Uni Notes

Daniel Alex Mineev

August 24, 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,

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

however, since $\alpha, \beta \in I$ then,

$$\begin{cases} \phi(\alpha) = \phi(\gamma_1 + c) = \phi(\gamma_1) + \phi(c) = \phi(c) \\ \phi(\beta) = \phi(\gamma_2 + c) = \phi(\gamma_2) + \phi(c) = \phi(c) \end{cases}$$

where $\gamma_1, \gamma_2 \in \ker\phi$, 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 injective and surjective, consequently an isomorphism, proving the desired result. ■

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 ϕ 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 $\operatorname{Spec}(A)$.

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 ϕ 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 ϕ 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. ■

§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 α 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 α.

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 α 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 α 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 α_i.

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