# Uni Notes

Daniel Alex Mineev

November 2, 2025

# Introduction

This document contains my personal notes from the courses I am taking at **Universitetet i Oslo**. It also includes some additional notes from my own independent studying, which are not directly part of the courses.

# Contents

# §1 Commutative Algebra

## 1.1 Ideals

**Theorem 1.1** **(The Fundamental Homomorphism Theorem)**
Let $\phi : A \to B$ be a homomorphism, then,

$$A/\ker\phi \cong \operatorname{im}\phi$$

*Proof.* Let $f(\alpha + \ker\phi) = \phi(\alpha)$. Then, notice this function is well defined, since, if $I = \alpha + \ker\phi = \beta + \ker\phi$, then we must show that,

$$\phi(\beta) = f(I) = \phi(\alpha)$$

Since $\alpha + \ker\phi = \beta + \ker\phi$ it must be that $\alpha + c = \beta + d$ and since $\ker\phi$ is an ideal it must be that $\alpha = \beta + \gamma$ where $\gamma \in \ker I$. Thus,

$$\phi(\alpha) = \phi(\beta + \gamma) = \phi(\beta) + \phi(\gamma) = \phi(\beta)$$

thus $\phi(\alpha) = \phi(\beta)$, so the function is well-defined.

Now, all that is left is to notice that if $x, y \in A/\ker\phi$, then,

$$\begin{aligned} f(x) \cdot f(y) &= f(\alpha + \ker\phi) \cdot f(\beta + \ker\phi) \\ &= \phi(\alpha) \cdot \phi(\beta) = \phi(\alpha\beta) = f(xy) \end{aligned}$$

$$f(x) + f(y) = \phi(\alpha) + \phi(\beta) = \phi(\alpha + \beta) = f(x + y)$$

thus $f$ is a homomorphism, trivially it is surjective.

Let us show that $f$ is injective, indeed if $f(\alpha + \ker\phi) = f(\beta + \ker\phi)$, then it must be that,

$$f(\alpha + \ker\phi) - f(\beta + \ker\phi) = f((\alpha - \beta) + \ker\phi) = 0$$
$$\implies \alpha - \beta \in \ker\phi$$

Thus, $\alpha \in \beta + \ker\phi$, thus it must be that $\alpha + \ker\phi = \beta + \ker\phi$, since $\ker\phi$ is known to be an ideal.

Thus, since $f$ is a homomorphism which is both surjective and injective it must be that an isomorphism, thus proving the desired isomorphism.

■

This theorem is quite useful since it connects two objects which might at first glance seem unrelated.

You might of noticed sometimes people use $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$ interchangibly to represent arithmitic modulo $n$. Notice, if $\mathbb{Z}_n$ is modular arithmetic mod $n$, then if one considers the remainder function $\phi : \mathbb{Z} \to \mathbb{Z}_n$, then its ime is $\mathbb{Z}_n$ and the kerner is $n\mathbb{Z}$, thus by the Fundemental Homomorphism theorem it must be that,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

This is arguably a trivial example, however at least now you know what the two different notations mean!

**Example 1.2** Let $\phi : \mathbb{Z}[X] \to \mathbb{C}$ be a homomorphism sending $x$ to $i$, thus,

$$\phi\left(\sum_j a_j x^j\right) = \sum_j a_j i^j$$

Then, trivially $\operatorname{im}\phi = \mathbb{Z}[i]$, it is also not difficult to show that,

$$\ker\phi = (x^2+1)$$

Then, by the Fundemental Homomorphism Theorem it must be that $\mathbb{Z}[X]/(x^2+1) \cong \mathbb{Z}[i]$.

As an exercise let us prove the theorem described in the example,

**Lemma 1.3** $\ker\phi = (x^2+1)$

*Proof.* Assume that $P(i) = 0$, then it must be that $P(x) = (x^2+1)Q(x)$, thus part of the ideal $(x^2+1)$. ■

Now, another useful theorem about ideals is the following,

**Theorem 1.4** Let $A$ be a ring and $I \subseteq A$ an ideal, then there is an *order-preserving* bijection between,

$$\left\{\text{ideals in } A/I\right\} \leftrightarrow \left\{\text{ideals } J \text{ of } A \text{ such that } I \subseteq J\right\}$$

and the bijection is given by,

1. If $J \subseteq A/I$ is an ideal, then it is sent to $\phi^{-1}(J) \subseteq A$.
2. If $J \subseteq A$ such that $I \subseteq J$, then it is sent to $\phi(J)$.

where $\phi$ is the quotient homomorphism.

To mention a bit of notation, given a ring $A$ the set of ideals $I \subseteq A$ is usually denoted as $\mathrm{Spec}(A)$.

## 1.2 Units and Fields

**Definition 1.5** Let $A$ be a ring, then $x \in A$ is,

1. A unit if there exists $y \in A$ such that,
$$xy = 1$$
2. A 0-divisor if there is $y \in A$,
$$xy = 0$$

Then,

**Definition 1.6** Notice,

1. A ring $A$ (non-zero) is a **field** if every $0 \neq x \in A$ is a unit.

2. $A$ is an **integral domain** if $A \neq 0$ and the only 0-divisor of $A$ is 0.

As an example in $\mathbb{Z}$ units are $\{1, -1\}$, thus not a *field*. However $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are *fields* and *integral domains*.

**Lemma 1.7** The only integral domains of the form $\mathbb{Z}_n$ are $\mathbb{Z}_p$ for a prime $p$.

Notice,

**Lemma 1.8** If $x \in A$, then, $x$ is a unit is equivelent to $(x) = A$.

*Proof.* Indeed, since if $x$ is a unit, then $(x)$ trivially contains 1, thus generates the entire ring $A$.

If $(x) = A$, then $1 \in (x)$, thus $xy = 1$, thus $x$ is a unit. ■

Another thing to notice,

**Lemma 1.9** $A$ is a field is equivalent to $A$ having exactly two ideals (0) and (1).

*Proof.* If $I \neq (0)$ is an ideal in $A$, then since each element is a unit it contains 1, thus is equal to (1). ■

Now, let us prove two important statements,

**Theorem 1.10** $I$ is prime $\Leftrightarrow$ $A/I$ is an integral domain.

*Proof.* Let us prove the statement both ways,

1. If $B = A/I$ is an integral domain, let $\phi$ be the quotient homomorphism. Then, if $xy \in I$, it must be that,

$$\phi(xy) = 0_B = \phi(x) \cdot \phi(y)$$

   thus, either $\phi(x)$ or $\phi(y)$ is $0_B$, which is equivelent to saying that either $x \in I$ or $y \in I$.

2. If $I$ is prime, then let $B = A/I$, then suppose $xy = 0_B$ and $\phi$ is the quotient homomorphism. Then, let $a \in \phi^{-1}(x)$ and $b \in \phi^{-1}(y)$, then, $ab \in I$, consequently either $a$ or $b$ is in $I$ which is equivelent to either $x$ or $y$ being $0_B$.

■

**Theorem 1.11** $I$ is maximal $\Leftrightarrow$ $A/I$ is a field.

*Proof.* Notice,

$$\left\{\text{ideals in } A/I\right\} \leftrightarrow \left\{\text{ideals } J \text{ of } A \text{ such that } I \subseteq J\right\}$$

thus since $I$ is maximal it must be that $A/I$ has only two ideals (0) and (1), which by the previous lemmas implies that $A/I$ is a field. ■

## 1.3 Prime/Maximal Ideals and Krull's theorem

Let us consider the following,

**Theorem 1.12** Let $I \subseteq J \subseteq A$, then $J$ being prime in $A$ is equivelent to $J/I$ being prime in $A/I$.

*Proof.* One proof is to consider the bijection theorem described earlier, however there is another approach. Notice, $J$ being prime is equivelent to $A/J$ being an integral domain. Analougously $J/I$ being prime in $A/I$ is equivelent to showing that $(A/I)/(J/I)$ being an integral domain as well.

Thus, the problem is equivalent to showing that $A/J$ being an integral domain is the same as showing that $(A/I)/(J/I)$ being an integral domain.

However, I claim that,

$$A/J \cong (A/I)/(J/I)$$

since if one considers the quotient homomorphism's $\phi : A \to A/I$ and $\psi : A/I \to (A/I)/(J/I)$, then, $\psi \circ \phi : A \to (A/J)/(I/J)$. Then,

$$\ker \psi \circ \phi = I$$

and $\psi \circ \phi$ is surjective (not difficult to show), consequently by the

fundemental homomorphism theorem it must be that,

$$A/I = A/(\ker \psi \circ \phi) \cong \operatorname{im} \psi \circ \phi = (A/J)/(I/J)$$

■

Similarly one can show that $J$ being maximal is equivelent to $J/I$ beeing maximal in $A/I$.

Notice another trivial property of prime/maximal ideals.

**Lemma 1.13** Every *maximal* ideal is prime.

*Proof.* Since $I \subseteq A$ is maximal it must be that $A/I$ is a field which is an integral domain which implies that $I$ is prime. ■

There is quite a beautiful example of a maximal ideal,

**Example 1.14** Let $k$ be an arbitrary field and $\vec{a} = (a_1, \ldots, a_n)$ be some $k$-tuple of size $n$. Then, consider the *evaluation* homomorphism,

$$\phi_{\vec{a}} : k[x_1, \ldots, x_n] \to k$$

$$\phi_{\vec{a}} : f \mapsto f(\vec{a})$$

Then, I claim that $\ker_{\phi_{\vec{a}}} \subseteq k[x_1, \ldots, x_n]$ is a maximal ideal. Since by the Fundamental Homomorphism theorem it must be that,

$$k[x_1, \ldots, x_n]/\ker_{\phi} \cong \operatorname{im} \phi = k$$

Thus, since $k$ is a field it must be that $\ker_\phi$ is a maximal ideal in $k[x_1, \ldots, x_n]$.

As it turns out we are actually always garanteed the existance of a maximal ideal within a ring by **Krull's theorem**.

**Theorem 1.15** **(Krull's Theorem)** Let $A$ be a ring $A \neq 0$, then $A$ has a maximal ideal.

*Proof.* Let $S$ be a poset on all ideals, where $I \geq J$ if $J \subseteq I$. Then, by Zorn's Lemma all that one must show is that every chain has an upper bound within $S$.

Let $R$ be some chain of ideals, then consider the following ideal,

$$X = \bigcup_i R_i$$

keep it mind that in general not all unions of ideals are themselves an ideal, however in this case it is an ideal (trivial to verify the axioms). Now, notice that $X \neq (1)$, since if $X = (1)$ then that would mean that one of the $R_i$ contains 1 since $1 \in (1)$, which would imply that some $R_i$ is the entire ring, contradiction!

Consequently, since $X$ is greater than all the elements in $R$ we have established an upper bound of $R$ for an abitrary chain $R$. Thus, by Zorn's lemma it must be that there exist maximal ideals! ■

We can use Krull's theorem to establish another useful property of ideals,

**Lemma 1.16** If $I$ is an ideal of $A$, then $I$ is contained within some maximal ideal $J$.

*Proof.* Indeed, notice that by the bijection established earlier showing the existance of such a $J$ is equivelent to finding a maximal ideal in $A/I$ which exists by Krull's theorem. ■

Another useful property of maximal ideals are their relationship with units of the ring $A$,

**Lemma 1.17** If $x$ is a unit, then it is not contained in any maximal ideal $I$ of a ring $A$.

*Proof.* If $x$ is a unit, then there exists $y$ such that $xy = 1$, consequently if $x \in I$ then by the aximos of ideals it must be that $1 \in I$ which implies that $I = (1) = A$, contradiction! ■

This leads us to an important piece of intuition that understanding the properties of units in a ring $A$ is essentialy equivelent to understanding the properties of maximal ideals of $A$.

**Lemma 1.18** Let $A$ be a ring such that for every $x \in A$ there exists such a $n \in \mathbb{Z}$ such that $x^n = x$, prove that every prime ideal of $A$ is maximal.

*Proof.* Let $I \subseteq A$ be a prime ideal, then in order to show that $I$ is maximal, one must show that $A/I$ is a field. Since $I$ is a prime ideal we already know that $A/I$ is an integral domain, meaning we must show that every element has a multiplicative inverse.

Let $x = \alpha + I \in A/I$ (for some $\alpha \neq 0$) then let us chose the minimal $n$ such that (it exists by the problem statement),

$$(\alpha + I)^n = \alpha^n + I = \alpha + I$$

$$x^n - x = x(x^{n-1} - 1) = 0$$

thus since $A/I$ is an integral domain it must be that $x^{n-1} = 1$, in other words there exists some $m$ that $x^m = 1$ in $A/I$. Consequently $x \cdot x^{m-1} = 1$. Thus, since $m - 1 < n$ it must be that $x^{m-1} \neq x$, thus $x$ has a multiplicative inverse.

Consequently $A/I$ is a field and thus it must be that $I$ is maximal. ■

## 1.4 Principle Ideal Domains & Unique Factorization Domains

The following natural definitions appear when dealing with rings,

**Definition 1.19** A ring $A$ is,

1. a *principle ideal domain* if every ideal $I \subseteq A$ is principle.

2. a *unique factorization domain* if every non-zero, non-unit is reducable.

Note, 0 is neither reducable or irreducable. Let us consider the following,

**Lemma 1.20** If $A$ is an integral domain and $(f)$ is prime (where $f \neq 0$), then $f$ is irreducable.

*Proof.* If $(f)$ is prime, it must be that $(f) \neq (1)$ and consequently $f$ is not a unit. Thus, assume that $g, h$ are such that $f = gh$, then,

$$(f) = (gh) \implies g \in (f) \vee h \in (f)$$

WLOG $g \in (f)$, then it must be that $g = af$. Thus,

$$f = gh = (af) \cdot h = (ah) \cdot f$$

since $A$ is an integral domain it must be that we can cancel $f$ on both sides and obtain $ah = 1$, thus implying that $h$ is a unit, contradiction! ■

Now, how to *precisely define* what it means for two factorizations to be equivelent. For example it would be nice to consider $2 \cdot 3 = (-2) \cdot (-3)$ as the same factorization of 6, thus the following definition is natural,

**Definition 1.21** Two factorizations are equivelent,

$$a = \prod_i p_i = \prod_i q_i$$

if there is some bijection between $p$ and $q$ such that,

$$p_i = u_i q_i$$

where $u_i$ is a unit.

**Example 1.22** Due to the fundamental theorem of arithmetic it must be that $\mathbb{Z}$ is a UFD (unique factorization domain).

Consider $\mathbb{Z}[i\sqrt{5}]$ it is not a UFD since,

$$6 = (1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \cdot 3$$

Now, notice,

**Lemma 1.23** If $A$ is a UFD and $f \in A$ is irreducable, then $(f)$ is prime.

*Proof.* Indeed, notice that $f$ being irreducable implies that $f$ is a non-unit, thus $(f) \neq (1)$.

Let $gh \in (f)$, then it must be that $gh = af$ for some $a \in A$. Notice, since $f$ is irreducable it must be that in the factorization of $g$ or $h$ the element $f$ is contained (possibly multiplied by some unit).

WLOG $g$ contains $f$ in its factorization.

Then, $g \in (f)$, which implies that $(f)$ is prime. ■

Here are two extremely useful results,

**Theorem 1.24** Every $PID$ is a $UFD$

**Theorem 1.25** **(Gauss)** If $A$ is a UFD, then $A[x]$ is a UFD as well.

This leads us to the following "chain" of inferences,

$$\text{field} \implies \text{PID} \implies \text{UFD} \implies \text{Integral Domain}$$

Now,

**Lemma 1.26** A ring $A$ is called *local* if it has exactly one maximal ideal.

**Example 1.27** Every field is local, $\mathbb{Z}$ is not local.

The ring $\mathbb{Z}/p^i\mathbb{Z}$ is local. (a very nice example to keep in mind)

Now,

**Lemma 1.28** Let $A$ be a local ring with a maximal ideal $M \subset A$, then the units of $A$ are $A \setminus M$.

$A$ is local $\iff$ the set of non-unit is ideal.

*Proof.* The first point is a consequence of a lemma discussed earlier.

To prove the second statement, assume that $A$ is a ring such that,

$$M = \{f \in A | f \text{ is not a unit}\}$$

is an ideal. Then,

$$M \text{ is a unique maximal ideal}$$
$$\Leftrightarrow \text{every ideal } I \neq (1) \text{ is such that } I \subseteq M$$

Let $x \in I$, then $(x) \subseteq I \subseteq (1)$ since this holds for all $x \in I$ it must be that $I \subseteq m$. ■

**Example 1.29** Consider,

$$\mathbb{R}(x) = \left\{\frac{f}{g} | f, g \in \mathbb{R}[x], g \neq 0\right\}$$

Then a subring

$$\mathbb{R}[x]_{(x)} = \left\{\frac{f}{g} | f, g \in \mathbb{R}[x] \text{ and } g \notin (x)\right\}$$

Then, it turns out that $\mathbb{R}[x]_{(x)}$ is local (basically the set of rational functions defined near zero).

## 1.5 The Chinese Remainder Theorem

A known result in number theory is that if $(n, m) = 1$, then $ax + by$ can equal any integer. This allows us to define relatively prime elements in a commutative ring,

**Definition 1.30** Ideals $I$ and $J$ are relatively prime if $I + J = (1)$.

**Example 1.31** In $\mathbb{Q}[x]$ we can consider the principle ideals $(x-2)$ and $(2x^2-2)$, then,

$$\begin{aligned}(x-2)+(2x^2-2) &= (x-2, 2x^2-2)\\ &= (x-2, 2x^2-2-2x^2+2x) = (x-2, 6) = (1)\end{aligned}$$

thus proving that $(x-2)$ is relatively prime to $(2x^2-2)$.

Notice, if we consider $\mathbb{Z}$, then if we have some relatively prime ideals $(2)$ and $(3)$, then $(2)\cdot(3) = (6)$ which is just $(2)\cap(3)$, this leads one to question whether this is always true. It turns out it is,

**Lemma 1.32** If $I, J \subseteq A$ are relatively prime, then $I \cdot J = I \cap J$.

*Proof.* One direction is trivial,

$$I \cdot J = \left\{ \sum_{i,j} a_i b_j \right\} \subseteq I \cap J$$

the other direction is no harder, assume that $c \in I \cap J$, then since $I$ and $J$ are relatively prime it must be that there exist some $a + b$ such that $a + b = 1$ where $a \in I$ and $b \in J$.

$$c = 1 \cdot c = (a + b) \cdot c = ac + bc \in I \cdot J$$

■

Let $A_1, \ldots, A_n$ be rings, then there is a natural definition of a *product* of these rings defined as,

$$\prod A_i = \{(a_1, \ldots, a_n) \mid a_i \in A_i\}$$

which is trivially a ring, where the operations are component-wise. Notice, we also have natural projection homomorphisms,

$$\phi_i : \prod_i A_i \to A_j$$

where $\phi_i((a_1, \ldots, a_n)) = a_i$. Another way to construct homomorphisms with ring products is to assume the existance of a homomorphism $\psi_i : B \to A_i$, then we can a product homomorphism defined as following,

$$\prod \psi_i : B \to \prod A_i$$

where $b \in B$ is sent to $(\psi_1(b), \ldots, \psi_n(b))$.

Now, we are ready to formulate the Generalized Chinese Remainder Theorem (sometimes written as CRT)

**Theorem 1.33** **(The Chinese Remainder Theorem)** Let $I_1, \ldots, I_n \subseteq A$ be ideals such that any two are coprime. Then,

$$A/\prod_i I_i \cong \prod A/I_i$$

**Example 1.34** Consider the two coprime ideals $(x-2)$ and $(x^2-2)$ in $\mathbb{Q}[x]$. Then,

$$\begin{aligned}\mathbb{Q}[x]/(x-2)(x^2-2) &\cong \mathbb{Q}[x]/(x-2) \times \mathbb{Q}[x]/(x^2-2) \\ &\cong \mathbb{Q} \times \mathbb{Q}(\sqrt{2})\end{aligned}$$

where the last step can be done due to the fundamental homomorphism theorem.

Another useful notion is the following,

**Definition 1.35** If $I, J \subseteq A$ are two ideals, then,

$$(I : J) = \{a \in A \mid aJ \subseteq I\}$$

then,

**Definition 1.36** Let $J \subseteq A$ be an indeal, then the annihlator of $J$ is,

$$\text{Ann}(J) = ((0) : J) = \{a \in A \mid b \in J : ab = 0\}$$

similarly we can define the annihlator of an element $x \in A$,

$$\text{Ann}(x) = \text{Ann}((x))$$

## 1.6 Extension & Contraction of ideals

**Definition 1.37** Let $I \subseteq A$ be an ideal of $A$, then the radical of $I$ is defined as,

$$\sqrt{I} = \{f \in A \mid \exists n \in \mathbb{Z} : f^n \in I\}$$

For example in $\mathbb{Z}$ the radical of $n$ simply looks at the prime factorization of $n$ and turns all the exponents into 1 coinciding the standard definition of a radical in number theory.

Similarly, notice that $\sqrt{(0)}$ are simply all elements such that $x^n = 0$ for some $n$, i.e. the nilpotents of $A$.

**Lemma 1.38** Let $I \subseteq A$ be an ideal, then $\sqrt{I}$ is an ideal.

Also, similarly to the formula charecterizing the set of nilpotents, the following theorem holds,

**Theorem 1.39** If $I \subseteq A$ is an ideal, then,

$$\sqrt{I} = \bigcap_{\substack{P \subset A \\ P \text{ prime}, \ I \subseteq P}} P$$

To prove this theorem we will first prove the following lemma,

**Lemma 1.40** If $I \subseteq A$ is an ideal, let $\phi$ be the quotient homomorphism, let $N \subseteq A/I$ be the nilradical, then,

$$\sqrt{I} = \phi^{-1}(N)$$

*Proof.* Notice, $p \in \sqrt{I}$ is equivelent to $f^n \in I$ which is equivelent to $\phi(f^n) = 0$. Due to properties of homomorphisms it must be that,

$$\phi(f^n) = \phi(f)^n = 0$$

thus it must be that $\phi(f)$ is nilpotent in $A/I$, thus is in $N$. ■

Using this lemma we can prove for example that $\sqrt{I}$ is an ideal, since $\sqrt{I}$ is the preimage of an ideal which is an ideal. We can also use this lemma to prove the theorem giving a description of the radical.

Notice,

$$\phi^{-1}(N) = \phi^{-1}\left(\bigcap_{\substack{P \subset A/I \\ P \text{ prime}}} P\right) = \bigcap_{\substack{P \subseteq A/I \\ P \text{ prime}}} \phi^{-1}(P) = \bigcap_{\substack{Q \in A, \\ Q \text{ prime}, \\ I \subseteq Q}} Q$$

which proves the theorem (assuming that the nilradical theorem is proven which will be proven later on).

As mentioned before, while preimages behave nicely with ideals, the same is not true for images, this naturally leads us to the following definition,

**Definition 1.41** Let $\phi : A \to B$ be a ring homomorphism, then let $I \subseteq A$, $J \subseteq B$, then,

- The **contraction** of $J$ *along* $\phi$ is $\phi^{-1}(J)$
- The **extension** of $I$ *along* $\phi$, denoted as $\phi(I)B$ (or $IB$ if $\phi$ is clear from the context) is the smallest ideal of $B$ containing $\phi(I)$.

Notice,

**Lemma 1.42** If $P \subset B$ is a prime ideal, then the contraction of $P$ is also prime in $A$.

*Proof.* Indeed, assume that $xy \in \phi^{-1}(P)$, then,

$$\phi(x) \cdot \phi(y) = \phi(xy) \in \phi(\phi^{-1}(P)) = P$$

which implies that either $\phi(x) \in P$ or $\phi(y) \in P$ since $P$ is prime. However, this means that either $x$ or $y$ is in $\phi^{-1}(P)$ which proves that $\phi^{-1}(P)$ is prime in $A$. ■

## 1.7 Modules & Free Modules and Quotient Modules

**Definition 1.43** Let $A$ be a ring, a module over $A$ is a set $M$ equiped with an operation $+ : M \times M \to M$ and a multiplication operation $\cdot : A \times M \to M$ such that,

1. $(M, +)$ is an Abelean group
2. $1_A m = m$
3. For any $a, b \in A$ and $m \in M$ it must be that $(a + b)m = am + bm$
4. For any $a \in A$ and $n, m \in M$ it must be that $a(n + m) = an + am$
5. $a(bm) = (ab)m$

As several examples, if $A$ is a vector space, then modules over $A$ is the same thing as a $A$ vector space. Another beautiful thing is that any Abelian group is actually simply a $\mathbb{Z}$-module, since we can define the multiplication by an integer as repeated addition.

Notice, for $\mathbb{Z}$-modules group homomorphisms and module homomorphisms are the same thing!

Another important concept is direct summation,

**Definition 1.44** Let $M, N$ be $A$-modules, then,

$$N \oplus M = M \times N$$

in fact for any finite number of $A$-modules, $\{M_i\}$ the direct sum of the modules is the same as the product of modules. However, when considering an infinite direct sum, a restriction on an element is added, that there is only a finite non-zero number of components.

Just as in vector spaces, a natural thing to do is to consider basis of modules. Trivially, some basis exists, since we can just consider all the elements, however what about uniqueness of expressability of each element in the module? Notice, the sums must be finite when spanning the module.

Let $N$ be a $A$-module. Let the basis be $E$, then consider the homomorphism $\phi : A^{\oplus E} \to N$.

Notice, if $f$ is not uniquely expressed as a linear combination of the basis elements, then we can consider the difference of the two linear combinations and thus obtain multiple representations of 0. Thus, in order for $f$ to have the nice property of unique linear combinations it must be that $\ker \phi = 0$, in other words that $\phi$ is an isomorphism. Thus, that $N \cong A^{\oplus E}$. This motivates the following definition,

**Definition 1.45** Let $N$ be an $A$-module. Then $N$ is **free** if $N \cong A^{\oplus \Lambda}$.

Notice, if $A$ is some commutative ring, then any ideal $I \subseteq A$ is actually an $A$-module! Since we can consider quotient rings, this motivates one to consider quotient modules.

**Definition 1.46** Let $N \subseteq M$ be a submodule, then,

$$M/N = \{m + N \mid m \in M\}$$

where the operations are defined canonically.

## 1.8 Module Isomorphism Theorems & Presentations of Modules

Just as in group theory there are fundamental isomorphism theorems there are module isomorphism theorems!

**Theorem 1.47** **(Module Isomorphism Theorems)**

1. Let $\phi : M \to N$, then

$$\operatorname{im} \phi \cong M/\ker \phi$$

2. Given $M_1 \subseteq M_2 \subseteq M_3$, then we have,

$$M_3/M_2 \cong (M_3/M_1)/(M_2/M_1)$$

3. Given submodules $M, N \subseteq P$ we have,

$$(N+M)/M \cong N/(M \cap N)$$

*Proof.* I will only prove the third statement to showcase the power of the first statement. Consider the homomorphism $\phi : N \to (N+M)/M$ where $\phi(n) = n+M$, then $\phi$ is surjective and $\ker \phi = M \cap N$, thus it must be that $(N+M)/M \cong N/(M \cap N)$. ■

If $M$ is free, then $M \cong A^{\oplus \Lambda}$, then if $\Lambda$ is finite, then the rank of $M$ is simply the cardinality of $\Lambda$.

**Lemma 1.48** Let $M$ be an $A$-module. Then there exists some free module $F$ and a surjective homomorphism $\phi : F \to M$.

*Proof.* Indeed, consider $A^{\oplus M}$, along with $\phi$ such that $\phi((a_m)_{m \in M}) = \sum_{m \in M} a_m m \in M$, then trivially $\phi$ is surjective, since for any $x \in A^{\oplus M}$ we can consider $e_x = (0, 0, \ldots, 1, \ldots, 0)$ where 1 is for the $x$ element. ■

This lemma allows us to make the following definition,

**Definition 1.49** Let $M$ be an $A$-module, then the **presentation** of $M$ are free modules $F'$ and $F$ along with a homomorphism $\phi : F' \to F$ where $M \cong \operatorname{cok} \phi$.

Notice,

**Theorem 1.50** Any module has a presentation.

*Proof.* Indeed, by the lemma proven earlier it must be that there exists some surjective homomorphism $\phi : F \to M$ and some surjective homomorphism $\psi : F' \to \ker \phi$ (since $\ker \phi$ is also a module). Thus,

$$\psi : F' \to \ker \phi \subseteq F \xrightarrow{\phi} M$$

then,

$$\operatorname{cok} \psi = F/\operatorname{im} \psi = F/\ker \phi \cong \operatorname{im} \phi = M$$

which proves the existance of the desired presentation. ■

This means that a presentation can equivelently be defined as a set $(G, R, \phi, \psi)$ where $G$ and $R$ are some sets and $\phi : A^{\oplus R} \to A^{\oplus G}$ and $\psi : A^{\oplus G} \to M$ are homomorphisms such that $\psi$ is surjective and $\operatorname{im} \phi = \ker \psi$. In other words a presentation of $M$ is,

$$F' \xrightarrow{\phi} F \to M \to 0$$

Due to the rather complex definition of a **presentation** of a module it is rather useful to think of it as some generators and relations. Indeed, since $F$ is free we can consider its basis, then the

surjection $F \to M$ says that this basis *generates* $M$. Notice, the kernel of $F \to M$ consists of all linear combinations of the generators that vanish in $M$, these represent the *relations* between the generators.

This leads us to a rather intuitive understanding of a presentation to be simply a generalized notion of a basis for modules.

## 1.9 Nakayama's Lemma

**Theorem 1.51** **(Nakayama's Lemma)** Let $A$ be a *local* ring and $M$ a finitely generated $A$-module. Then, if $m$ is the maximal ideal of $A$, then if $mM = M$, then $M = 0$.

*Proof.* Assume that $mM = M$, then if $m_1, \ldots, m_n$ are the generators of $M$, then,

$$m_i = \sum_{j=1}^{n} a_{ij} m_j, \text{ where } a_{i,j} \in m$$

thus, notice that we can rewrite this as that for any $i$ that,

$$a_{i1}m_1 + a_{i2}m_2 + \ldots + (a_{ii} - 1)m_i + \ldots + a_{in}m_n = 0$$

Let $T = (a_{ij})$ be a matrix. Then, this condition can be rewritten as,

$$T \begin{pmatrix} m_1 \\ m_2 \\ \dots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

now multiplying both sides by $\text{adj}(T)$ we obtain,

$$\det(T) I_n \begin{pmatrix} m_1 \\ m_2 \\ \dots \\ m_n \end{pmatrix} = \begin{pmatrix} \det(T)m_1 \\ \det(T)m_2 \\ \dots \\ \det(T)m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

however, notice that using the determinant can be expressed as using the Leibniz formula, then the main diagonal term is,

$$(a_{11} - 1)(a_{22} - 1) \dots (a_{nn} - 1) = (-1)^n + X, \text{ where } X \in m$$

indeed, since any product of $a_{ij}$ must lie in $m$ due to it being closed under multiplication. All the other terms thus will also "cancel" and lie in $m$. Thus, $\det(T) = (-1)^n + Y$ where $Y \in m$, this implies that $\det(T) \notin m$ (since otherwise $m$ is not proper). However, since $A$ is local this must mean that $\det(T)$ is a unit. However,

$$\det(T)m_i = 0$$

which implies that $m_i = 0$ (since we can multiply both sides by $\frac{1}{\det(T)}$). This implies that $m_1 = \dots = m_n = 0$ which implies that $M = 0$. ■

## 1.10 Additive functions & exact sequences

**Definition 1.52** A *short* exact sequence is an exact sequence of the form,

$$0 \to M' \to M \to M'' \to 0$$

amusingly any short exact sequence has a well-behaved structure as the following lemma shows,

**Lemma 1.53** If

$$0 \to M \xrightarrow{\phi} N \xrightarrow{\psi} P \to 0$$

is a short exact sequence of $A$-modules, then there exists an $A$-module $K \subset N$ such that $M \cong K$ and $P \cong N/K$.

*Proof.* Let $K = \operatorname{im} \phi$, then since $\phi$ is injective it must be that $M \cong K$. Now, due to the fundamental homomorphism theorem it must be that,

$$P = \operatorname{im} \psi \cong N/\ker \psi = N/K$$

which proves the desired result. ■

**Definition 1.54** A function $v : \mathrm{Mod}_A \to G$ (where $G$ is some abelian group) is additive if,

$$0 \to M' \to M \to M'' \to 0$$

being exact implies that $v(M) = v(M') + v(M'')$.

a trivial example is that when $A$ is a field, then $v(M) = \dim_e(M)$ is an additive function, however there is another more interesting example,

**Example 1.55** Let $S$ be all finite $\mathbb{Z}$-module (i.e. finite abelian groups), let $v : S \to (\mathbb{Q}^\star, \cdot)$ be defined as simply the cardinality of the given $\mathbb{Z}$-module. Then, notice that due to a previously proven lemma we know that a short exact sequence must be of the form,

$$0 \to N \to M \to M/N \to 0$$

then by Lagrange's theorem we know that $|M/N| \cdot |N| = |M|$ which proves that $v$ is additive in $(\mathbb{Q}^\star, \cdot)$.

**Theorem 1.56** Let $v$ be an additive function defined all the submodules of $M_1, \ldots, M_n$ and the modules themselves, let,

$$0 \to M_1 \to \ldots \to M_n \to 0$$

be exact then,

$$\sum_{i=1}^{n} (-1)^i v(M_i) = 0$$

*Proof.* To prove this rather interesting theorem we will first prove

the following lemma,

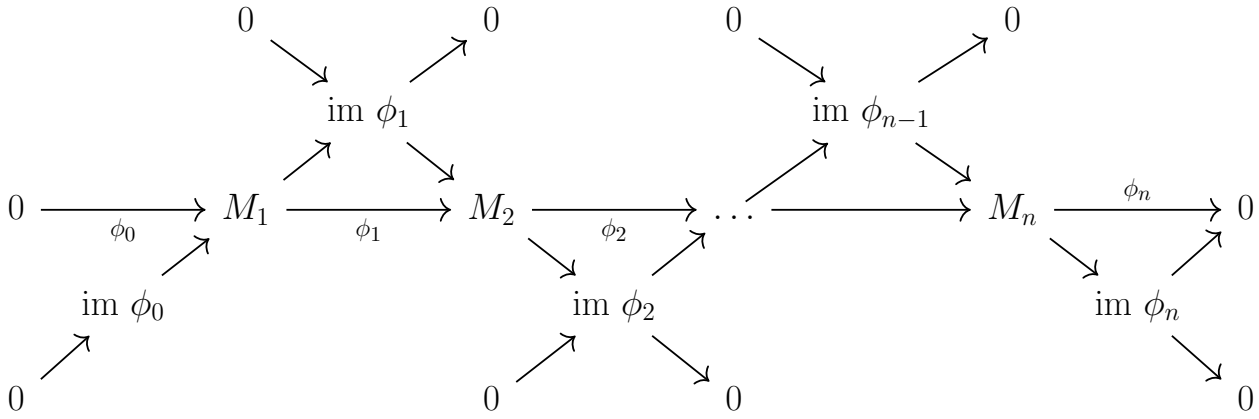
**Lemma 1.57** Let $M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$ be exact, then,

$$0 \to \operatorname{im}\phi \to M \to \operatorname{im}\psi \to 0$$

is exact.

*Proof.* Per definition the homomorphism between $M$ and $\operatorname{im}\psi$ is surjective, proving exactness of the later sequence at $\operatorname{im}\psi$. Analogously the canonical homorphism between $\operatorname{im}\phi$ and $M$ is injective. Exactness at $M$ means that $\operatorname{im}\phi = \ker\psi$, however that follows from the exactness of the original sequence. ■

Consequently we can draw the following monsterous diagram,




it must be exact. Thus, we know that,

$$v(\operatorname{im}\phi_i) + v(\operatorname{im}\phi_{i+1}) = v(M_{i+1})$$

thus we see that,

$$\sum_{i=1}^{n}(-1)^i v(M_i) = 0$$

which proves the theorem. ■

# §2 Galois Theory

An import concept related to fields is,

**Definition 2.1** $K$ is a *field extension* of $F$ if $K \subseteq F$, where $K$ and $F$ are fields, usually denoted as $K/F$.

A natural concept to consider from here is,

**Definition 2.2** An *algebraic closure* of a field $F$ is the minimal *field extension* $K$ of $F$ such that for all $P(X) \in F[X]$ the roots of $P$ lie in $K$.

As an example the *algebraic closure* of $\mathbb{Q}$ are algebraic numbers and the *algebraic closure* of $\mathbb{R}$ is $\mathbb{C}$.

Let *embedding* be an *injective field homomorphism* $f : K \hookrightarrow \mathbb{C}$ which fixes $\mathbb{Q}$. Then,

**Lemma 2.3** Under an *embedding* an element gets sent to one of its Galois conjugates.

*Proof.* Let us consider the minimal polynomial over $\mathbb{Q}$, then,

$$a_1 + a_2\alpha + \ldots + a_n\alpha^n = 0$$

Then, applying an embedding $f$ to both sides we obtain,

$$f(a_1) + f(a_2)f(\alpha) + \ldots + f(a_n)f(\alpha)^n = f(0)$$

$$a_1 + a_2 f(\alpha) + \ldots + a_n f(\alpha)^n = 0$$

Thus, $f(\alpha)$ is a root of the minimal polynomial, thus one of the Galois conjugates of $\alpha$ by definition. ■

This lemma actually tells us a lot about the behaviour of *embeddings*. Consider $\mathbb{Q}(\sqrt{2})$, since the minimal polynomial of $\sqrt{2}$ is $x^2 - 2 = 0$ which contains two roots, thus a *embedding* can send $\sqrt{2}$ only to one of those two roots, then the rest of the function is determined. Consequently there are only 2 embeddings of $\mathbb{Q}(\sqrt{2})$.

In general the same logic can be applied to derive that the number of embeddings $f : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ is simply the *algebraic degree* of $\alpha$.

Actually a more general theorem holds,

**Theorem 2.4** The number of embeddings $f : K \hookrightarrow \mathbb{C}$ is precisely the degree of field $K/\mathbb{Q}$.

*Proof.* Let $K = \mathbb{Q}(a_1, \ldots, a_n)$. Then, the number of embeddings $f : \mathbb{Q}(a_1, \ldots, a_k) \hookrightarrow \mathbb{C}$ is simply,

$$[\mathbb{Q}(a_1, \ldots, a_k) : \mathbb{Q}(a_1, \ldots, a_{k-1})] \ldots [\mathbb{Q}(a_1, a_2) : \mathbb{Q}(a_1)] \cdot [\mathbb{Q}(a_1) : \mathbb{Q}] = [\mathbb{Q}(a_1, \ldots, a_k) : \mathbb{Q}] = [K : \mathbb{Q}]$$

which proves the desired result. ■

The logic here is quite general, thus it can be generalized further to abritrary algebraic closures, all that is required is that a polynomial being irreducable implies that it doesn't have double roots (this

is allowed since we are working in an algebraic closure). A more general theorem holds, the proof is trivially the same,

**Theorem 2.5** Let $K/F$ be an a field extension and let $G$ be an algebraic closure of $F$, then there exist $[K : F]$ embeddings $\sigma : K \to G$ that fix $F$.

Now, given a field extension $K/F$ we can consider the group of automorphisms from $K/F$ to itself. Then,

**Lemma 2.6** $|\operatorname{Aut}(K/F)|$ divides $[K : F]$

*Proof.* TODO (Consequence of Lagrange) ■

Notice, that we can determine $|\operatorname{Aut}(K/F)|$ given $K = F(\alpha_1, \ldots, \alpha_n)$, since $\alpha$ has to go to its Galois conjugates, however since it is an automorphism those roots must go to the roots which are in $K$. To provide several examples,

1. $|\operatorname{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$, since the Galois conjugates of $\sqrt{2}$ are $-\sqrt{2}$ and $\sqrt{2}$ both of which lie in $\mathbb{Q}(\sqrt{2})$. Thus it is also true that $\operatorname{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

2. $|\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$, since the Galois conjugates of $\sqrt[3]{2}$ are complex, the only one in $\mathbb{Q}(\sqrt[3]{2})$ being $\sqrt[3]{2}$, thus there is only one automorphism, and it is the identity function.

Notice,

**Theorem 2.7** Let $K/F$ be a finite seperable field extension and let $K/F = F(\alpha_1, \ldots, a_h)$. Then, let $\mu(\alpha)$ be the number of Galois conjugates of $\alpha$ present in $K/F$. Then,

$$|\operatorname{Aut}(K/F)| \leq \prod_{i=1}^{h} \mu(\alpha_i)$$

*Proof.* Since each of the generators may be sent to one of the $\mu(\alpha_i)$ elements, we obtain the desired result. (notice inequality is important since not any configurtion gives rise to a valid automorphism) ■

However, it turns out that due to **Artin's primitive element theorem** that all finite seperable field extensions have the minimal generator set of size 1, i.e. $K/F = F(\alpha)$ for some $\alpha \in K$, thus reducing the above theorem to just one factor.

Now, this discussion naturally leads to the following definition,

**Definition 2.8** A finite field extension $K/F$ is a Galois field extension if and only if,

$$|\operatorname{Aut}(K/F)| = [K : F]$$

Notice, if $K/F = F(\alpha_1, \ldots, \alpha_n)$, then,

$$\begin{aligned} |\operatorname{Aut}(K/F)| &= [F(a_1, \ldots, a_k) : F(a_1, \ldots, a_{k-1})] \cdot \ldots \cdot [F(a_1) : F] \\ &= [K : F] \end{aligned}$$

the only condition required for this proof to work is that $K/F$ is *normal* (i.e. given any irreducable polynomial $p \in F[X]$ with at least one root in $K/F$ it splits completely in $K/F$) and seperable, thus we obtain the following,

**Theorem 2.9** If a field extension is seperable and *normal*, then it is a Galois field extension.

obviously the definitions are now equivelent. However, it turns out there is another way to define a Galois extension, an equivelent formulation,

**Theorem 2.10** A field extension $K/F$ is Galois if and only if it is a splitting field of some separable polynomial $p \in F[X]$.

The proof for why $K/F = \mathrm{Spl}_F(p)$ implies $K/F$ is Galois is the exact same the one one provided above, since the minimal polynomials of $a_i$ all split since $p$ splits. The other direction is a bit trickier, thus I will not provide the proof of this statement.

When a field extension $K/F$ is Galois, the group of automorphisms on it is denoted as $\mathrm{Gal}(K/F)$ and called the Galois group of $K/F$.

Similarly one can define a *Galois closure* of $K/F$ which is the minimal field extension $L/K$ such that $L/F$ is a Galois field extension, where minimality means any other field extension satisfying this property contains $L$.

It turns out constructing Galois closure's isn't that difficult, in fact,

**Theorem 2.11** Suppose $K = F(\alpha_1, \ldots, \alpha_n)$, then the Galois closure $L$ is,

$$L = \mathrm{Spl}_F(m_1, \ldots, m_n)$$

where $m_i$ is the minimal polynomial of $\alpha_i$.

*Proof.* Notice, trivially $K \subseteq L$ since $(\alpha_1, \ldots, \alpha_n)$ all must be present in $L$ since the minimal polynomials contain $\alpha_i$ as roots.

Notice, $L/F$ is a seperable and normal field extension, thus a Galois field extension.

It is minimal, since the Galois closure must be seperable and normal it must be the roots of the minimal polynomials of $\alpha_i$ are present in the Galois closure, thus we obtain that any Galois closure must contain $L$.

Consequently, we obtain the the Galois closure of $K/F$ is simply the splitting field of the minimal polynomials of the generators of $K/F$. ■