. Proof of 1.14.22 general case

Assume K/E and E/k are separable. Take $\alpha \in K$. Then Lemma 1.14.13 shows the existence of a finite sub-extension E_0/k of E such that $m_{\alpha,E} = m_{\alpha,E_0}$. Therefore α is separable over E_0. By Lemma 1.14.25 we see that $[E_0(\alpha):E_0]_s = [E_0(\alpha):E_0]$. We've seen from the finite case that E_0/k is separable so by Proposition 1.14.21 $[E_0:k]_s = [E_0:k]$. By multiplicativity $[E_0(\alpha):k]_s = [E_0(\alpha):k]$ and the same result again shows that $E_0(\alpha)/k$ is separable. In particular α is separable over k as required. □

Proof. Proof of 1.14.24 1 $\implies$ 2) is trivial and 2 $\iff$ 3 follows from Proposition 1.14.21. We need only show 2 $\implies$ 1.

Consider $\alpha \in K$. Then by Lemma 1.14.13 there exists a finite sub-extension E/k such that α is algebraic over E. Therefore $E(\alpha)/k$ is finite, and by assumption $E(\alpha)/k$ separable as required. □

1.14.5 Applications of Separability

Definition 1.14.14 (Bounds on $\mathrm{Aut}(K/k)$)
Let K/k be an algebraic extension and $i_K : K \to \bar{k}$ a fixed k-embedding. Then there is a natural injection

$$\begin{aligned} \mathrm{Mor}_k(K,i_K) : \mathrm{Aut}(K/k) &\to \mathrm{Mor}_k(K,\bar{k}) \\ \sigma &\to i_K \circ \sigma \end{aligned}$$

In particular in the finite case

$$\#\,\mathrm{Aut}(K/k) \leq [K:k]_s \leq [K:k] < \infty$$

If i_K is inclusion, then we may regard $\mathrm{Aut}(K/k)$ as a subset of $\mathrm{Mor}_k(K,\bar{k})$

Corollary 1.14.26 (Extension to algebraic closure II)
Let K/k be an algebraic extension and $i_K : K \to \bar{k}$ a k-embedding. Then every $\sigma : K \to \bar{k}$ lifts to $\sigma : \bar{k} \to \bar{k}$. i.e. there is a canonical surjection by restriction

$$\begin{aligned} \mathrm{Mor}_k(i_K, \bar{k}) : \mathrm{Aut}(\bar{k}/k) &\longrightarrow \mathrm{Mor}_k(K, \bar{k}) \\ \sigma &\longrightarrow \sigma \circ i_K \end{aligned}$$

When i is inclusion then this is simply the restriction to K.

Proof. Given $\sigma \in \mathrm{Mor}_k(K, \bar{k})$ there exists an extension $\tilde{\sigma} \in \mathrm{Mor}_k(\bar{k}, \bar{k})$ by Proposition 1.14.18 with $L = M = \bar{k}$. This is automatically an automorphism by Proposition 1.14.8 as required.

□

Corollary 1.14.27 (Conjugate elements)
We say $\alpha, \beta \in \bar{k}$ are conjugate if they have the same minimal polynomial.
This is the case if and only if there is an element $\sigma \in \mathrm{Aut}(\bar{k}/k)$ such that $\sigma(\alpha) = \beta$.

Proof. By Proposition 1.14.15 there is an isomorphism $k(\alpha) \to k(\beta)$. Corollary 1.14.26 gives the required automorphism. The converse is easy. □

As an application of the concept of separability degree we prove

Proposition 1.14.28 (Primitive Element Theorem)
Let K/k be a finite separable extension of k then $K = k(\alpha)$ is simple.

Proof. We only prove the case k is infinite. The finite case can be proven separately by showing that the $K^\star$ is cyclic.

Consider the set $\mathrm{Mor}_k(K, \bar{k}) = \{\sigma_1, \ldots, \sigma_n\}$ which by Proposition **??** has order $n = [K : k]$. By induction we can assume that $K = k(\alpha, \beta)$. We claim that there exists $0 \neq c \in k$ such that $\sigma_i(\alpha + c\beta)$ are all distinct. In this case we clearly have $\#\,\mathrm{Mor}_k(k(\alpha + c\beta), \bar{k}) \geq n$ so by the same result $[k(\alpha + c\beta) : k] \geq n$ whence $k(\alpha + c\beta) = K$.

We have $\sigma_i(\alpha + c\beta) = \sigma_j(\alpha + c\beta) \iff c(\sigma_i(\beta) - \sigma_j(\beta)) = (\sigma_i(\alpha) - \sigma_j(\alpha))$. Therefore consider the polynomial

$$f(X) = \prod_{i \neq j} (X(\sigma_i(\beta) - \sigma_j(\beta)) - (\sigma_i(\alpha) - \sigma_j(\alpha)))$$

Then the embeddings are distinct precisely when $f(c) \neq 0$. Since $f(X)$ has at most finitely many roots and k is infinite, there must exist such a c. □

1.14.6 Perfect Fields

For large classes of base fields all algebraic extensions are separable :

Proposition 1.14.29 (Perfect field)
Let k be a field. Then TFAE

- *Every irreducible polynomial in $k[X]$ is separable*
- *Every algebraic extension K/k is separable*
- *$\bar{k}$ is separable*

In this case we say k is perfect.

Proposition 1.14.30 (Criteria for perfectness)
k is perfect if and only if one of the following holds

- *k has characteristic 0*
- *k has characteristic p and every element is a p-th power*

In particular finite fields are perfect.

1.14.7 Normal Extensions

We characterize normal extensions in terms of morphisms $\mathrm{Mor}_k(K, \bar{k})$.

Proposition 1.14.31 (Normal Criteria)
Let K/k be an algebraic extension and $\bar{k}$ a given algebraic closure, then the following are equivalent

NOR1 *For any two k-embeddings $\sigma, \tau \in \mathrm{Mor}_k(K, \bar{k})$ we have $\sigma(K) = \tau(K)$.*

NOR2 *K is the splitting field of some family of polynomials $f_i \in k[X]$.*

NOR3 *K/k is normal (i.e. every minimal polynomial in $k[X]$ splits completely in K)*

Proof. Clearly 3 $\implies$ 2, for K is the splitting field of all the minimal polynomials of elements in K.

We show 2 $\implies$ 1. Define $T_j = \{\alpha \in K \mid f_j(\alpha) = 0\}$ and $T_j' = \{\alpha \in \bar{k} \mid f_j(\alpha) = 0\}$. By hypothesis $K = k(\cup_j T_j)$.

It's clear that any σ induces a bijection between T_j and T_j'. In particular $\sigma(\cup_j T_j) = \cup_j T_j'$. By Lemma 1.14.5 we have $\sigma(K) = k(\cup_j T_j')$. In particular any two embeddings σ, τ have the same image.

Finally we show 1 $\implies$ 3. Suppose $f(X)$ is an irreducible polynomial with roots $\alpha_1', \ldots, \alpha_n' \in \bar{k}$ and $\alpha_1 \in K$ such that $i_K(\alpha_1) = \alpha_1'$. By Corollary 1.14.27 there is a morphism $\phi \in \mathrm{Aut}(\bar{k}/k)$ such that $\phi(\alpha_1) = \alpha_j$. By hypothesis i_K and the composite map $\phi \circ i_K$ must have the same image, K. Therefore $\alpha_j \in K$ as required. □

We provide some more straight-forward criteria based on a specific embedding $K \subset \bar{k}$.

Proposition 1.14.32 (Normal Criteria II)
Let K/k be an algebraic extension and $i_K : K \to \bar{k}$ a given k-embedding then the following are equivalent

1. *K/k is normal*
2. *Every $\sigma \in \mathrm{Mor}_k(K, \bar{k})$ has image $i_K(K)$*
3. *The embedding $\mathrm{Mor}_k(K, i_K) : \mathrm{Aut}(K/k) \to \mathrm{Mor}_k(K, \bar{k})$ (1.14.14) is a bijection*

When K/k is finite it's necessary and sufficient that $\#\,\mathrm{Aut}(K/k) = [K : k]_s$

Proof. 1 $\iff$ 2). This is clear by NOR1.

2 $\implies$ 3). Given $\sigma \in \mathrm{Mor}_k(K, \bar{k})$, by hypothesis it has image $i_K(K)$, so we may define $\tau(x) = i_K^{-1}(\sigma(x))$ and $\tau \in \mathrm{Aut}(K/k)$.

3 $\implies$ 2). Conversely given $\sigma \in \mathrm{Mor}_k(K, \bar{k})$, by hypothesis $\sigma = i_K \circ \tau$, and so has image $i_K(K)$.

For the final statement if K/k is finite, then we've shown in Proposition 1.14.21 that $[K : k]_s < \infty$. So the embedding $\mathrm{Mor}_k(K, i_K)$ is bijective if and only if $\#\,\mathrm{Aut}(K/k) = \#\,\mathrm{Mor}_K(K, \bar{k}) = [K : k]_s$ as required. □

Corollary 1.14.33 (Galois Criteria)
Let K/k be a finite extension. Then

$$\#\,\mathrm{Aut}\,K/k \leq [K : k]_s \leq [K : k]$$

with equalities if and only if K/k is Galois.

Proof. We've seen the inequalities (Definition 1.14.14)

$$\#\,\mathrm{Aut}(K/k) \leq [K : k]_s \leq [K : k] < \infty$$

with equality if and only if K/k is both normal (Proposition 1.14.32) and separable (Proposition 1.14.21) □

Corollary 1.14.34 (Subfield is Normal)
Let K/k be a normal extension and $F \subset K$ a subfield, then K/F is normal.

Proof. We assume the tower F/k has compatible embeddings into $\bar{k}$, then we have

$$\mathrm{Mor}_F(K, \bar{k}) \subset \mathrm{Mor}_k(K, \bar{k})$$

and the result follows from NOR1 . □

Proposition 1.14.35 (Automorphisms of Normal Extension)
Let K/k be a normal extension with compatible embeddings in $\bar{k}$. There is a canonical isomorphism of groups

$$\begin{aligned} \mathrm{Aut}(\bar{k}/k)/\,\mathrm{Aut}(\bar{k}/K) &\to \mathrm{Aut}(K/k)\,. \\ \sigma &\to i_K^{-1} \circ \sigma \circ i_K \end{aligned}$$

When $K \subset \bar{k}$ then this map is simply restriction to K.

Proof. By NOR1 $(\sigma \circ i_K)(K) = i_K(K)$ so that the mapping is well-defined. We verify that the image of σ indeed fixes k :

$$\left(i_K^{-1} \circ \sigma \circ i_K\right) \circ i_{kK} = i_K^{-1} \circ \sigma \circ i_k = i_K^{-1} \circ i_k = i_K^{-1} \circ i_K \circ i_{kK} = i_{kK}$$

as required. Given any $\hat{\sigma} \in \mathrm{Aut}(K/k)$ there is by Corollary 1.14.26 there is $\sigma \in \mathrm{Aut}(\bar{k}/k)$ such that $i_K \circ \hat{\sigma} = \sigma \circ i_K$. Clearly the image of $\hat{\sigma}$ under this mapping is σ as required.

For the final statement note that $i_K^{-1} \circ \sigma \circ i_K = \mathrm{id} \iff \sigma \circ i_K = i_K \iff \sigma$ fixes K. □

In fact we can replace $\bar{k}$ with a normal overfield and obtain results corresponding to Corollary 1.14.26 and Proposition 1.14.32 respectively. Due to the explicit embeddings in $\bar{k}$ the arguments become slightly awkward.

Corollary 1.14.36 (Extension to normal overfield)
Let L/k be a normal extension such that $K \subset L$ then there is a canonical surjective monoid morphism

$$\mathrm{Aut}(L/k) \to \mathrm{Mor}_k(K, L)$$

by restriction. The kernel is $\mathrm{Aut}(L/K)$.

Proof. Assume an embedding $i_L : L \to \bar{k}$.
Consider $\sigma \in \mathrm{Mor}_k(K, L)$, then by Corollary 1.14.26 there exists an extension $\tilde{\sigma} \in \mathrm{Aut}(\bar{k}/k)$ such that $i_L \circ \sigma = \tilde{\sigma} \circ i_K$. As in the previous Proposition there exists $\hat{\sigma} \in \mathrm{Aut}(L/k)$ such that $\tilde{\sigma} \circ i_L = i_L \circ \hat{\sigma}$. Therefore $i_L \circ \sigma = i_L \circ \hat{\sigma}|_K$ which implies $\sigma = \hat{\sigma}|_K$ as required.

□

Corollary 1.14.37 (Automorphisms of Normal subextension)
Let L/k be a normal extension and $K \subset L$, then the following are equivalent

1. *K/k is normal*
2. *$\mathrm{Mor}_k(K, L) = \mathrm{Aut}(K/k)$, i.e. every k-embedding $\sigma : K \to L$ has $\sigma(K) = K$.*
3. *For every $\sigma \in \mathrm{Aut}(L/k)$ we have $\sigma(K) = K$*

In this case $\mathrm{Aut}(L/K) \triangleleft \mathrm{Aut}(L/k)$ is normal and we have a canonical group isomorphism

$$\mathrm{Aut}(L/k)/\mathrm{Aut}(L/K) \to \mathrm{Aut}(K/k)$$

Proof. 1 $\implies$ 2). Given $\sigma \in \mathrm{Mor}_k(K, L)$, then by definition we have $(i_L \circ \sigma)(K) = (i_L)(K)$, which means $\sigma(K) = K$
2 $\implies$ 1). Given any $\sigma \in \mathrm{Mor}_k(K, \bar{k})$, this extends to $\tilde{\sigma} \in \mathrm{Mor}_k(L, \bar{k})$ by hypothesis. Since L is normal $\tilde{\sigma}(L) = i_L(L)$, we see $\hat{\sigma} := i_L^{-1} \circ \tilde{\sigma} \in \mathrm{Aut}(L/k)$. By hypothesis $\hat{\sigma}(K) = K$. Furthermore $\sigma(K) = \tilde{\sigma}(K) = i_L(\hat{\sigma}(K)) = i_L(K)$. Since σ is arbitrary then it shows K is normal.
2 $\implies$ 3). This is clear
3 $\implies$ 2). Given $\sigma \in \mathrm{Mor}_k(K, L)$ by the previous Corollary we can extend to $\mathrm{Aut}(L/k)$ and the result follows easily. By the previous corollary the canonical map given is surjective, which yields the isomorphism. □

The following is straight-forward

Corollary 1.14.38 (Conjugate Elements)
Let K/k be a normal extension and two elements $\alpha, \beta \in K$ be two elements with the same minimal polynomial. Then there exists $\sigma \in \mathrm{Aut}(K/k)$ such that $\sigma(\alpha) = \beta$.

Proof. By Proposition 1.14.15 there is an isomorphism $k(\alpha) \to k(\beta)$. Corollary 1.14.36 gives the required extension. □

1.14.8 Finite Fields

A finite field K necessarily has positive characteristic p, and therefore the prime subfield is isomorphic to the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. We list some necessary properties of a finite field

Proposition 1.14.39 (Properties of finite fields)
Every finite field K is a finite-dimensional vector space over its prime subfield $\mathbb{F}_p$. Define $n = [K : \mathbb{F}_p]$.

- $\#K = p^n$
- *K is a splitting field for $X^{p^n} - X \in \mathbb{F}_p[X]$, and indeed is equal to the set of roots*
- *The multiplicative group of units $K^\star$ is cyclic.*
- *$K/\mathbb{F}_p$ is simple*

Proof. Since $K/\mathbb{F}_p$ is a finite-dimensional vector space it must have order p^n.

The group of units has order $p^n - 1$, so by Lagrange's theorem every non-zero element satisfies $X^{p^n-1} - 1 = 0$, so therefore every element satisfies $X^{p^n} - X = 0$. Since this polynomial can have at most p^n roots it shows that the roots are exactly all the elements of K.

We note that $X^d - 1$ as at most d roots by Corollary 1.9.9. Therefore the fact $K^\star$ is cyclic follows from Proposition 1.2.8. □

Proposition 1.14.40 (Frobenius morphism)
Given any field $K/\mathbb{F}_p$ the Frobenius map

$$\phi : x \to x^p$$

is an injective field homomorphism. In particular when K is finite it is an automorphism over $\mathbb{F}_p$.

Proof. The only non-trivial step is showing

$$(x + y)^p = x^p + y^p$$

which follows from elementary calculations on binomial coefficients. □

Further we can show existence and uniqueness of finite fields.

Proposition 1.14.41 (Existence and uniqueness of finite fields)
Consider the algebraic closure $\overline{\mathbb{F}_p}$ and let $\mathbb{F}_{p^n}$ denote the splitting field of $f(X) = X^{p^n} - X$ in $\overline{\mathbb{F}_p}$. Then

- *$\mathbb{F}_{p^n}$ is equal to the set of roots of $X^{p^n} - X$*
- *It is the unique subfield of order p^n and every finite field of order p^n is isomorphic to this.*
- *$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m \mid n$*

Proof. By the previous Proposition the set of roots of $f(X)$ forms a subfield of $\overline{\mathbb{F}_p}$.

Furthermore $f'(X) = -1$ so $f(X)$ is separable because clearly $(f, f') = 1$. Therefore by Proposition 1.9.13 $f(X)$ has p^n distinct roots and the splitting field of $f(X)$ is exactly the set of roots.

Furthermore every subfield of order p^n must satisfy this polynomial by Lagrange's Theorem 1.2.4, so it is the unique such subfield.

Since every algebraic extension of $\mathbb{F}_p$ is isomorphic to a subfield of $\overline{\mathbb{F}_p}$ it's also the unique algebraic extension of order p^n up to isomorphism.

Clearly if $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ we see that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p]$, so we must have $m \mid n$. Conversely if $\alpha \in \mathbb{F}_{p^m}$ then $\alpha^{p^m} = \alpha \implies \alpha^{p^{rm}} = \alpha$ for all $r > 0$, so $\alpha \in \mathbb{F}_{p^n}$. □

It is usually most convenient to work in $\overline{\mathbb{F}_p}$ and consider the finite fields of the form $\mathbb{F}_{p^n}$ as in the Proposition. We've seen in Proposition 1.14.30 that every finite field $\mathbb{F}_q := \mathbb{F}_{p^n}$ is perfect and therefore every algebraic extension is separable. In fact we may show that every finite extension is Galois.

Proposition 1.14.42
The field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle$$

cyclic of order n generated by the Frobenius automorphism.

Proof. Let $G = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. We've observed that $\phi \in G$. Let $d = o(\phi)$, and we wish to prove that $n = d$. Certainly by Lagrange's theorem $\phi^n = 1$, whence d divides n. By definition of ϕ every $\alpha \in \mathbb{F}_{p^n}$ satisfies $X^{p^d} - X = 0$. This has at most p^d roots sp we must have $d \geq n$, and therefore $d = n$. Clearly ϕ generates a cyclic subgroup of order n. However by Corollary 1.14.33 G has at most order n, whence $G = \langle \phi \rangle$ as required. Furthermore by the same result $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois. □

Proposition 1.14.43 (Subfields of $\mathbb{F}_{p^n}$)
Consider the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. Then it has a unique subfield of order p^m if and only if $m \mid n$. In this case $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois and

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \phi^m \rangle$$

and in particular has order n/m.

Proof. We've already shown that $\mathbb{F}_{p^n}$ has a unique subfield of order p^m, by assuming an embedding in $\overline{\mathbb{F}_p}$. Let $H = \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$. Note ϕ^m has order n/m and clearly is in H, so $\#H \geq n/m$. By Corollary 1.14.33 $\#H \leq [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$, whence we have equality and the extension is Galois generated by ϕ^m. □

1.14.9 Galois Theory

We've seen that for K/k a finite extension

$$\#\operatorname{Aut}(K/k) \leq [K:k]_s \leq [K:k]$$

with equality if and only if K/k is Galois, by Corollary 1.14.33.

Remark 1.14.15
If k is perfect then $\bar{k}/k$ is Galois.

The main result of Galois Theory is that in the finite case there is an order-reversing bijection between subgroups and subfields

$$\begin{aligned} \{H \leq \operatorname{Gal}(K/k)\} &\longleftrightarrow \{F \subseteq K\} \\ \phi : H &\longrightarrow K^H := \{x \in K \mid h(x) = x \quad \forall h \in H\} \\ \psi : \operatorname{Gal}(K/F) &\longleftarrow F \end{aligned}$$

Such an order reversing map is usually called an (antitone) Galois connection, as the first such type arose from Galois Theory. Note it is well-defined because of the following proposition.

Proposition 1.14.44
If K/k is Galois and $F \subset K$ then K/F is Galois.

Proof. This follows from Corollary 1.14.34 and Proposition 1.14.22. □

We need to show that $\phi \circ \psi = \mathrm{id}$ and $\psi \circ \phi = \mathrm{id}$. The first is marginally easier, and follows purely from the definition of Galois without making any finiteness assumptions.

Proposition 1.14.45 (Fixed field of Galois group)
If K/k is Galois and $F \subset K$ then

$$K^{\mathrm{Gal(K/F)}} = F$$

or in other words $\phi \circ \psi = \mathrm{id}$, and in particular ϕ is injective.

Proof. Clearly $F \subseteq K^{\mathrm{Gal(K/F)}}$. Conversely given $\alpha \in K \setminus F$, then $\deg m_{\alpha,F} > 1$. Since α is separable it must have another root $\beta \in K$. By Corollary 1.14.38 there is an element $\sigma \in \operatorname{Gal}(K/F)$ such that $\sigma(\alpha) = \beta$. In other words $\alpha \notin K^{\mathrm{Gal}(K/F)}$, which shows the reverse inclusion. □

Proposition 1.14.46
Let K/k be a field extension and $H \subseteq \operatorname{Aut}(K/k)$ a finite subgroup then K/K^H is finite Galois with

$$H = \operatorname{Gal}(K/K^H)$$

and order equal to $[K:K^H]$. In particular for a finite Galois Extension K/k we have $\psi \circ \phi = \mathrm{id}$.

Proof. Firstly observe that trivially $H \subseteq \operatorname{Aut}(K/K^H)$. If we know that $[K:K^H] < \infty$, then by Corollary 1.14.33 we have

$$\#H \leq \#\operatorname{Aut}(K/K^H) \leq [K:K^H]_s \leq [K:K^H]$$

We can prove equality everywhere if we show that $[K:K^H] \leq \#H$, which is shown either by Lemma 1.14.47 or Lemma 1.14.48. Note equality also shows that K/K^H is finite Galois by the same result.

□

We present two approaches to showing the inequality $[K:K^H] \leq \#H$. The first uses independence of characters style argument (see Garling, JMilne), and the second which is more straightforward uses the action of H to show that every element has degree at most $\#H$ (Artin).

Lemma 1.14.47 (Bound degree of fixed field I)
Let K/k be a field extension and $H \subset \operatorname{Aut}(K/k)$ a finite subgroup. Then $[K:K^H] \leq \#H$

Proof. Let $H = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}$ and $\alpha_1, \ldots, \alpha_m$ a K^H-basis for K.

Consider the vector space K^n and the elements $\hat{\alpha}_j = (\sigma_1(\alpha_j), \ldots, \sigma_n(\alpha_j))$ for $j = 1 \ldots m$. It's enough to show that these are linearly independent over K, as that shows $m \leq n$.

Let $S(K) := \{v \in K^m \mid \sum_{j=1}^m v_j \hat{\alpha}_j = 0\}$, we aim to show that $S(K) = \{0\}$. If we also consider $S(K^H)$, any non-zero elements will be a K^H linear-dependence for $\alpha_1, \ldots, \alpha_m$ by considering the first component ($\sigma_1 = \mathrm{id}$). Therefore by assumption $S(K^H) = \{0\}$. Finally we see it's enough to show that $S(K) \neq \{0\} \implies S(K^H) \neq \{0\}$.

First observe that $K^\star$ and H both act on $S(K)$. The first by scaling and the second component-wise. This is well-defined because $v \in S(K)$ if and only if

$$\sum_j v_j \sigma(\alpha_j) = 0 \quad \forall \sigma \in H\,.$$

Apply τ to obtain

$$\sum_j \tau(v_j)(\tau \circ \sigma)(\alpha_j) = 0 \quad \forall \sigma \in H$$

and since multiplication by τ permutes H we see $\tau(v) \in S(K)$ as required.

If there exists $0 \neq v \in S(K)$, consider v with a minimal number of non-zero components. By scaling we can assume λv has at least one component in K^H. The vector $\tau(\lambda v) - \lambda v$ then has at least one fewer non-zero components, so by minimality must be zero. Since τ was arbitrary we see $0 \neq \lambda v \in S(K^H)$ as required.

□

Lemma 1.14.48 (Bound degree of fixed field II)
Let K/k be a field extension and H a finite subgroup of $\mathrm{Aut}(K/k)$. *Then K/K^H is finite separable, and simple, with* $[K : K^H] \leq \#H$

Proof. We show that K/K^H is separable and every element has degree at most $\#H$. For any $\alpha \in K$, consider the orbit $H(\alpha) = \{\sigma(\alpha) \mid \sigma \in H\}$, which is of order at most $\#H$. Then the polynomial

$$f(X) = \prod_{\beta \in H(\alpha)} (X - \beta)$$

has α as a root and is separable by Proposition 1.9.13. Furthermore $f^\tau = f$ because τ permutes $H(\alpha)$ (it's injective and hence bijective). Therefore $f \in K^H[X]$ and $m_{\alpha,K^H} \mid f$. We see that α has degree at most $\#H$ and is separable by Proposition 1.9.12.

If K/k is finite, then a-fortiori K/K^H is finite, so we may apply the Primitive Element Theorem 1.14.28 directly to show the result.

More generally let $K^H(\alpha)$ be a simple subfield of K of maximal degree. This exists because the degree of α is bounded above by $\#H$. We claim $K^H(\alpha) = K$, for if not then $K^H \subseteq K^H(\alpha) \subsetneq K^H(\alpha, \beta)$ is a finite separable extension of K^H, whence it must be simple by the Primitive Element Theorem 1.14.28, contradicting maximality. Finally the degree of $[K : K^H]$ is the degree of α, which we've seen is bounded above by $\#H$. □

Now we may demonstrate straightforward criteria for subfield to be normal

Proposition 1.14.49
Let K/k be a finite Galois extension and $F \subset K$ a subfield.
Then F/k is Galois if and only if $\mathrm{Gal}(K/F) \triangleleft \mathrm{Gal}(K/k)$ *is normal. In this case we have a canonical isomorphism*

$$\mathrm{Gal}(K/k)/\mathrm{Gal}(K/F) \to \mathrm{Gal}(F/k)$$

Proof. Recall from Corollary 1.14.37 we have F/k is normal iff $\sigma(F) = F$ for all $\sigma \in \mathrm{Gal}(K/k)$. We also observe that

$$\mathrm{Gal}(K/\sigma(F)) = \sigma\,\mathrm{Gal}(K/F)\sigma^{-1}$$

By the correspondence $\mathrm{Gal}(K/F) = \mathrm{Gal}(K/F') \iff F = F'$.
Therefore

$$\begin{aligned}
F/k \text{ normal} &\iff \sigma(F) = F \quad \forall \sigma \in \mathrm{Gal}(K/k) \\
&\iff \mathrm{Gal}(K/\sigma(F)) = \mathrm{Gal}(K/F) \quad \forall \sigma \in \mathrm{Gal}(K/k) \\
&\iff \sigma\,\mathrm{Gal}(K/F)\sigma^{-1} = \mathrm{Gal}(K/F) \quad \forall \sigma \in \mathrm{Gal}(K/k) \\
&\iff \mathrm{Gal}(K/F) \triangleleft \mathrm{Gal}(K/k)
\end{aligned}$$

Finally the natural restriction map is surjective by Corollary 1.14.36 and has the required kernel. □

1.15 Localization

Reference for this section is [**?** , Chap 1], [AM69, Section 3, Ex. 7-9].

Algebraically, localization can be seen as enlargening a ring to include inverses. In terms of the ideal structure this means removing (proper) ideals which contain the newly inverted elements. Geometrically ideals correspond to points/subsets, so localization may be viewed as reducing the set of interest.

Recall the definition of multiplicatively closed set. Some rather canonical examples are as follows

Example 1.15.1
The set $S_f = \{1, f, f^2, \ldots\}$ is m.c. but not necessarily saturated. As an example consider $A = \mathbb{Z}$ and $S_n = \{1, n, n^2, \ldots\}$ for n compositive. Then $pq \in S_n$ but $p \notin S_n$.

Example 1.15.2
The set $A \setminus \mathfrak{p}$ is a saturated multiplicatively closed set. More generally any set of the form

$$A \setminus \bigcup_i \mathfrak{p}_i$$

is a saturated multiplicatively closed subset.

The localization of A at a m.c. set S is denoted by $S^{-1}A$ and is typically defined as the set of fractions

$$S^{-1}A := \{\left[\frac{a}{s}\right] \mid a \in A\, s \in S\}/\sim$$

under the equivalence relation

$$\left[\frac{a}{s}\right] \sim \left[\frac{b}{t}\right] \iff u(at - bs) = 0 \quad \text{some } u \in S\,.$$

Proposition 1.15.1
The relation thus defined is an equivalence relation. The set $S^{-1}A$ is a ring under the obvious ring operations. It is non-zero precisely when S is proper. There is a canonical homomorphism

$$\begin{array}{rcl} i_S : A & \to & S^{-1}A \\ a & \to & \left[\frac{a}{1}\right] \end{array}$$

- *This is an isomorphism if and only if $S \subseteq A^\star$ already consists only of invertible elements (e.g. $S = \{1\}$).*
- *This is injective iff S has no zero-divisors*

Note when A is an integral domain and S is proper then the equivalence relation may be weakened to $at - bs = 0$.
The localization may be characterized more abstractly.

Definition 1.15.3 (S-invertible)
Let A be a ring with a m.c. subset S, then a homomorphism

$$\phi : A \to B$$

is said to be S-invertible if $\phi(S) \subseteq B^\star$. We denote by

$$\mathrm{Mor}_S(A, B)$$

the set of S-invertible homomorphisms.

We show that localization satisfies the following universal property

Proposition 1.15.2 (Universal Property of Localization)
Let A be a ring and S a proper m.c. subset then the map

$$\begin{array}{rcl} \mathrm{Mor}(S^{-1}A, B) & \to & \mathrm{Mor}_S(A, B) \\ \tilde{\phi} & \to & \tilde{\phi} \circ i_S \end{array} \tag{1.4}$$

is well-defined and a bijection. That is every S-invertible morphism $\phi : A \to B$ factors uniquely as $\tilde{\phi} \circ i_S$.

Proof. Define $\tilde{\phi}(a/s) = \phi(a)\phi(s)^{-1}$. This is well-defined, for suppose $a/s = a'/s'$. Then

$$t(as' - a's) = 0 \implies \phi(t)(\phi(a)\phi(s') - \phi(a')\phi(s)) = 0 \implies \phi(a)\phi(s') = \phi(a')\phi(s) \implies \phi(a)\phi(s)^{-1} = \phi(a')\phi(s')^{-1}$$

as required. This is clearly a ring homomorphism and satisfies $\phi = \tilde{\phi} \circ i_S$. Note any such $\tilde{\phi}$ satisfies $\tilde{\phi}(a/s) = \tilde{\phi}(a/1)\tilde{\phi}(1/s) = \tilde{\phi}(a/1)\tilde{\phi}(s/1)^{-1} = \phi(a)\phi(s)^{-1}$ and so is unique. □

Corollary 1.15.3
A localization $(i_S, S^{-1}A)$ satisfying the universely property (1.4) *above is unique up to unique isomorphism.*

Proof. The previous Proposition shows that the functor $\mathrm{Mor}(S^{-1}A, -)$ is naturally isomorphic to the functor $\mathrm{Mor}_S(A, -)$. The Yoneda Lemma shows that any two localizations have a canonical isomorphism.

More concretely if we have two localizations i_S, i'_S then they each factor through each other. By uniqueness these must be inverses, and hence isomorphisms. □

In the case that A is an integral domain then generally everything becomes a lot simpler.

Example 1.15.4 (Field of fractions)
Let A be an integral domain then $A \setminus 0 = A^\star$ and we define the field of fractions

$$\mathrm{Frac}(A) := (A \setminus 0)^{-1} A$$

Proposition 1.15.4 (Field of fractions contains all localization)
Let A be an integral domain, and $\mathrm{Frac}(A)$ the field of fractions. Define another model for $S^{-1}A$ as follows

$$S^{-1}A := \left\{ \frac{a}{s} \in \mathrm{Frac}(A) \mid a \in A \; s \in S \right\}$$

The canonical map $A \to S^{-1}A \subset \mathrm{Frac}(A)$ is injective, and satisfies the universal property for localization.

Proof. It's injective because A has no zero-divisors. That it satisfies the universal property is very similar as before. □

1.15.1 Canonical maps $S^{-1}A \to T^{-1}A$

In what follows consider all the proper multiplicatively closed subsets S of A, and fix models of the rings $S^{-1}A$ and morphisms i_S. We wish to consider canonical maps $i_{ST} : S^{-1}A \to T^{-1}A$ such that $i_{ST} \circ i_S = i_T$. First consider the saturation

Proposition 1.15.5 (Saturation)
Let A be a ring and S a multiplicatively closed set. Then the following sets are equal

- $(i_S)^{-1}((S^{-1}A)^\star)$
- $\{t \mid at \in S \text{ for some } a \in A\}$
- $\bigcap_{T \supseteq S : T \text{ saturated}} T$

which we denote by $\overline{S}$. We have the following properties

- *$\overline{S}$ is saturated.*
- *S is saturated if and only if $S = \overline{S}$*
- *$\overline{\overline{S}} = \overline{S}$.*

Proof. Denote the sets by S_1, S_2, S_3. Trivially they each contain S. Note that the group of units is a saturated multiplicatively closed set so that S_1 is saturated. And by definition S_2 and S_3 are saturated.

Suppose $t \in S_2$, then $at \in S \implies \phi(at) \in (S^{-1}A)^\star \implies \phi(t) \in (S^{-1}A)^\star \implies t \in S_1$. Conversely suppose $t \in S_1$, then $at/s = 1/1 \implies s'(at - s) = 0 \implies t \in S_2$.

It's clear that $S_3 \subseteq S_2$. Suppose that $S \subseteq T$ is saturated, we're required to show that $S_2 \subseteq T$. Suppose $t \in S_2$, then $at \in S \subseteq T \implies t \in T$ as required.

We have already noted that $\overline{S}$ is saturated. Clearly if S is saturated then $\overline{S} = S_2 = S$ as required. Conversely suppose $st \in S$, then clearly $s, t \in S_2 = S$ as required.

Since $\overline{S}$ is saturated we have $\overline{\overline{S}} = \overline{S}$. □

We can now characterize the existence of i_{ST}

Proposition 1.15.6
Let A be a ring and S, T two multiplicatively closed subsets. Then TFAE

- *There exists a unique $i_{ST} : S^{-1}A \to T^{-1}A$ such that $i_{ST} \circ i_S = i_T$.*
- *$S \subseteq \overline{T}$.*

We have commutativity

$$i_{TU} \circ i_{ST} = i_{SU}$$

$$i_{SS} = \mathbf{1}_{S^{-1}A}$$

and furthermore i_{ST} is an isomorphism if and only if $\overline{S} = \overline{T}$. In particular $i_{S\overline{S}}$ is an isomorphism.

Proof. Suppose i_{ST} exists then $i_T(S) = i_{ST}(i_S(S)) \subseteq i_{ST}((S^{-1}A)^\star) \subseteq (T^{-1}A)^\star$, whence $S \subseteq \overline{T}$.

Conversely $S \subseteq \overline{T} \implies i_T(S) \subseteq (T^{-1}A)^\star$ so i_{ST} exists by the universal property.

Commutativity follows from uniqueness.

If i_{ST} is an isomorphism then $i_{TS} = i_{ST}^{-1}$ exists so that $S \subseteq \overline{T}$ and $T \subseteq \overline{S}$. By minimality of saturation we see that $\overline{S} = \overline{T}$. Conversely if this holds, then clearly i_{ST} and i_{TS} exist. Furthermore by commutivity $i_{ST} \circ i_{TS} = i_{SS}$ and $i_{TS} \circ i_{ST} = i_{TT}$ as required.

Since $\overline{S} = \overline{\overline{S}}$ the last statement follows. □

Finally we give another characterization of saturated multiplicatively closed subsets

Proposition 1.15.7
Let A be a ring and S a multiplicatively closed subset. Then

$$\overline{S} = A \setminus \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p}$$

Proof. Denote the right hand side by T. Then clearly $S \subseteq T$ and as noted before T is saturated. Therefore $\overline{S} \subseteq T$.

Conversely suppose $a \notin \overline{S}$. Consider the principal ideal (a) then $(a) \cap S = \emptyset$ (because $ab \in S \implies a \in \overline{S}$ by Proposition 1.15.5). Therefore by Lemma 1.12.2 there is a prime ideal $\mathfrak{p}$ containing a which does not intersect S. Therefore $a \notin T$. We have shown that $a \notin \overline{S} \implies a \notin T$, contrapositively $T \subseteq \overline{S}$ as required. □

1.15.2 Ideal Structure

1.16 Local Rings

Definition 1.16.1 (Local Ring)
A pair $(A, \mathfrak{m})$ is a local ring if $\mathfrak{m}$ is the unique maximal ideal of the ring A. In this case we may write

$$\kappa(\mathfrak{m}) := A/\mathfrak{m}$$

which we call the "residue field".
We say it is a local k-algebra if A is also a k-algebra.

Generally we expect the residue field to be at most a finite extension of the base field k, as in the following

Proposition 1.16.1 (Finite residue field)
If $(A, \mathfrak{m})$ is a local k-algebra then there is a natural field extension

$$k \to A \to A/\mathfrak{m} = \kappa(\mathfrak{m})$$

If in addition A is a finitely generated k-algebra then $\kappa(\mathfrak{m})$ is a f.g. field extension of k, which is therefore finite algebraic. Finally if k is algebraically closed then $k = \kappa(\mathfrak{m})$.

Proof. See [AM69, Cor 7.10] for the second statement. □

Bibliography

[AM69] M. Atiyah and I.G. McDonald. *Introduction to Commutative Algebra*. Westview Press, 1969.