Solutions for Neukirch's Algebraic Number Theory

Gao, Xu

June 22, 2015

Preface

This document is a collection of solutions for exercises from Jürgen Neukirch's *Algebraic Number Theory* (ANT for short) and is based on the discussion of an after-class seminar organized by me.

In addition to solutions, I also put some extra contents related to each exercise. To emphasize this, the numbering is counted by exercises instead of sections. After that, I hide the section information in the label of exercises to reduce its length. In order to avoid confusion, when I cite something from ANT, I will put a pair of brackets on its label. For instance, Proposition 2.2 means a proposition related to Exercise 2 of this section while Proposition (2.2) means the corresponding proposition in §2 of ANT.

For self-contain, I included the statements of the propositions from ANT with remarks from our discussion. The labels of propositions from ANT keep the same format with in ANT and the additional remarks use alphabeta labels.

Gao, Xu[1]

A list of Unfinish Terms

- Proposition I.2.5.8
- Exercise I.8.2

[1] Email: GauSyu@gmail.com

Contents

List of Theorems

Notations

I

Algebraic Integers

§ 1 The Gaussian Integers

I Review

The book start the discussion by review the following *Fermat's theorem* on sums of two squares.

(1.1) Theorem *For all prime numbers $p \neq 2$, one has:*

$$p = a^2 + b^2 \quad (a, b \in \mathbb{Z}) \iff p \equiv 1 \bmod 4.$$

To get the proof, the ***gaussian integer***

$$Z[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

are introduced.

(1.2) Proposition *The ring $\mathbb{Z}[i]$ is euclidean, therefore in particular factorial.*

Then, a useful concept ***norm***, is defined as

$$N(x + iy) = x^2 + y^2.$$

(1.3) Proposition *The group of units of the ring $\mathbb{Z}[i]$ consists of the fourth roots of unity,*

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

Two elements α, β in a ring are called ***associated***, symbolically $\alpha \sim \beta$, if they differ only by a unit factor.

(1.4) Theorem *The prime elements π of $\mathbb{Z}[i]$, up to associated elements, are given as follows.*

1. $\pi = 1 + i$,
2. $\pi = a + bi$ *with* $a^2 + b^2 = p, p \equiv 1 \bmod 4, a > |b| > 0$,
3. $\pi = p, p \equiv 3 \bmod 4$.

Here, p denotes a prime number of $\mathbb{Z}$.

(1.5) Proposition *$\mathbb{Z}[i]$ consists precisely of those elements of the extension field $\mathbb{Q}(i)$ of $\mathbb{Q}$ which satisfy a monic polynomial equation*

$$x^2 + ax + b = 0$$

with coefficients $a, b \in \mathbb{Z}$.

The last proposition leads us to the general notion of an algebraic integer.

II Exercises

1 $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$.

Proof: Let $\alpha = x + iy$, where $x, y \in \mathbb{Z}$, then $N(\alpha) = x^2 + y^2 \in \mathbb{Z}$.

If α is a unit, then $N(\alpha)N(\alpha^{-1}) = N(1) = 1$ implies $N(\alpha) = 1$. Conversely, if $N(\alpha) = 1$, then it conjugate $\bar{\alpha} = x - iy$ is its inverse. □

2 Show that, in the ring $\mathbb{Z}[i]$, the relation $\alpha\beta = \varepsilon\gamma^n$, for α, β relatively prime numbers and ε a unit, implies $\alpha = \varepsilon'\xi^n$ and $\beta = \varepsilon''\eta^n$, with $\varepsilon', \varepsilon''$ units.

We prove a general result:

2.1 Proposition *In a UFD, the relation $\alpha\beta = \varepsilon\gamma^n$, for α, β relatively prime numbers and ε a unit, implies $\alpha = \varepsilon'\xi^n$ and $\beta = \varepsilon''\eta^n$, with $\varepsilon', \varepsilon''$ units.*

Proof: By the unique factorization, we may assume $\alpha = \varepsilon_1\pi_1^{l_1}\pi_2^{l_2}\cdots\pi_s^{l_s}$, $\beta = \varepsilon_2\pi_1^{m_1}\pi_2^{m_2}\cdots\pi_s^{m_s}$ and $\gamma = \varepsilon_3\pi_1^{n_1}\pi_2^{n_2}\cdots\pi_s^{n_s}$. Then from $(\alpha, \beta) = 1$, we know that $l_j m_j = 0$ for $j = 1, 2, \cdots, s$. From $\alpha\beta = \varepsilon\gamma^n$, we know that $l_j + m_j = nn_j$ for $j = 1, 2, \cdots, s$. Thus we have $l_j = nn_j$ or $m_j = nn_j$ for $j = 1, 2, \cdots, s$, and the conclusion follows. □

3 Show that the integer solutions of the equation

$$x^2 + y^2 = z^2$$

such that $x, y, z > 0$ and $(x, y, z) = 1$ ("pythagorean triples") are all given, up to possible permutation of x and y, by the formula

$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2,$$

where $u, v \in \mathbb{Z}$, $u > v > 0$, $(u, v) = 1$, u, v not both odd.

Proof: Let $\alpha = x + iy$, then (x, y, z) is a pythagorean triple just means $N(\alpha) = z^2$ and we may then assume $(\alpha, \bar{\alpha}) = 1$. Thus, by Exercise 2, we have $\alpha = \varepsilon\xi^2$ with ε a unit. Let $\xi = u + iv$, then the conclusion follows. □

4 Show that the ring $\mathbb{Z}[i]$ can not be ordered.

Proof: First, we recall the definition of ordered rings.

4.1 An ***ordered ring*** is a ring R with a total order $\leqslant$ such that for all a, b and c in R:

- if $a \leqslant b$ then $a + c \leqslant b + c$.
- if $0 \leqslant a$ and $0 \leqslant b$ then $0 \leqslant ab$.

An element $a \neq 0$ is said to be ***positive*** if $0 \leqslant a$, and ***negative*** if $a \leqslant 0$. The element 0 is considered to be neither positive nor negative.

A basic fact is the following

4.2 Proposition *For every element a in an ordered ring, exactly one of the following is true: a is positive, $-a$ is positive, or $a = 0$. In particular, a is negative if and only if $-a$ is positive.*

Assume $\mathbb{Z}[i]$ is ordered by a total order $\leqslant$. Consider i, if it is positive, then $-1 = i^2$ is positive, thus so is $1 = (-1)^2$, which contradicts the above proposition. □

5 Show that the only units of the ring $\mathbb{Z}[\sqrt{-d}]$ for every rational integer $d > 1$, are ± 1.

Proof: The norm of an element $\alpha = x + y\sqrt{-d}$ is $N(\alpha) = x^2 + dy^2$. One can see α is a unit if and only if $N(\alpha) = 1$ (cf. Exercise 1). Thus, α is a unit if and only if (x, y) is an integer solution of the equation $x^2 + dy^2 = 1$. Since $d > 1$, the only integer solution of the equation must be $(\pm 1, 0)$. □

6 Show that the ring $\mathbb{Z}[\sqrt{d}]$, for every square-free integer $d > 1$, has infinitely many units.

Proof: (cf. Exercise 1 and Exercise 5) This equals to prove the Pell's equation $x^2 - dy^2 = \pm 1$ has infinitely many integer solutions. □

6.1 Proposition *For every square-free integer $d > 1$, the* **Pell's equation** *$x^2 - dy^2 = 1$ has infinitely many integer solutions.*

Here we provide a proof using *Dirichlet's approximation theorem.*

6.2 Lemma (Dirichlet's approximation theorem) *For an irrational number θ, there exist infinitely many pairs of integers (x, y) such that $\left|\theta - \frac{x}{y}\right| < \frac{1}{y^2}$.*

Proof: By *Dirichlet's drawer principle*, one can see that for every positive integer N, there exists integers x and y such that $1 \leqslant y \leqslant N$ and

$$|x - y\theta| \leqslant \frac{1}{N+1}.$$

Indeed, let $\theta_y = y\theta - [y\theta]$ for $1 \leqslant y \leqslant N$. If there exists some y such that $\theta_y \in \left(0, \frac{1}{N+1}\right)$ or $\theta_y \in \left[\frac{N}{N+1}, 1\right)$, then either $|[y\theta] - y\theta| < \frac{1}{N+1}$, or $|([y\theta]+1) - y\theta| < \frac{1}{N+1}$. If it is not the case, we have N numbers θ_y and $N-1$ remaining intervals $\left[\frac{1}{N+1}, \frac{2}{N+1}\right), \cdots, \left[\frac{N-1}{N+1}, \frac{N}{N+1}\right)$, thus there must exist $1 \leqslant y_1 < y_2 \leqslant N$ and $0 < k < N$ such that $\theta_{y_1}, \theta_{y_2} \in \left[\frac{k}{N+1}, \frac{k+1}{N+1}\right)$. Then we have $|([y_2\theta] - [y_1\theta]) - (y_2 - y_1)\theta| < \frac{1}{N+1}$.

Then the conclusion follows directly: once we get a pair of integers (x, y) such that $|x - y\theta| \leqslant \frac{1}{N+1}$, we can choose some large integer N' such that $|x - y\theta| > \frac{1}{N'+1}$ and then get another pair of integers (x', y'). Then we will get infinitely many different pairs of integers and each pair (x, y) satisfies $\left|\theta - \frac{x}{y}\right| < \frac{1}{y^2}$. □

6.3 Corollary *For every square-free integer $d > 1$, there exist infinitely many pairs of integers (x, y) such that $\left|x^2 - dy^2\right| < 1 + \sqrt{d}$.*

Proof: First, there exist infinitely many pairs of integers (x, y) such that $\left|x - y\sqrt{d}\right| < \frac{1}{y}$. For those pairs, we have

$$\begin{aligned}\left|x + y\sqrt{d}\right| &= \left|x - y\sqrt{d} + 2y\sqrt{d}\right| \\ &\leqslant \left|x - y\sqrt{d}\right| + 2y\sqrt{d} \\ &< \frac{1}{y} + 2y\sqrt{d}.\end{aligned}$$

Therefore,

$$\begin{aligned}\left|x^2 - dy^2\right| &= \left|x - y\sqrt{d}\right| \left|x + y\sqrt{d}\right| \\ &< \frac{1}{y}(\frac{1}{y} + 2y\sqrt{d}) \\ &= 1 + 2\sqrt{d}.\end{aligned}$$

□

6.4 Corollary *For every square-free integer $d > 1$, there exists some integer k such that $1 < |k| < 1 + \sqrt{d}$ and the equation $x^2 - dy^2 = k$ has infinitely many integer solutions.*

Proof: It is obvious that the only integer solution for $x^2 - dy^2 = 0$ is $(0, 0)$. Then the result follows from *Dirichlet's drawer principle.* □

Proof (Proposition 6.1): Assume the equation $x^2-dy^2=k$ has infinitely many integer solutions and (x_1,y_1) and (x_2,y_2) are two positive solutions such that $x_1 \equiv x_2 \bmod |k|, y_1 \equiv y_2 \bmod |k|$. Then we have

$$(x_1x_2-dy_1y_2)^2-d(x_1y_2-x_2y_1)^2=(x_1^2-dy_1^2)(x_2^2-dy_2^2)=k^2.$$

But we already have k divides $x_1y_2-x_2y_1$, thus it also divides $x_1x_2-dy_1y_2$. Therefore $(\frac{1}{k}(x_1x_2-dy_1y_2),\frac{1}{k}(x_1y_2-x_2y_1))$ is an integer solution of the equation $x^2-dy^2=1$.

Let (x_0,y_0) denote the smallest positive integer solution of $x^2-dy^2=1$ in the sense that $x_0+y_0\sqrt{d}$ is minimal. Then we claim

> The integer solutions of the equation $x^2-dy^2=1$ are precisely $\Big\{(x,y)\Big||x+y\sqrt{d}|=|x_0+y_0\sqrt{d}|^n,\text{ for some } n\in\mathbb{Z}\Big\}$.

Indeed, let (x,y) be any integer solution, we may assume it is positive. If there exist some $n>0$ such that $(x_0+y_0\sqrt{d})^n<x+y\sqrt{d}<(x_0+y_0\sqrt{d})^{n+1}$, then we have $1<(x+y\sqrt{d})(x_0-y_0\sqrt{d})^n<(x_0+y_0\sqrt{d})$. Let $x'+y'\sqrt{d}=(x+y\sqrt{d})(x_0-y_0\sqrt{d})^n$. Since $x'+y'\sqrt{d}>1$ and $x'-y'\sqrt{d}=(x'+y'\sqrt{d})^{-1}$, we have $0<x'-y'\sqrt{d}<1$. Thus

$$x'=\frac{1}{2}((x'+y'\sqrt{d})+(x'-y'\sqrt{d}))>0,$$
$$y'=\frac{1}{2}((x'+y'\sqrt{d})-(x'-y'\sqrt{d}))>0.$$

Therefore (x',y') is a positive integer solution smaller than (x_0,y_0), which is a contradiction. □

6.5 Remark Another approach is using *Minkowski's theorem* (cf. § 4, Theorem (4.4)). This answer in Math.StackExchage provide a wonderful solution.

7 Show that the ring $\mathbb{Z}[\sqrt{2}]$ is Euclidean. Show furthermore that its units are given by $\pm(1+\sqrt{2})^n, n\in\mathbb{Z}$, and determine its prime elements.

Recall: A domain A is said to be ***Euclidean*** if it can be equipped with an ***Euclidean function*** $\delta(x)$. That is a function from A to $\mathbb{N}$ such that $\delta(\alpha)=0$ implies $\alpha=0$ and that for every $\alpha,\beta\in A,\beta\neq 0$, there exists $\kappa,\gamma\in A$ satisfying $\alpha=\kappa\beta+\gamma$ and $\delta(\gamma)<\delta(\beta)$.

Proof: To show $\mathbb{Z}[\sqrt{2}]$ is Euclidean, we prove that the absolute value of norm $|N(a+b\sqrt{2})|=|a^2-2b^2|$ is an *Euclidean function*. Notice that this function, when extended to $\mathbb{Q}(\sqrt{2})$, is a multiplicative homomorphism, thus we only need to show that for every $\alpha=a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$, there exists a

$\gamma = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that $|N(\alpha - \gamma)| < 1$. Note that, we can always choose integers x, y such that $|a - x| < \frac{1}{2}$ and $|b - y| < \frac{1}{2}$. But then one can see that such a pair of integers x, y already satisfies the required condition since $|(a - x)^2 - 2(b - y)^2| < |a - x|^2 + 2|b - y|^2 < 1$.

It is easy to check that $\pm(1+\sqrt{2})^n, n \in \mathbb{Z}$ are units of the ring $\mathbb{Z}[\sqrt{2}]$. To show they are the only units, it suffices to show that $1 + \sqrt{2}$ is the smallest unit whose coefficients are positive, which is obvious.

To determine all the prime elements, we proceed analogously to the case $\mathbb{Z}[i]$. See Proposition 7.6 below. □

Recall: An element p is said to be ***prime*** if the principal ideal (p) is a nonzero prime ideal. In an UFD, prime elements are precisely irreducible elements.

To go foreword to determine all the prime elements, we need a lemma.

7.1 Lemma *For a prime number $p > 2$, the diophantine equation*

$$a^2 - 2b^2 = p$$

has integer solutions if and only if $p \equiv 1$ or $7 \bmod 8$.

Proof: It is obvious that for every integers a, b, $a^2 - 2b^2$ cannot be 3 or 5 modulo 8. To see the "if", we only need to show such p is not a prime element in $\mathbb{Z}[\sqrt{2}]$. Then, let $p = \alpha\beta$, we get $N(\alpha)N(\beta) = N(p) = p^2$, thus $p = N(\alpha) = a^2 - 2b^2$, where $\alpha = a + b\sqrt{2}$.

To do this, we verify that the congruence $x^2 \equiv 2 \bmod p$ has solutions when $p \equiv 1$ or $7 \bmod 8$. If so, we have $p \mid x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. But both $\frac{x+\sqrt{2}}{p}$ and $\frac{x-\sqrt{2}}{p}$ are not in $\mathbb{Z}[\sqrt{2}]$, thus p can not be a prime element.

To show 2 is *quadratic residue modulo p*, i.e., congruence $x^2 \equiv 2 \bmod p$ has solutions, when $p \equiv 1$ or $7 \bmod 8$, we quote the *Legendre symbols* and *Gauss's lemma.* □

7.2 (Legendre symbol) An integer a is said to be ***quadratic residue modulo*** n if the congruence $x^2 \equiv a \bmod n$ has solutions. We define the ***Legendre symbol*** of a modulo n as follow

$$\left(\frac{a}{n}\right) := \begin{cases} 1 & \text{if } a \text{ is quadratic residue modulo } n \text{ and } a \not\equiv 0 \bmod p, \\ 0 & \text{if } a \equiv 0 \bmod p, \\ -1 & \text{if } a \text{ is quadratic nonresidue modulo } n. \end{cases}$$

7.3 Lemma *Let p be an odd prime number and a an integer. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof: We pair integers in the *positive residue system* $1, 2, \cdots, p-1$ as follow: if $xy \equiv a \bmod p$, we match x with y.

If a is quadratic residue, then there must be some x_0 in the positive residue system such that $x_0^2 \equiv a \bmod p$. Note that, in this case, the congruence $x^2 \equiv a \bmod p$ has exact two solutions in the positive residue system: x_0 and $p - x_0$. Thus the pairing provides $\frac{p-3}{2}$ pairs and two single elements, and their product gives rise to be

$$(p-1)! \equiv a^{\frac{p-3}{2}} x_0(p-x_0) \equiv -a^{\frac{p-1}{2}} \bmod p.$$

Since $(p-1)! \equiv -1 \bmod p$ (*Wilson's theorem*), we get $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

If a is quadratic nonresidue, then the pairing provides $\frac{p-1}{2}$ pairs, and their product gives rise to be

$$(p-1)! \equiv a^{\frac{p-1}{2}} \bmod p.$$

Thus $a^{\frac{p-1}{2}} \equiv -1 \bmod p$. In conclusion, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$.. □

Recall: The ***(positive) residue*** of an integer a modulo n is a positive integer x such that $x < n$ and $x \equiv a \bmod n$. The ***absolute residue*** of a modulo n is an integer between $-\frac{n}{2}$ and $\frac{n}{2}$ such that $x \equiv a \bmod n$.

7.4 Lemma (Gauss's lemma) *Let p be an odd prime number and a an that is coprime to p. Then*

$$\left(\frac{a}{p}\right) \equiv (-1)^{\mu} \bmod p,$$

here μ is the number of negative integers in the absolute residues *modulo p of $a, 2a, \cdots, \frac{p-1}{2}a$.*

Proof: Let $r_1, r_2, \cdots, r_\tau$ be all the positive integers in the absolute residues modulo p of $a, 2a, \cdots, \frac{p-1}{2}a$, while $s_1, s_2, \cdots, s_\mu$ the negative ones. Then $\tau + \mu = \frac{p-1}{2}$. Note that $r_1, r_2, \cdots, r_\tau, -s_1, -s_2, \cdots, -s_\mu$ are distinct, thus they are just a permutation of $1, 2, \cdots, \frac{p-1}{2}$. Therefore we have

$$r_1 r_2 \cdots r_\tau (-s_1)(-s_2) \cdots (-s_\mu) \equiv (\frac{p-1}{2})! \bmod p.$$

But

$$r_1 r_2 \cdots r_\tau s_1 s_2 \cdots s_\mu \equiv (\frac{p-1}{2})! a^{\frac{p-1}{2}} \bmod p.$$

Thus $a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \bmod p$. The result then follows from Lemma 7.3. □

7.5 Remark Using this Gauss's lemma, one can easily determine $\left(\frac{2}{p}\right)$. Indeed, the absolute residues modulo p of $2, 4, \cdots, p-1$ are $2, 4, \cdots, 2[\frac{p-1}{4}]$ and $2[\frac{p-1}{4}] - p, \cdots, -1$. Thus $\mu = \frac{p-1}{2} - [\frac{p-1}{4}]$ and we conclude $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - [\frac{p-1}{4}]} = (-1)^{\frac{p^2-1}{8}}$. In §8, Theorem (8.6) provides another proof this result.

7.6 Proposition *The prime elements π of $\mathbb{Z}[\sqrt{2}]$, up to associated elements, are given as follows.*

1. $\pi = \sqrt{2}$,
2. $\pi = a + b\sqrt{2}$ *with* $a^2 - 2b^2 = p, p \equiv 1, 7 \bmod 8, a > b\sqrt{2} > 0$,
3. $\pi = p, p \equiv 3, 5 \bmod 8$.

Here, p denotes a prime number of $\mathbb{Z}$.

Proof: Let π be a prime element. We factorize $N(\pi)$ into prime numbers, then π must divide one of them, say p. Then we have $N(\pi) \mid N(p) = p^2$, thus $N(\pi) = \pm p$ or $\pm p^2$. To determine π, it suffices to determine $a^2 - 2b^2 = p$: if it has no positive integer solutions, then $\pi = p$ is a prime element, this is case 3; if it has positive integer solution (a, b), then $\pi = a + b\sqrt{2}$ is a prime element, this is case 1 and 2. Then the results follow from Lemma 7.1. □

§ 2 Integrality

I Review

II Exercises

1 Is $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ an algebraic integer?

Proof: Let $\theta = \frac{3+2\sqrt{6}}{1-\sqrt{6}} = -\frac{3+2\cdot 6+5\sqrt{6}}{5} = -(3+\sqrt{6})$. Then one can see that θ is a solution of the integral equation $x^2+6x+3=0$, thus an algebraic integer. □

2 Show that, if the integral domain A is integrally closed, then so is the polynomial ring $A[t]$.

Proof: Let K be the fraction field of A. Then $K[t]$ is a PID, thus integrally closed (cf. Proposition 2.1 or 2.2). Note that $K(t)$ is the fraction field of both $A[t]$ and $K[t]$.

Let $f(t) \in K(t)$ be integral over $A[t]$, thus also over $K[t]$. Therefore we have $f(t) \in K[t]$ and there exist $a_{n-1}(t), \cdots, a_0(t) \in A[t]$ such that

$$f(t)^n + a_{n-1}(t)f(t)^{n-1} + \cdots + a_0(t) = 0.$$

Let m be an integer greater than degrees of $a_{n-1}(t), \cdots, a_0(t)$ and $f(t)$. By replacing $f(t)$ by $t^m - f(t)$, we may assume $f(t)$ is monic and then so is $-a_0(t)$. Then we have

$$f(t)\left(f(t)^{n-1} + a_{n-1}(t)f(t)^{n-2} + \cdots + a_1(t)\right) = -a_0(t).$$

Since both $-a_0(t)$ and $f(t)$ are monic, and $-a_0(t)$ is over A, a generalization of *Gauss's lemma* (cf. Lemma 2.4) shows that the coefficients of $f(t)$ are integral over A. Thus $f(t) \in A[t]$ since A is integrally closed. □

Note that PID = UFD $\cap$ Dedekind domain. Therefore, to show any PID is integrally closed, it suffices to prove either the following Proposition 2.1 or 2.2.

2.1 Proposition *Every unique factorization domain is integrally closed.*

Proof: Let A be a UFD. An element of the fraction field of A can be written as a/b with $a, b \in A$. If a/b is integral over A, then it satisfies an equation

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0.$$

By multiplying b^n, we get

$$a^n = -(a_{n-1}a^{n-1}b + \cdots + a_0b^n).$$

Since b divides the right side, we have $b \mid a^n$. Since no prime element of A divides both a and b, it follows that b must be a unit by unique factorization. Hence $a/b \in A$. □

2.2 Proposition *Every Dedekind domain is integrally closed.*

Proof: Let $\mathcal{O}$ be a Dedekind domain and r be a element of the fraction field of $\mathcal{O}$. If r is integral over $\mathcal{O}$, then there exists an integer n such that $r^n \in (r^{n-1}, r^{n-2}, \cdots, 1)$. Thus

$$\begin{aligned}(r,1)^n &= (r^n, r^{n-1}, r^{n-2}, \cdots, 1)\\ &= (r^{n-1}, r^{n-2}, \cdots, 1) = (r,1)^{n-1}.\end{aligned}$$

Since $\mathcal{O}$ is Dedekind, the ideal $(r,1)$ is invertible, thus we have $(r,1) = \mathcal{O}$, i.e., $r \in \mathcal{O}$. □

Recall the Gauss's lemma is

2.3 Lemma (Gauss's lemma) *Let A be a UFD, and K its fraction field. Let $f, g \in K[t]$ be monic polynomials such that g divides f. If $f \in A[t]$, then so is g.*

Since in our case A is just integrally closed not necessary a UFD, thus we need a generalization. Here it is

2.4 Lemma *Let A be a ring, and let B be an A-algebra. Let $f, g \in B[t]$ be monic polynomials such that g divides f. If the coefficients of f are integral over A, then so are those of g.*

Proof: Let A' be the A-subalgebra of B generated by the coefficients of f, then A' is integral over A. Consider the roots of f in the splitting field, they are integral over A', and thus also integral over A since the integrality is transitive (cf. §2, Proposition (2.4)). Note that roots of g are also roots of f, they are integral over A, thus so are the coefficients of g. □

Use this lemma, we can prove further the following by the same proof of Exercise 2.

2.5 Proposition *Let A be an integral domain, and let A' be its integral closure, then the integral closure of $A[t]$ is $A'[t]$.*

3 In the polynomial ring $A = \mathbb{Q}[X, Y]$, consider the principal ideal $\mathfrak{p} = (X^2 - Y^3)$. Show that $\mathfrak{p}$ is a prime ideal, but $A/\mathfrak{p}$ is not integrally closed.

Proof: To show $\mathfrak{p}$ is a prime ideal, it suffices to show $x^2 - Y^3$ is irreducible over $\mathbb{Q}$, which is obvious. To show $A/\mathfrak{p}$ is not integrally closed, we only need to see that the integral equation $T^2 - Y = 0$ has a solution $T = \frac{X}{Y}$ in the fraction field of $A/\mathfrak{p}$ but not in $A/\mathfrak{p}$. □

4 Let D be a square-free rational integer $\neq 0, 1$ and d the discriminant of the quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Show that

$$\begin{aligned} d &= D \quad \textbf{if } D \equiv 1 \bmod 4, \\ d &= 4D \quad \textbf{if } D \equiv 2 \textbf{ or } 3 \bmod 4, \end{aligned}$$

and that an integral basis of K is given by $\{1, \sqrt{D}\}$ in the second case, by $\{1, \frac{1}{2}(1 + \sqrt{D})\}$ in the first case, and by $\{1, \frac{1}{2}(d + \sqrt{d})\}$ in both case.

Proof: Let $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ be an algebraic integer, its minimal polynomial is $x^2 - 2ax + a^2 - Db^2$. Therefore, we have $2a \in \mathbb{Z}$ and $a^2 - Db^2 \in \mathbb{Z}$. If $a \in \mathbb{Z}$, then $Db^2 \in \mathbb{Z}$, thus $b \in \mathbb{Z}$ since D is square-free. If $a \notin \mathbb{Z}$, then $2a$ is odd, thus $D(2b)^2$ is an integer $\equiv 1 \bmod 4$. Since D is square-free, we have $2b \in \mathbb{Z}$ in this case. But then $(2b)^2 \equiv 1 \bmod 4$ thus D must $\equiv 1 \bmod 4$. From this discussion, we conclude that $\mathcal{O}_K = \mathbb{Z} + \frac{1}{2}(1 + \sqrt{D})\mathbb{Z}$ in the case $D \equiv 1 \bmod 4$ and $\mathcal{O}_K = \mathbb{Z} + \sqrt{D}\mathbb{Z}$ in the case $D \equiv 2$ or $3 \bmod 4$.

Now we calculate the discriminant d of K. Note that all the embeddings $K \to \mathbb{C}$ are the identity id and $\sigma\colon a + b\sqrt{D} \mapsto a - b\sqrt{D}$. In the case $D \equiv 1 \bmod 4$, we have

$$d = d(1, \frac{1}{2}(1 + \sqrt{D})) = \det \begin{pmatrix} 1 & \frac{1}{2}(1 + \sqrt{D}) \\ 1 & \frac{1}{2}(1 - \sqrt{D}) \end{pmatrix}^2 = D.$$

In the case $D \equiv 2$ or $3 \bmod 4$, we have

$$d = d(1, \sqrt{D}) = \det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^2 = 4D.$$

In both case, we have $\mathcal{O}_K = \mathbb{Z} + \frac{1}{2}(d + \sqrt{d})\mathbb{Z}$. □

Another prove is using the Proposition (2.12), from which we know that if the discriminant of a basis is quare-free, then it is an integral basis.

Recall (Discriminant): Let $A \subset B$ be an extension of rings, and assume B is free of rank m as an A-module. Let $\beta_1, \cdots, \beta_m$ be elements of B. The ***discriminant*** of this basis is

$$d(\beta_1, \cdots, \beta_m) = \det(\mathrm{Tr}_{B|A}(\beta_i\beta_j)).$$

One can check that $(\alpha, \beta) \mapsto \mathrm{Tr}_{B|A}(\alpha\beta)$ is a symmetric bilinear form, thus for $\gamma_j = \sum_i a_{ji}\beta_i, a_{ij} \in A$, we have

$$d(\gamma_1, \cdots, \gamma_m) = \det(a_{ij})^2 d(\beta_1, \cdots, \beta_m).$$

If both $\beta_1, \cdots, \beta_m$ and $\gamma_1, \cdots, \gamma_m$ are basis of B, then $\det(a_{ij})$ is a unit in A. Thus up to multiplication by the square of a unit of A, the discriminant is independent of the choice of the basis. We can then regard it as an element of A/A^{*2}, and call it the ***discriminant*** $d(B/A)$ of B over A.

4.1 Remark When $A = \mathbb{Z}$, the discriminant $d(B/A)$ a well-defined integer, because 1 is the only square of a unit in $\mathbb{Z}$. In this case, we will omit the base ring $\mathbb{Z}$ and just write $d(B)$.

When K is a number field of degree m over $\mathbb{Q}$, the ring of integers $\mathcal{O}_K$ in K is free of rank m over $\mathbb{Z}$, and so $d(\mathcal{O}_K)$ is a well-defined integer. In this case, $d(K/\mathbb{Q})$ is the element of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ represented by the integer $d(\mathcal{O}_K)$. We also denote this integer by d_K and call it the ***discriminant of the algebraic number field*** K,

More general, Let K be the field of fractions of A, and let L be an extension of K of degree m. If the integral closure B of A in L is free of rank m over A, then $d(B/A)$ represents $d(L/K)$. Moreover, $d(L/K) \neq 0$ if and only if $L|K$ is separable.

When $L|K$ is separable and A is a PID, then every finitely generated B-submodule M of L is a free A-module of rank m. In particular, B admits an *integral basis* over A. (§2, Proposition (2.10))

Let $\beta_1, \cdots, \beta_m$ be an integral basis of M over A, we have the discriminant $d(\beta_1, \cdots, \beta_m) \in A$. It is independent of the choice of the basis up to multiplication by the square of a unit of A. We can then regard it as an element of A/A^{*2}, and call it the ***discriminant*** $d(M/A)$ of M over A.

In the case $A = \mathbb{Z}$, the discriminant $d(M/A)$ a well-defined integer. We will omit the base ring $\mathbb{Z}$ and just write $d(M)$.

4.2 Proposition (§2, Proposition (2.12)) *If $\mathfrak{a} \subset \mathfrak{a}'$ are two nonzero finitely generated $\mathcal{O}_K$-submodules of K, then the index $(\mathfrak{a}' : \mathfrak{a})$ is finite and satisfies*

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}').$$

Proof: Let $\beta_1, \cdots, \beta_m$ be an integral basis of $\mathfrak{a}'$, then by the *fundamental theorem of finitely generated $\mathbb{Z}$-modules*, there exist integers $a_1, \cdots, a_m$ such that $a_i \mid a_{i+1}$ for $i = 1, \cdots, m-1$ and $a_1\beta_1, \cdots, a_m\beta_m$ form an integral basis of $\mathfrak{a}$. Moreover, $\mathfrak{a}'/\mathfrak{a} \cong \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_m)$. Thus $(\mathfrak{a}' : \mathfrak{a}) = a_1 a_2 \cdots a_m$.

Therefore, we have

$$d(\mathfrak{a}) = d(a_1\beta_1, \cdots, a_m\beta_m) = \det(T)^2 d(\beta_1, \cdots, \beta_m) = \det(T)^2 d(\mathfrak{a}').$$

Here, the base change matrix T is $\mathrm{diag}(a_1, a_2, \cdots, a_m)$, thus $\det(T) = a_1 a_2 \cdots a_m$. So $d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}')$. □

Proof (Another proof of Exercise 4): When $D \equiv 1 \bmod 4$, $d(1, \frac{1}{2}(1 + \sqrt{D})) = D$ is square-free, so everything is done. When $D \equiv 2$ or $3 \bmod 4$, $d(1, \sqrt{D}) = 4D$ is not square-free, but the index $(\mathcal{O}_K : \mathbb{Z}[\sqrt{D}]) \mid 4D$. Since D is square-free, $(\mathcal{O}_K : \mathbb{Z}[\sqrt{D}])$ must be 1 or 2. If the index equals 2, then $2\mathcal{O}_K \subset \mathbb{Z}[\sqrt{D}]$ and either $\frac{1}{2}, \frac{1}{2}\sqrt{D}$ or $\frac{1}{2}(1 + \sqrt{D})$ lies in D. However, the minimal polynomial of them are $X - \frac{1}{2}, X^2 - \frac{D}{4}$ and $X^2 - X + \frac{1}{4}(1 - D)$, none of them are integral, which is a contradiction. Therefore the index must equals 1 and $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. □

4.3 Remark Exercise 7 shows that the discriminant $d \equiv 0$ or $1 \bmod 4$, thus d must equals $4D$ when $D \equiv 2$ or $3 \bmod 4$.

5 Show that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{2})$.

Proof: Let's first calculate the discriminant of the basis $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$. Note that the embeddings $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ are $\sigma_1 = \mathrm{id}$, $\sigma_2 \colon \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$ and $\sigma_3 \colon \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$, where ω is the cube root of unity.

Then, we have

$$\begin{aligned} d(1, \sqrt[3]{2}, \sqrt[3]{2}^2) &= \det \begin{pmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{2}^2 \\ 1 & \sqrt[3]{2}\omega & \sqrt[3]{2}^2\omega^2 \\ 1 & \sqrt[3]{2}\omega^2 & \sqrt[3]{2}^2\omega \end{pmatrix}^2 \\ &= (\sqrt[3]{2} - \sqrt[3]{2}\omega)^2(\sqrt[3]{2}\omega - \sqrt[3]{2}\omega^2)^2(\sqrt[3]{2} - \sqrt[3]{2}\omega^2)^2 \\ &= 4(1-\omega)^2(\omega - \omega^2)^2(1-\omega^2)^2 \\ &= 4(1-\omega)^6 = 4(-3\omega)^3 = -108. \end{aligned}$$

So, by Proposition 4.2, $(\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}])^2 d_K = -108 = -2^2 \cdot 3^3$. Let denote the index by m. Then we have $m = 1, 2, 3$ or 6. By Exercise 7, we have $m = 1$ or 3. If $m = 3$, then $3\mathcal{O}_K \subset \mathbb{Z}[\sqrt[3]{2}]$ and there exists an element $\alpha = \frac{1}{3}(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)$ lies in $\mathcal{O}_K$ but not in $\mathbb{Z}[\sqrt[3]{2}]$. Moreover, we may assume $a, b, c \in \{0, -1, 1\}$. However, the minimal polynomials of α is

$$X^3 - aX^2 + \frac{1}{3}(a^2 - 2bc)X - \frac{1}{27}(a^3 + 2b^3 + 4c^3 - 6abc),$$

which is not integral in this case. Thus $m = 1$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. □

Another approach is using *Eisenstein polynomial.*

5.1 (Eisenstein polynomial) A polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ over $\mathbb{Z}$ is said to be ***Eisenstein with respect to*** p if $p \mid a_i$ for $1 \leqslant i \leqslant n-1$ and $p \parallel a_0$, i.e., $p \mid a_0$ but $p^2 \nmid a_0$.

5.2 Lemma *Let K be a number field of degree n, and $\alpha \in K$ a nonzero algebraic integer of degree n. Suppose the minimal polynomial of α is* Eisenstein *with respect to a prime p. Then p does not divide $(\mathcal{O}_K : \mathbb{Z}[\alpha])$.*

Proof: Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the minimal polynomial of α. Suppose $p \mid (\mathcal{O}_K : \mathbb{Z}[\alpha])$, then there exists some $\beta \in \mathcal{O}_K$ such that $p\beta \in \mathbb{Z}[\alpha]$ but $\beta \notin \mathbb{Z}[\alpha]$. We write

$$p\beta = b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0,$$

where $b_i \in \mathbb{Z}$ and not every b_i is divisible by p. Let j be the smallest index with $0 \leqslant j \leqslant n{-}1$ for which $p \nmid b_j$. Then we want to pick out the term $\frac{b_j}{p}$ to cause a contradiction.

To do this, we note that for those b_i divisible by p, we already have $\frac{b_i}{p}\alpha^i \in \mathcal{O}_K$. Thus we have

$$\gamma := \frac{b_{n-1}}{p}\alpha^{n-1} + \cdots + \frac{b_j}{p}\alpha^j = \beta - \frac{b_{j-1}}{p}\alpha^{j-1} - \cdots - \frac{b_0}{p} \in \mathcal{O}_K.$$

To drop the terms higher than j, we use the following trick: since $f(X)$ is Eisenstein, p divides every a_i, we thus get

$$\frac{1}{p}\alpha^n = -\frac{a_{n-1}}{p}\alpha^{n-1} - \cdots - \frac{a_0}{p} \in \mathcal{O}_K.$$

Therefore

$$\frac{b_j}{p}\alpha^{n-1} = \gamma\alpha^{n-j-1} - (b_{n-1}\alpha^{n-j-2} + \cdots + b_{j+1})\frac{1}{p}\alpha^n \in \mathcal{O}_K.$$

Then, we have $N_{K|\mathbb{Q}}(\frac{b_j}{p}\alpha^{n-1}) \in \mathbb{Z}$.

However,

$$N_{K|\mathbb{Q}}(\frac{b_j}{p}\alpha^{n-1}) = \frac{b_j^n}{p^n}N_{K|\mathbb{Q}}(\alpha)^{n-1} = \frac{b_j^n a_0^{n-1}}{p^n} \notin \mathbb{Z}$$

since $p \nmid b_j$ and $p^2 \nmid a_0$. This contradiction shows that $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$ as desired. □

Use this lemma, we can prove the desired result in another way:

Proof (Another approach to Exercise 5): Let $m = (\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}])$, we have $m^2 d_K = -108$ as previous. So $m = 1, 2, 3$ or 6. Thus we only need to show 2 and 3 do not divide m.

Note that the minimal polynomial of $\sqrt[3]{2}$ is $X^3 - 2$, which is Eisenstein with respect to 2, thus $2 \nmid m$. Now we set $\alpha = 1 + \sqrt[3]{2}$, so that $K = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\alpha)$. The minimal polynomial of α is $X^3 - 3X^2 + 3X - 3$, which is Eisenstein with respect to 3, thus $3 \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$. But $\mathbb{Z}[\alpha] = \mathbb{Z}[\sqrt[3]{2}]$, thus $3 \nmid m$. So we conclude that $m = 1$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. □

Another approach is doing at *local*. First, we point out that integrality is a *local property*. Here we need a lemma, that is easy to see.

5.3 Lemma *Let $A \subset B$ be an extension of rings and x an element of B that is integral over A. Then for every A-algebra C, $x \otimes 1 \in B \otimes_A C$ is integral over C.*

Since localization is a functor constructed by tensor, so we also have that for every multiplicatively closed subset S of A and an element integral over A in B, its imagine in $S^{-1}B$ is also integral over $S^{-1}A$.

5.4 Proposition (Integrality is a local property.) *Let $A \subset B$ be an extension of rings and x an element of B. Then the following are equivalent:*

1. *x is the integral over A;*
2. *$x \in S^{-1}B$ is the integral over $S^{-1}A$ for every multiplicatively closed subset S of A;*
3. *$x \in B_\mathfrak{p}$ is the integral over $A_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of A;*
4. *$x \in B_\mathfrak{m}$ is the integral over $A_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of A.*

Proof: Assume 4, we then get the minimal polynomials $f_\mathfrak{m}(t) \in A_\mathfrak{m}[t]$ of $x \in B_\mathfrak{m}$ for every $\mathfrak{m}$. By reduction to common denominators, we can lift every $f_\mathfrak{m}(t)$ into a polynomial $g_\mathfrak{m}(t) \in A[t]$ whose coefficient of leading term $a_\mathfrak{m} \notin \mathfrak{m}$. Since the collection of all $a_\mathfrak{m}$ generate whole A, we get the global polynomial by gluing those $g_\mathfrak{m}(t)$. □

5.5 Remark Another approach is using the fact the $x \in B$ is integral over A if and only if $A[x]$ is finitely generated A-module (§2, Proposition (2.2)), and that being finitely generated module is a local property.

Using Proposition 5.4, we can prove Exercise 5 as follow:

Proof (Another proof of Exercise 5): Let $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \in \mathcal{O}_K$, we need to show $a, b, c \in \mathbb{Z}$. The minimal polynomial of α is

$$X^3 - 3aX^2 + (a^2 - 2bc)X - (a^3 + 2b^3 + 4c^3 - 6abc).$$

By Proposition 5.4, α is also integral over $\mathbb{Z}_{(p)}$ for every prim number p. Note that the intersection of all $\mathbb{Z}_{(p)}$ in $\mathbb{Q}$ is $\mathbb{Z}$, thus we only need to deduce $a, b, c \in \mathbb{Z}_{(p)}$ from $3a, a^2 - 2bc, a^3 + 2b^3 + 4c^3 - 6abc \in \mathbb{Z}_{(p)}$, which is obverse for $p \neq 2, 3$. When $p = 2$, we can deduce $a \in \mathbb{Z}_{(2)}$ from $3a \in \mathbb{Z}_{(2)}$ and then deduce $2bc \in \mathbb{Z}_{(2)}$. Let's look at $a^3 + 2b^3 + 4c^3 - 6abc \in \mathbb{Z}_{(2)}$, thus $2b^3 + 4c^3 \in \mathbb{Z}_{(2)}$, from this and $2bc \in \mathbb{Z}_{(2)}$, we have $b, c \in \mathbb{Z}_{(2)}$. The reasoning for case $p = 3$ is similar but more circuitous. □

5.6 Remark The above proof can also be interpreted as first prove the conclusion for every localization (the integral closure of $\mathbb{Z}_{(p)}$ in $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}_{(p)}[\sqrt[3]{2}]$), then deduce the global result from the locals.

To formalize this approach, we need to show that being integral closure is a local property.

5.7 Proposition (Being integral closure is a local property.) *Let $A \subset B$ be an extension of rings and A' a A-subalgebra of B. Then the following are equivalent:*

1. *A' is the integral closure of A in B;*
2. *$S^{-1}A'$ is the integral closure of $S^{-1}A$ in $S^{-1}B$ for every multiplicatively closed subset S of A;*
3. *$A'_\mathfrak{p}$ is the integral closure of $A_\mathfrak{p}$ in $B_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of A;*
4. *$A'_\mathfrak{m}$ is the integral closure of $A_\mathfrak{m}$ in $B_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of A.*

Proof: *1⇒2*: By Proposition 5.4, $S^{-1}A'$ is contained in the integral closure of $S^{-1}A$ in $S^{-1}B$. Conversely, for every $\frac{b}{s} \in S^{-1}B$ integral over $S^{-1}A$, suppose its minimal polynomial is

$$X^n + \frac{a_{n-1}}{s_{n-1}}X^{n-1} + \cdots + \frac{a_0}{s_0} \in S^{-1}A[X].$$

Then one can see that $s_0 s_1 \cdots s_{n-1} b$ is integral over A, thus is contained in A'. So $\frac{b}{s} = \frac{s_0 s_1 \cdots s_{n-1} b}{s_0 s_1 \cdots s_{n-1} s} \in S^{-1}A'$ as desired.

2⇒3⇒4 is obverse.

4⇒1: For every element of A' its imagine in $B_\mathfrak{m}$ is contained in $A'_\mathfrak{m}$, thus is integral over $A_\mathfrak{m}$. By Proposition 5.4, those elements are contained in the integral closure of A in B.

Conversely, for every $b \in B$ integral over A, by Proposition 5.4, its imagines in $B_\mathfrak{m}$ is contained in the integral closure $A'_\mathfrak{m}$ of $A_\mathfrak{m}$ in $B_\mathfrak{m}$. Since we have $\frac{b}{1} \in A'_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of A, thus $b \in A'$ as desired. □

5.8 Proposition *Let D be a cube-free integer. Set $D = hk^2$, where h and k are square-free and $(h,k) = 1$. Set $\alpha = \sqrt[3]{D}$ and $K = \mathbb{Q}(\alpha)$. Then an integral basis for K is*

$$\begin{array}{ll} \{1, \alpha, \frac{1}{k}\alpha^2\} & \textit{if } D^2 \not\equiv 1 \bmod 9; \\ \{1, \alpha, \frac{1}{3k}(k^2 \pm k^2\alpha + \alpha^2)\} & \textit{if } D \equiv \pm 1 \bmod 9. \end{array}$$

6 Show that $\{1, \theta, \frac{1}{2}(\theta + \theta^2)\}$ is an integral basis of $\mathbb{Q}(\theta)$, $\theta^3 - \theta - 4 = 0$.

Proof: Let's first calculate the discriminant of the basis $\{1, \theta, \frac{1}{2}(\theta + \theta^2)\}$. Let $\sigma_1, \sigma_2, \sigma_3$ be all the embeddings $\mathbb{Q}(\theta) \to \mathbb{C}$ and $\theta_i = \sigma_i\theta$ for $i = 1, 2, 3$. Then we have

$$\begin{aligned} d(1, \theta, \frac{1}{2}(\theta + \theta^2)) &= \det \begin{pmatrix} 1 & \theta_1 & \frac{1}{2}(\theta_1 + \theta_1^2) \\ 1 & \theta_2 & \frac{1}{2}(\theta_2 + \theta_2^2) \\ 1 & \theta_3 & \frac{1}{2}(\theta_3 + \theta_3^2) \end{pmatrix}^2 \\ &= \frac{1}{4} \det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 \\ 1 & \theta_2 & \theta_2^2 \\ 1 & \theta_3 & \theta_3^2 \end{pmatrix}^2 \\ &= \frac{1}{4} \prod_{1 \leqslant i < j \leqslant 3} (\theta_i - \theta_j)^2 \\ &\overset{6.1}{=} \frac{1}{4}(-27(-4)^2 - 4(-1)^3) = -107, \end{aligned}$$

which is a prime number. Thus, by Proposition 4.2, $\{1, \theta, \frac{1}{2}(\theta + \theta^2)\}$ must be an integral basis. □

Recall: For a polynomial $f(X) \in K[X]$ with roots $\theta_1, \theta_2, \cdots, \theta_n$ in its split field, the ***discriminant*** of f is

$$\Delta(f) := \prod_{1 \leqslant i < j \leqslant n} (\theta_i - \theta_j)^2.$$

6.1 Proposition $\Delta(X^3 + aX + b) = -27b^2 - 4a^3$.

There are many ways to prove obtain this result, here we put two. The first one use a lemma from the theory of symmetric polynomials.

Recall (Weight): Let $X_1, x_2, \cdots, X_n$ be variables. the ***weight*** of a monomial $X_1^{v_1} X_2^{v_2} \cdots X_n^{v_n}$ is $v_1 + 2v_2 + \cdots + nv_n$. The weight of a polynomial is the maximum of the weights of its monomials.

6.2 Lemma ([Lan02, IV, Theorem 6.1]) *Let $f(t) \in A[t_1, t_2, \cdots, t_n]$ be symmetric and of degree d. Then there exists a polynomial $g(X_1, \cdots, X_n)$ of weight $\leqslant d$ such that*

$$f(t) = g(s_1, s_2, \cdots, s_n).$$

Here s_i is the i-th elementary symmetric polynomial of $t_1, t_2, \cdots, t_n$.

Proof (Proposition 6.1): Let $\theta_1, \theta_2, \theta_3$ be the roots of $f(X) = X^3 + aX + b$. The discriminant $\Delta(f)$ is a homogenous symmetric polynomial of $\theta_1, \theta_2, \theta_3$. Thus by Lemma 6.2, it should be a polynomial with weight 6 of the elementary symmetric polynomials of $\theta_1, \theta_2, \theta_3$. By *Vieta's formulas*, they are $s_1 = 0$, $s_2 = a$ and $s_3 = -b$. Thus $\Delta(f) = va^3 + wb^2$. To determine v and w, we only need to consider two special cases.

For $f(X) = X^3 - X$, we have $a = -1, b = 0$, thus $\Delta(f) = -v$. But the roots are $-1, 0, 1$, thus $\Delta(f) = 4$, so $v = -4$. For $f(X) = X^3 - 1$, we have $a = 0, b = -1$, thus $\Delta(f) = w$. But the roots are the third roots of unit, thus $\Delta(f) = -27$, so $w = -27$. Therefore, we conclude that $\Delta(f) = -27b^2 - 4a^3$. □

6.3 Proposition *The discriminant of the polynomial*

$$X^n + aX + b, \quad a, b \in K,$$

assumed to be irreducible and separable, is

$$\Delta(X^n + aX + b) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n).$$

Proof: Let $f(X) = X^n + aX + b$ and $\theta_1, \theta_2, \cdots, \theta_n$ are the roots of $f(X)$ in its split field. We have

$$\begin{aligned}\Delta(X^n + aX + b) &= \prod_{1 \leqslant i < j \leqslant n} (\theta_i - \theta_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{j \neq i} (\theta_i - \theta_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\theta_i) \\ &= (-1)^{\frac{n(n-1)}{2}} N_{L|K}(f'(\theta)).\end{aligned}$$

Here $N_{L|K}$ is the norm of the extension $L|K$ and θ is one of the roots.

Let $\gamma = f'(\theta) = n\theta^{n-1} + a$. Then we have $\theta = -\frac{nb}{\gamma + (n-1)a}$ and thus $K(\gamma) = K(\theta)$. If we write

$$f\left(\frac{-nb}{X + (n-1)a}\right) = \frac{P(X)}{Q(X)},$$

then $P(\gamma)/Q(\gamma) = f(\theta) = 0$ and so $P(\gamma) = 0$. Thus the minimal polynomial of γ is

$$P(X) = (X + (n-1)a)^n - na(X + (n-1)a)^{n-1} + (-n)^n b^{n-1}.$$

So

$$N_{L|K}(\gamma) = (-1)^n P(0) = (-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}.$$

and the desired formula follows directly. □

7 (Stickelberger's discriminant relation) The discriminant d_K of an algebraic number field K is always $\equiv 0$ or $1 \bmod 4$.

Proof: The determinant $\det(\sigma_i \alpha_j)$ of an integral basis $\alpha_1, \cdots, \alpha_m$ of $\mathcal{O}_K$ is a sum of terms, each of them is a product of a permutation of all embeddings acting on $\alpha_1, \cdots, \alpha_m$. Writing P, resp. $-N$, for the sum of the terms corresponding to even, resp. odd permutations, we have

$$d_K = (P - N)^2 = (P + N)^2 - 4PN.$$

Let G be the Galois group of the Galois closure of K over $\mathbb{Q}$. Note that every embeding of K can be extended to an element of G and vice versa, thus for every $\tau \in G$, $\tau\sigma_1, \cdots, \tau\sigma_m$ is just a permutation of $\sigma_1, \cdots, \sigma_m$. Therefore, depending on whether this permutation is even or not, we have either $\tau P = P, \tau N = N$ or $\tau P = N, \tau N = P$. Then $P + N$ and PN are fixed by G thus lie in $\mathbb{Q}$. Since they are integral over $\mathbb{Z}$, they must in fact be integers, from which it follows that

$$d_K \equiv (P + N)^2 \equiv 0 \text{ or } 1 \mod 4.$$ □

§ 3 Ideals

I Review

II Exercises

1 Decompose $33+11\sqrt{-7}$ into irreducible integral elements of $\mathbb{Q}(\sqrt{-7})$.

Proof: By Exercise 2.4, the ring of integers in $\mathbb{Q}(\sqrt{-7})$ is $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. In this ring, $33+11\sqrt{-7}$ can be first decomposed as:

$$33+11\sqrt{-7} = 11 \cdot 2 \cdot \frac{3+\sqrt{-7}}{2}.$$

Note that the norm of elements in $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ is

$$N\left(x+y(\frac{1+\sqrt{-7}}{2})\right) = (x+\frac{y}{2})^2 + 7(\frac{y}{2})^2.$$

We separate the proof step by steps.

Step 1. We now decompose 11 into irreducible elements: note that

$$N(11) = 121 = 11 \cdot 11.$$

Thus either 11 itself is irreducible or it can be decomposed into two irreducible elements α and β, each of them has norm 11. So we consider the equation

$$(x+\frac{y}{2})^2 + 7(\frac{y}{2})^2 = 11.$$

It has integral solutions $(1,2), (-3,2), (3,-2)$ and $(-1,-2)$, which are corresponding to the elements $2+\sqrt{-7}, -2+\sqrt{-7}, 2-\sqrt{-7}$ and $-2-\sqrt{-7}$.

Fortunately, those four elements are differed by a sign or a conjugate. Thus we get the decomposition

$$11 = 2+\sqrt{-7} \cdot 2-\sqrt{-7},$$

which is unique up to units.

Step 2. We similarly decompose 2 and $\frac{3+\sqrt{-7}}{2}$ into irreducible elements: since

$$N(2) = N\left(\frac{3+\sqrt{-7}}{2}\right) = 4 = 2 \cdot 2,$$

we consider the equation

$$(x+\frac{y}{2})^2 + 7(\frac{y}{2})^2 = 2.$$

It has integral solutions $(0,1),(-1,1),(0,-1)$ and $(1,-1)$, which are corresponding to the elements $\frac{1+\sqrt{-7}}{2}$, $\frac{-1+\sqrt{-7}}{2}$, $\frac{-1-\sqrt{-7}}{2}$ and $\frac{1-\sqrt{-7}}{2}$.

Fortunately, those four elements are differed by a sign or a conjugate. Thus we get the decomposition

$$2=\frac{1+\sqrt{-7}}{2}\cdot\frac{1-\sqrt{-7}}{2}, \text{ and } \frac{3+\sqrt{-7}}{2}=-\left(\frac{1-\sqrt{-7}}{2}\right)^2,$$

which are unique up to units.

Step 3. Therefore, we can decompose $33+11\sqrt{-7}$ as follows:

$$33+11\sqrt{-7}=-(2+\sqrt{-7})\cdot(2-\sqrt{-7})\cdot\frac{1+\sqrt{-7}}{2}\cdot\left(\frac{1-\sqrt{-7}}{2}\right)^3. \quad \square$$

2 Show that

$$54=2\cdot 3^3=\frac{13+\sqrt{-47}}{2}\cdot\frac{13-\sqrt{-47}}{2}$$

are two essentially different decompositions into irreducible integral elements of $\mathbb{Q}(\sqrt{-47})$.

Proof: Since both

$$\frac{13\pm\sqrt{-47}}{2\cdot 2} \text{ and } \frac{13\pm\sqrt{-47}}{2\cdot 3}$$

do not belong to the ring of integers in $\mathbb{Q}(\sqrt{-47})$, the numbers 2 and 3, *a fortiori* other nontrivial factors of $2\cdot 3^3$, are not associated to $\frac{13+\sqrt{-47}}{2}$ or $\frac{13-\sqrt{-47}}{2}$. The two factorizations are therefore essentially different. □

2.1 Remark They are not the only decompositions of 54, for instance, $54=3^2\cdot\frac{5+\sqrt{-47}}{2}\cdot\frac{5-\sqrt{-47}}{2}$ is another one.

3 Let d be square-free and p a prime number not dividing $2d$. Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$. Show that $(p)=p\mathcal{O}$ is a prime ideal of $\mathcal{O}$ if and only if the congruence $x^2\equiv d \bmod p$ has no solution.

Proof: We quote the terms in 1.7.2 of §1.1. By Exercise 2.4, the ring of integers $\mathcal{O}$ must be either $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

If d is *quadratic residue modulo* p, i.e. exists an integer x such that $x^2\equiv d \bmod p$. Then $p\mid x^2-d=(x+\sqrt{d})(x-\sqrt{d})$. However both $\frac{x+\sqrt{d}}{p}$ and $\frac{x-\sqrt{d}}{p}$ are not in $\mathcal{O}$ since $p\neq 2$. Therefore p is not a prime element.

Conversely, if d is not *quadratic residue modulo* p, then we will show that p is a prime element. To do this, consider two element $x_1 + y_1\sqrt{d}$ and $x_2+y_2\sqrt{d}$ of $\mathcal{O}$ and assume their product lies in (p). Since $p \neq 2$, thus $\frac{x}{p} \in \mathbb{Z}$ and $\frac{x}{p} \in \frac{1}{2}\mathbb{Z}$ are the same thing. Therefore, after change symbols, we may reduce to the case $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$. Then we can deduce from

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) \in (p)$$

that

$$p^2 = N(p) \mid N(x_1 + y_1\sqrt{d})N(x_2 + y_2\sqrt{d}).$$

Then p must divide one of $N(x_1 + y_1\sqrt{d})$ and $N(x_2 + y_2\sqrt{d})$, say the first one. Then we have

$$p \mid N(x_1 + y_1\sqrt{d}) = x_1^2 - dy_1^2,$$

and thus

$$x_1^2 \equiv dy_1^2 \bmod p.$$

Since d is not quadratic residue modulo p, y_1 should not be invertible modulo p, thus $p \mid y_1$ and x_1. Then $x_1 + y_1\sqrt{d} \in (p)$ as desired. □

4 A Dedekind domain with a finite number of prime ideals is a principal ideal domain.

Proof: We first prove the result for the case $\mathcal{O}$ has only one nonzero prime ideal $\mathfrak{p}$, e.g. when $\mathcal{O}$ is *local.* In this case, there exists an element $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then consider the ideal (π), it must be uniquely factorized as $(\pi) = \mathfrak{p}^\nu$ for some ν by Theorem (3.3) in this section. But $\pi \notin \mathfrak{p}^2$, thus $(\pi) = \mathfrak{p}$, which shows the only prime ideal of $\mathcal{O}$ is principal, thus so are all its ideals due to Theorem (3.3) again.

For the case $\mathcal{O}$ has finitely many prime ideals, let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be all the prime ideals. If $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r} \neq 0$ is an ideal, then chose $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. By the Chinese remainder theorem, there exists an element $a \in \mathcal{O}$ corresponding to the cosets $\pi_i^{\nu_i} \bmod \mathfrak{p}_i^{\nu_i+1}$. Consider the fraction $(a) = \mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_r^{\mu_r}$. Since $a \equiv \pi_i^{\nu_i} \bmod \mathfrak{p}_i^{\nu_i+1}$, $a \notin \mathfrak{p}_i^{\nu_i+1}$, thus $\mu_i \leqslant \nu_i$, and also $a \in \mathfrak{p}_i^{\nu_i}$, thus $\mu_i \geqslant \nu_i$. Therefore $(a) = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r} = \mathfrak{a}$ as desired. □

5 The quotient ring $\mathcal{O}/\mathfrak{a}$ of a Dedekind domain by an ideal $\mathfrak{a} \neq 0$ is a principal ideal domain.

5.1 Remark This result is wrong because $\mathcal{O}/\mathfrak{a}$ is not a domain in general. The correct result is: $\mathcal{O}/\mathfrak{a}$ is a ***principal ring***, that is a ring in which every ideal is principal.

Proof: We first prove the result for the case $\mathfrak{a} = \mathfrak{p}^n$. In this case, the only proper ideals of $\mathcal{O}/\mathfrak{a}$ are $\mathfrak{p}/\mathfrak{p}^n, \cdots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$. Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, then $\pi^i \mathcal{O}/\mathfrak{p}^n$ must be one of those $\mathfrak{p}^j/\mathfrak{p}^n$. Since $\pi^i \in \mathfrak{p}^i$ and $\pi^i \notin \mathfrak{p}^{i+1}$, we must have $i = j$ and so that every proper ideals in $\mathcal{O}/\mathfrak{a}$ is principal as desired.

For the general case, just note that the quotient ring of a PID is again a PID and use induction. □

Although the quotient of a Dedekind domain may not even be a domain, but the localization must be. In deed, we have:

5.2 Proposition (Dedekindness is a local property) *Let D be a domain, then the following are equivalent:*

1. *D is Dedekind;*
2. *D is Noetherian and $S^{-1}D$ is Dedekind for every multiplicatively closed subset S of D;*
3. *D is Noetherian and $D_{\mathfrak{p}}$ is Dedekind for every prime ideal $\mathfrak{p}$ of D;*
4. *D is Noetherian and $D_{\mathfrak{m}}$ is Dedekind for every maximal ideal $\mathfrak{m}$ of D.*

Proof: Recall that a domain is Dedekind if it is Noetherian, integrally closed, and every nonzero prime ideal is maximal. Since the prime ideals of $S^{-1}D$ correspond to prime ideals contained in $D \setminus S$ of D, the last condition is a local property. Then the conclusion follows from that being integrally closed is also a local property and that every localization of a Noetherian ring is again Noetherian. □

5.3 Remark When we say *Dedekindness is a local property*, we actually mean Proposition 5.2. In fact, it is NOT a local property in the *strict* sense. For example, the integral closure of $\mathbb{Z}$ in the field obtained by adjoining to $\mathbb{Q}$ the p-th roots of unity for all prime numbers p. However, this ring is not Noetherian, thus not Dedekind.

5.4 Remark The ring of all algebraic integers is integrally closed and in which every nonzero prime ideal is maximal. However, it is not Noetherian.

6 Every ideal of a Dedekind domain can be generated by two elements.

Proof: For every ideal $\mathfrak{a}$ of a Dedekind domain $\mathcal{O}$, consider an element $a \in \mathfrak{a}$ and the quotient ring $\mathcal{O}/(a)$. By Exercise 5, this quotient ring is principal, thus the image of $\mathfrak{a}$ in $\mathcal{O}/(a)$ is generated by $b \bmod (a)$ for some $b \in \mathfrak{a}$, thus $\mathfrak{a} = (a) + (b)$ as desired. □

So Dedekind domains are very close to PIDs, however, they are not the same thing. For example, $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain since it is the ring of integers in $\mathbb{Q}(\sqrt{5})$, but it is not a PID since it is not a UFD.

The class group can be used to measure the distance of a Dedekind domain from being PID. We have

6.1 Theorem *A Dedekind domain $\mathcal{O}$ is a PID if and only if its class group is trivial.*

Proof: In the case class group is trivial, every fractional ideal is principal, particularly, $\mathcal{O}$ is a PID. Conversely, if $\mathcal{O}$ is a PID, then for every fractional ideal $\mathfrak{a}$, there exists $c \in \mathcal{O}$ such that $c\mathfrak{a}$ is an ideal of $\mathcal{O}$, thus is principal, thus so is $\mathfrak{a}$ and therefore the class group is trivial. □

7 In a Noetherian ring R in which every prime ideal is maximal, each descending chain of ideals $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots$ becomes stationary.

7.1 Remark Note that the condition "every prime ideal is maximal" implies that the (0) must not be prime unless R is a field.

Proof: First, we prove that in a Noetherian ring, (0) has a *prime decomposition* $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. One can see that the Lemma (3.4) in this section actually holds for every proper ideals, including (0), of a Noetherian ring. Thus we have $(0) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$. But $(0) = \{0\}$, thus $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$.

Moreover, $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ are the all prime ideals. Indeed, if they are not, then there exists another prime ideal $\mathfrak{q}$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r = (0) \subset \mathfrak{q}$. Thus one of those prime ideals, say $\mathfrak{p}_1$ must be contained in $\mathfrak{q}$. But every prime ideal is maximal, thus $\mathfrak{p}_1 = \mathfrak{q}$, a contradiction.

Therefore, we have a descending chain of ideals

$$R \supset \mathfrak{p}_1 \supset \mathfrak{p}_1\mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = (0).$$

Each factor $\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}/\mathfrak{p}_1 \cdots \mathfrak{p}_i$ is a vector space over the field $R/\mathfrak{p}_i$. For a vector space V, the chain conditions are equivalent to $\dim V$ is finite. Therefore $\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}/\mathfrak{p}_1 \cdots \mathfrak{p}_i$ is Noetherian if and only if it is Artinian, as $R/\mathfrak{p}_i$-modules thus R-modules. Repeated application of Lemma 7.2, we see that R is Noetherian if and only if it is Artinian. □

7.2 Lemma *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of R-modules. Then M is Noetherian (resp. Artinian) if and only if both M' and M'' are Noetherian (resp. Artinian).*

Proof: For the "if", note that a chain (M_i) of submodules of M would be controlled by its inverse image (M_i') in M' and image (M_i'') in M'' by the Five-Lemma:

$$\begin{tikzcd}
0 \arrow[r] & M_i' \arrow[r] \arrow[d, "f_i'"'] & M_i \arrow[r] \arrow[d, "f_i"'] & M_i'' \arrow[r] \arrow[d, "f_i''"'] & 0 \\
0 \arrow[r] & M_{i+1}' \arrow[r] & M_{i+1} \arrow[r] & M_{i+1}'' \arrow[r] & 0
\end{tikzcd}$$

Indeed, for large i, the inclusions f_i' and f_i'' become identities, thus so is f_i.

For the "only if", just note that a chain of submodules of M' or M'' would give rise to a chain of submodules of M, hence is stationary. □

Proof (Another proof of Exercise 7): Another approach is using the concept of *composition series.*

7.3 **(Composition series)** A ***composition series*** of a R-module M is a chain of submodules of M

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

such that no extra submodules can be inserted into this strict inclusion chains. One can see that if a module has a composition series, then all its composition series have same length (called the ***length*** of M) and any chain of submodules of M can be extended into a composition series. (cf. [AM94])

7.4 **Proposition** *M has a composition series if and only if M is both Noetherian and Artinian.*

Proof: If M has a composition, then every chain of submodules of M has bounded length, hence M is both Noetherian and Artinian.

If M is both Noetherian and Artinian, we construct a composition series of M as follow. Since $M_0 = M$ is Noetherian, it has a maximal submodule M_1. Similarly, M_1 has a maximal submodule M_2. keep going we get a descending chain: $M = M_0 \supset M_1 \supset M_2 \supset \cdots$, which must be finite since M is also Artinian. Thus we get a composition series. □

7.5 **Corollary** *For a vector space V, the followings are equivalent:*

1. *V has finite dimension;*
2. *V has finite length;*
3. *V is Noetherian;*
4. *V is Artinian.*

Applying this result to the our case, one can see that the vector space $\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}/\mathfrak{p}_1 \cdots \mathfrak{p}_i$ has finite length, but the subspaces of it are one-one corresponding to the ideals between $\mathfrak{p}_1 \cdots \mathfrak{p}_i$ and $\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}$, therefore the chain $R \supset \mathfrak{p}_1 \supset \mathfrak{p}_1\mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = (0)$ can be extended into a composition series, hence R is Artinian. □

8 Let $\mathfrak{m}$ be a nonzero integral ideal of the Dedekind domain $\mathcal{O}$. Show that in every ideal class of Cl_K, there exists an integral ideal prime to $\mathfrak{m}$.

Although not necessary, we still quote some details of the theory of Dedekind domain here to prepare our proof.

First, we generalize the result of Theorem (3.3) as follow (which is actually Corollary 3.9)

8.1 Theorem *Every nonzero fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ admits a unique factorization*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}},$$

where $\mathfrak{p}$ take over all nonzero prime ideals of $\mathcal{O}$ and all but finite number of the integers $\operatorname{ord}_{\mathfrak{p}}$ are zero.

Proof: Let $c \in \mathcal{O}$ be the element such that $c\mathfrak{a} \in \mathcal{O}$. Then we have unique factorization $(c) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and $c\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$. Hence

$$\mathfrak{a} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}\mathfrak{q}_1 \cdots \mathfrak{q}_r.$$

combine the repeated prime ideals we get the desired decomposition. □

8.2 (Order) For a nonzero fractional ideal $\mathfrak{a}$ of $\mathcal{O}$, such an integer $\operatorname{ord}_{\mathfrak{p}}$ in the factorization is called the ***order*** of $\mathfrak{a}$ at $\mathfrak{p}$. If $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a} > 0$, we say that $\mathfrak{a}$ has a ***zero*** at $\mathfrak{p}$. If $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a} < 0$, we say that it has a ***pole*** at $\mathfrak{p}$.

For a nonzero element $c \in K$, regarding it as the principal fractional ideal $(c) := c\mathcal{O}$, we may apply the notions of *order*, *zero* and *pole* to c.

When $\operatorname{ord}_{\mathfrak{p}} c = 0$, we can see immediately that c becomes a unit in the local ring $\mathcal{O}_{\mathfrak{p}}$. Therefore, we say c is a ***unit*** at $\mathfrak{p}$.

The following proposition is an immediate consequence of the *Chinese remainder theorem.*

8.3 Proposition *Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be prime ideals of a Dedekind domain $\mathcal{O}$, then for every integers $\nu_1, \cdots, \nu_r$, there exists an element $x \in \mathcal{O}$ such that* $\operatorname{ord}_{\mathfrak{p}_i} x = \nu_i$.

Use this proposition, the proof of the exercise is straightforward.

Proof (of Exercise 8): It suffices to show that for every two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$, there exist some $c \in K$ such that $c\mathfrak{a}$ is prime to $\mathfrak{b}$.

Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be all the distinct prime ideals containing $\mathfrak{b}$. Then by Proposition 8.3, there exists a $c_1 \in \mathcal{O}$ such that $\operatorname{ord}_{\mathfrak{p}_i} c_1 = \operatorname{ord}_{\mathfrak{p}_i} \mathfrak{a}$, hence $\operatorname{ord}_{\mathfrak{p}_i} c_1^{-1}\mathfrak{a} = 0$ for $1 \leqslant i \leqslant r$.

However, this $c_1^{-1}\mathfrak{a}$ may not be an integral ideal. If so, let $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ be all the prime ideals containing c_1 and different from $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$. By Proposition 8.3, there exists a $c_2 \in \mathcal{O}$ such that $\operatorname{ord}_{\mathfrak{p}_i} c_2 = 0$ for $1 \leqslant i \leqslant r$ and $\operatorname{ord}_{\mathfrak{q}_j} c_2 = \operatorname{ord}_{\mathfrak{q}_j} c_1$ for $1 \leqslant j \leqslant s$. Then $c_2 c_1^{-1}\mathfrak{a}$ is an integral ideal since and is prime to $\mathfrak{b}$. □

8.4 Remark (discrete valuation) The *order* at a prime ideal $\mathfrak{p}$ induces a ***discrete valuation*** on K, that is a function

$$v \colon K \longrightarrow \mathbb{Z} \cup \{\infty\}$$

such that for every $x, y \in K$,

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x+y) \geqslant \min\{v(x), v(y)\}$.

Once we have a discrete valuation on a field K, we get a subring

$$\mathcal{O}_{K,v} := \{x \in K | v(x) \geqslant 0\}.$$

Such kind of rings are called ***discrete valuation rings***.

In the case $v = \operatorname{ord}_{\mathfrak{p}}$, one can check that $\mathcal{O}_{K,v}$ is nothing but the localization $\mathcal{O}_{\mathfrak{p}}$. It is a PID since its only prime ideal is $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$.

8.5 Proposition *Discrete valuation rings = localizations of Dedekind rings.*

Proof: One has seen that localizations of Dedekind rings are discrete valuation rings. Conversely, one can see that for a discrete valuation ring $\mathcal{O}_{K,v}$ the only maximal ideal is

$$\mathfrak{m}_v := \{x \in K | v(x) \geqslant 1\}.$$

Let π be a ***uniformizing parameter*** in the sense that $v(\pi) = 1$. Then for any $x \in \mathcal{O}_{K,v}$, one has $v(x\pi^{-v(x)}) = 0$. Therefore any element of $\mathcal{O}_{K,v}$ is of the form $\varepsilon\pi^n$ with $\varepsilon \in \mathcal{O}_{K,v}^*$. Then any ideal of $\mathcal{O}_{K,v}$ is of the form $\mathfrak{m}_v^n$ and thus $\mathcal{O}_{K,v}$ is a PID. □

9 Let $\mathcal{O}$ be an integral domain in which all nonzero ideals admit a unique factorization into prime ideals. Show that $\mathcal{O}$ is a Dedekind domain.

The notion of *fractional ideals* can be extended to general integral domain R. A R-submodule M of K, the fraction field of R, is said to be a ***fractional ideal***, if there exists a nonzero $r \in R$ such that $rM \subset R$. In this sense, the integral ideals are always fractional ideals. From the context, we know that every finitely generated R-submodule of K is a fractional ideal, and the converse is true if we assume R is Noetherian.

For a R-submodule M of K, we can define M^{-1} as the set

$$M^{-1} := (R : M) = \{x \in K | xM \in R\}.$$

It is a fractional ideal and we have $MM^{-1} \subset R$ in general. If moreover $MM^{-1} = R$, then we say M is ***invertible***.

Proof: Before we start the proof, we need two general observations.

9.1 Lemma *Let $\mathfrak{a}$ be an ideal in an integral domain R. If $\mathfrak{a}$ can be factored as a product of invertible prime ideals, then the factorization is unique.*

Proof: Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_m = \mathfrak{q}_1 \cdots \mathfrak{q}_n$ are two such factorizations of $\mathfrak{a}$. We may assume $\mathfrak{q}_1$ is minimal among $\mathfrak{q}_i$. Since $\mathfrak{a} \subset \mathfrak{q}_1$, there must be some $\mathfrak{p}_i \subset \mathfrak{q}_1$, we may assume it is $\mathfrak{p}_1$. Similarly, $\mathfrak{q}_j \subset \mathfrak{p}_1$ for some j, thus $\mathfrak{q}_j \subset \mathfrak{p}_1 \subset \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is minimal, we must have $\mathfrak{q}_j = \mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying by $\mathfrak{p}_1^{-1}$, we get $\mathfrak{p}_2 \cdots \mathfrak{p}_m = \mathfrak{q}_2 \cdots \mathfrak{q}_n$. Then the conclusion follows by induction. □

9.2 Lemma *Let R be an integral domain and let $x \neq 0$ in K, its fraction field. Suppose that (x) can be written as a product $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ of fractional ideals. Then each $\mathfrak{a}_i$ is invertible.*

Proof: Indeed, $x^{-1}\mathfrak{a}_1 \cdots \mathfrak{a}_{i-1}\mathfrak{a}_{i+1} \cdots \mathfrak{a}_n$ is the inverse of $\mathfrak{a}_i$. □

Now, let's go back to our situation. To show $\mathcal{O}$ is Dedekind, the crucial step is the following:

9.3 Proposition *Every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ is maximal.*

Proof: We separate the proof into two steps:

Step 1. We first prove the result for *invertible* prime ideals $\mathfrak{p}$.

To do this, we only need to show that for every $a \in \mathcal{O} \setminus \mathfrak{p}$, $(a) + \mathfrak{p} = \mathcal{O}$. If not, then we can write $\mathfrak{p} + (a)$ and $\mathfrak{p} + (a^2)$ as products $\mathfrak{p}_1 \cdots \mathfrak{p}_m$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_n$ of prime ideals. Let b be the image of a im $\mathcal{O}/\mathfrak{p}$, then we have

$$(b) = \mathfrak{p}_1/\mathfrak{p} \cdots \mathfrak{p}_m/\mathfrak{p}, \quad \text{and} \quad (b^2) = \mathfrak{q}_1/\mathfrak{p} \cdots \mathfrak{q}_n/\mathfrak{p}.$$

By Lemma 9.2, each $\mathfrak{p}_i/\mathfrak{p}$ and $\mathfrak{q}_j/\mathfrak{p}$ is invertible. Then we can apply Lemma 9.1 to the following

$$(\mathfrak{p}_1/\mathfrak{p})^2 \cdots (\mathfrak{p}_m/\mathfrak{p})^2 = \mathfrak{q}_1/\mathfrak{p} \cdots \mathfrak{q}_n/\mathfrak{p},$$

and get that $n = 2m$ and each $\mathfrak{p}_i/\mathfrak{p}$ appears twice among the $\mathfrak{q}_j/\mathfrak{p}$. Note that $\mathfrak{p}$ is contained in each $\mathfrak{p}_i/\mathfrak{p}$ and $\mathfrak{q}_j/\mathfrak{p}$, thus we also have that each $\mathfrak{p}_i$ appears twice among the $\mathfrak{q}_j$. Hence $(a^2) + \mathfrak{p} = ((a) + \mathfrak{p})^2$. Then

$$\mathfrak{p} \subset (a^2) + \mathfrak{p} = ((a) + \mathfrak{p})^2 \subset (a) + \mathfrak{p}^2.$$

So, if $p \in \mathfrak{p}$, then $p = ax + y$ with $x \in \mathcal{O}$ and $y \in \mathfrak{p}^2$. Hence $ax \in \mathfrak{p}$, and since $a \notin \mathfrak{p}$, then $x \in \mathfrak{p}$. Thus $\mathfrak{p} \subset a\mathfrak{p} + \mathfrak{p}^2 \subset \mathfrak{p}$, and so $\mathfrak{p} = \mathfrak{p}((a) + \mathfrak{p})$. Since $\mathfrak{p}$ is invertible, $\mathcal{O} = (a) + \mathfrak{p}$ as desired.

Step 2. Now, we prove that every non-zero prime ideal $\mathfrak{p}$ is invertible.

Let $a \in \mathfrak{p}$ and $a \neq 0$. Then $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ with each $\mathfrak{p}_i$ prime. By Lemma 9.2 and *Step 1*, they are invertible and thus maximal. Since $(a) \subset \mathfrak{p}$, we must have $\mathfrak{p}_i \subset \mathfrak{p}$ for some i. Then $\mathfrak{p} = \mathfrak{p}_i$ is invertible. □

From the above proof, we know that in $\mathcal{O}$, every nonzero prime ideal is maximal and invertible. This is actually another equivalent definition of Dedekind domain. To see this, let's introduce some more properties about *invertible ideals.* So we consider a general integral domain R for now.

9.4 Proposition *Invertible ideals are finitely generated.*

Proof: for since $MM^{-1} = R$, we have $\sum x_i y_i = 1$ for some $x_i \in M$ and $y_i \in M^{-1}$ $(1 \leqslant i \leqslant n)$. Hence for every $x \in M$, $x = \sum (y_i x) x_i$, and since each $y_i x \in R$, then M is generated by $x_1, \cdots, x_n$. □

9.5 Proposition (Invertibility is a local property) *Let M be a submodule of K, then the following are equivalent:*

1. *M is an invertible ideal;*

2. *M is finitely generated and $S^{-1}M$ is an invertible ideal for every multiplicatively closed subset S of R;*

3. *M is finitely generated and $M_{\mathfrak{p}}$ is an invertible ideal for every prime ideal $\mathfrak{p}$ of R;*

4. *M is finitely generated and $M_{\mathfrak{m}}$ is an invertible ideal for every maximal ideal $\mathfrak{m}$ of R.*

Proof: Before proof, we give three remarks:

1. It is easy to see that localization operation commutes with the products of fractional ideals.

2. The fraction field of $S^{-1}R$ is again K, so we can regard all localizations as subrings of K.

3. For M a finitely generated R-submodule M of K, the localization $S^{-1}M^{-1}$ of M^{-1} is $(S^{-1}M)^{-1} = \{x \in K | x(S^{-1}M) \subset S^{-1}R\}$.

   Proof: First, $S^{-1}M^{-1} \subset (S^{-1}M)^{-1}$. Indeed, for every $\frac{x}{s} \in S^{-1}M^{-1}$, we have $\frac{x}{s}S^{-1}M = S^{-1}(xM) \subset S^{-1}R$. To show the converse, consider any $z \in (S^{-1}M)^{-1}$. Let $x_1, \cdots, x_n$ be a system of generators of M. Then, for every i, we have $z \cdot \frac{x_i}{1} \in S^{-1}R$, and thus there exists s_i such that $s_i z x_i \in R$. Let $s = s_1 \cdots s_n$, then $szx_i \in R$ for every i, thus $sz \in M^{-1}$. Then $z = \frac{sz}{s} \in S^{-1}M^{-1}$. □

Note that in both *1, 2, 3* and *4*, M is finitely generated, thus we may always assume M is finitely generated. Then, by the above remarks, the proposition becomes to say that the identity $MM^{-1} = R$ holds if and only if it holds locally, which is true since localization preserves identity. □

9.6 Remark Invertibility is NOT a *strict* local property since one can see the condition "finitely generated" is necessary. Remark 5.3 has already provide an counterexample.

Now, we go back to our situation. So $\mathcal{O}$ is an integral domain in which all nonzero ideals admit a unique factorization into prime ideals, and we now also know that its every nonzero prime ideal is maximal and invertible.

9.7 Proposition *$\mathcal{O}$ is Notherian.*

Proof: Since every nonzero ideal admits a unique factorization into prime ideals and every nonzero prime ideal is invertible, then every nonzero ideal is invertible and thus finitely generated since Proposition 9.4. Therefore $\mathcal{O}$ is Noetherian. □

Now the only problem is to show $\mathcal{O}$ is integrally closed. To do this, we first consider the local case.

9.8 Proposition *Assume $\mathcal{O}$ is local, then it is integrally closed.*

Proof: It suffices to show $\mathcal{O}$ is a PID. Moreover, it suffices to show the only prime ideal $\mathfrak{m}$ is principal. First, there exists an element $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then consider the ideal (π), it admits a unique factorization $(\pi) = \mathfrak{p}^\nu$ for some ν. But $\pi \notin \mathfrak{p}^2$, thus $(\pi) = \mathfrak{p}$ as desired. □

Combined Propositions 9.3, 9.7 and 9.8, we have

9.9 Theorem *Assume $\mathcal{O}$ is local, then it is a Dedekind domain.*

Now we have proved the result for local case. For the global case, let $\mathfrak{p}$ any prime ideal of $\mathcal{O}$. Since ideals of $\mathcal{O}_\mathfrak{p}$ correspond to ideals of $\mathcal{O}$ contained in $\mathfrak{p}$, all nonzero ideals of $\mathcal{O}_\mathfrak{p}$ admit a unique factorization into prime ideals. Thus, by Theorem 9.9, $\mathcal{O}_\mathfrak{p}$ is a Dedekind domain. By Proposition 9.7, $\mathcal{O}$ is Noetherian, thus by Proposition 5.2, we have

9.10 Theorem *$\mathcal{O}$ is a Dedekind domain.*

9.11 Remark Combined with context, we have proved that for an integral domain $\mathcal{O}$ the following are equivalent:

DD1 $\mathcal{O}$ is Noetherian, integrally closed and every nonzero prime ideal is maximal;

DD2 Every nonzero fractional ideal of $\mathcal{O}$ is invertible;

DD3 Every nonzero ideal admits a unique factorization into primes.

10 The fractional ideals $\mathfrak{a}$ of a Dedekind domain $\mathcal{O}$ are projective $\mathcal{O}$-modules, i.e., given any surjective homomorphism $f\colon M \to N$ of $\mathcal{O}$-modules, each homomorphism $g\colon \mathfrak{a} \to N$ can be lifted to a homomorphism $h\colon \mathfrak{a} \to M$ such that $f \circ h = g$.

(The following can refer [Lan02] or my collection of solutions to its exercise.)

Recall: Let P be a module over a ring R, then the following are equivalent.

P1 Given a homomorphism $f\colon P \longrightarrow M''$ and surjective homomorphism $g\colon M \longrightarrow M''$, there exist a homomorphism $h\colon P \longrightarrow M$ make the following diagram commutative.

$$\begin{tikzcd}
& P \arrow[dl, "h"'] \arrow[d, "f"] & \\
M \arrow[r, "g"'] & M'' \arrow[r] & 0
\end{tikzcd}$$

P2 Every exact sequence $0 \longrightarrow M' \longrightarrow M'' \longrightarrow P \longrightarrow 0$ splits.

P3 There exists a module M such that $P \oplus M$ is free, or in words, P is a direct summand of a free module.

P4 The functor $M \mapsto \operatorname{Hom}_R(P, M)$ is exact.

If any of those condition holds, we say P is a ***projective module***. We omit the proof of this conclusion.

Note that in a Dedekind domain, fractional ideals are finitely generated torsion-free $\mathcal{O}$-modules. So we prove the following

10.1 Proposition *Every finitely generated torsion-free $\mathcal{O}$-module is projective.*

Proof: By the structure theorem of modules over PID ([Lan02, III, Theorem 7.3]), every finitely generated torsion-free module over a PID is free, *a fortiori* projective.

Let M be a finitely generated torsion-free $\mathcal{O}$-module, and $\mathfrak{p}$ a prime ideal, then the localized module $M_\mathfrak{p}$ is finitely generated and torsion-free over $\mathcal{O}_\mathfrak{p}$. Thus $M_\mathfrak{p}$ is projective.

To show M is projective, we use P3. Let F be finite free over $\mathcal{O}$, and $f\colon F \to M$ be a surjective homomorphism, then $f_\mathfrak{p}\colon F_\mathfrak{p} \to M_\mathfrak{p}$ admits a splitting $g_\mathfrak{p}\colon M_\mathfrak{p} \to F_\mathfrak{p}$. Since $g_\mathfrak{p}(M)$ is finitely generated, there exists $c_\mathfrak{p} \in \mathcal{O}$ such that $c_\mathfrak{p} \notin \mathfrak{p}$ and $c_\mathfrak{p} g_\mathfrak{p}(M) \subset F$. Moreover, the family $\{c_\mathfrak{p}\}$ generates the unit ideal $\mathcal{O}$: if not then $\{c_\mathfrak{p}\}$ generates an proper ideal hence belongs to some maximal ideal $\mathfrak{m}$, but $c_\mathfrak{m} \notin \mathfrak{m}$ which is a contradiction. So there is a finite number of elements $c_{\mathfrak{p}_i}$ and elements $x_i \in \mathcal{O}$ such that $\sum x_i c_{\mathfrak{p}_i} = 1$. Let

$$g = \sum x_i c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}$$

Then $g\colon M \to F$ is a homomorphism, and $f \circ g = f \circ (\sum x_i c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}) = \sum x_i f \circ c_{\mathfrak{p}_i} g_{\mathfrak{p}_i} = \sum x_i c_{\mathfrak{p}_i} f_{\mathfrak{p}_i} \circ g_{\mathfrak{p}_i} = \sum x_i c_{\mathfrak{p}_i} \mathrm{id}_{\mathfrak{p}_i} = \mathrm{id}$. □

We will give more properties about projective modules over Dedekind domain.

10.2 Proposition (Steinitz theorem) *Let $\mathfrak{a}, \mathfrak{b}$ be ideals, then there is an isomorphism:*

$$\mathfrak{a} \oplus \mathfrak{b} \xrightarrow{\cong} \mathcal{O} \oplus \mathfrak{a}\mathfrak{b}$$

Proof: Assume $\mathfrak{a}, \mathfrak{b}$ are relatively prime. Then $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$ and $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$. Consider the canonical map from $\mathfrak{a} \oplus \mathfrak{b}$ to $\mathfrak{a} + \mathfrak{b}$, we get the following exact sequence:

$$0 \longrightarrow \mathfrak{a}\mathfrak{b} \longrightarrow \mathfrak{a} \oplus \mathfrak{b} \longrightarrow \mathcal{O} \longrightarrow 0$$

Since $\mathcal{O}$ is a free $\mathcal{O}$-module, $\mathfrak{a} \oplus \mathfrak{b} \cong \mathcal{O} \oplus \mathfrak{a}\mathfrak{b}$.

As for the general case, thanks to Exercise 8, there exists some $c \in K$ such that $c\mathfrak{a}$ is relatively prime to $\mathfrak{b}$. Hence we have

$$\mathfrak{a} \oplus \mathfrak{b} \cong c\mathfrak{a} \oplus \mathfrak{b} \cong \mathcal{O} \oplus c\mathfrak{a}\mathfrak{b} \cong \mathcal{O} \oplus \mathfrak{a}\mathfrak{b}.$$ □

10.3 Proposition *Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals, and let $f\colon \mathfrak{a} \to \mathfrak{b}$ be an isomorphism (as $\mathcal{O}$-modules, of course). Then f has an extension to a K-linear map $f_K\colon K \to K$. Let $c = f_K(1)$. Then $\mathfrak{b} = c\mathfrak{a}$ and f is given by the mapping $m_c\colon x \mapsto cx$.*

Proof: We only need to show that for every $x \in \mathfrak{a}$, $x^{-1}f(x)$ is a constant c, then we can safely define $f_K(x) = cx$ and check it is a K-linear map and an extension of f. This is true since for every two $x, y \in \mathfrak{a}$, we have $yf(x) = f(xy) = xf(y)$, thus $x^{-1}f(x) = y^{-1}f(y)$. □

10.4 Remark This shows that isomorphic fractional ideals are differed by a principal fractional ideal, thus *the ideal classes in Cl_K are precisely the isomorphic classes.*

10.5 Corollary *Let $\mathfrak{a}$ be a fractional ideal. For each $b \in \mathfrak{a}^{-1}$ the map $m_b\colon \mathfrak{a} \to \mathcal{O}$ is an element of the dual $\mathfrak{a}^\vee = \mathrm{Hom}(\mathfrak{a}, \mathcal{O})$, and $\mathfrak{a}^{-1} \cong \mathfrak{a}^\vee$ under this corresponding, and so $\mathfrak{a}^{\vee\vee} \cong \mathfrak{a}$.*

Proof: The map $b \mapsto m_b$ is clearly injective and an $\mathcal{O}$-homomorphism. It suffices to show that it is surjective. For every $f \in \mathfrak{a}^\vee$, by Proposition 10.3, there exists some $c \in K$ such that $f = m_c$ and $c\mathfrak{a} \subset \mathcal{O}$. Since $\mathfrak{a}^{-1} = \{c \in K | c\mathfrak{a} \subset \mathcal{O}\}$, we have $c \in \mathfrak{a}^{-1}$. □

10.6 Proposition *Let M be a projective finite module over the Dedekind ring $\mathcal{O}$. Then there exist free modules F and F' such that $F \supset M \supset F'$, and F, F' have the same rank, which is called the* **rank** *of M. Moreover, there exists a basis $\{e_1, \cdots, e_n\}$ of F and ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ of $\mathcal{O}$ such that $M = \mathfrak{a}_1 e_1 + \cdots + \mathfrak{a}_n e_n$, or in other words, $M = \bigoplus \mathfrak{a}_i$.*

Proof: Let $x_1, \cdots, x_n$ generated M, then there exists a maximal linear independent subterm, say $x_1, \cdots, x_k$, then $F' = \langle x_1, \cdots, x_k \rangle \subset M$. For every $x_i, k < i \leqslant n$, assume that $a_i x_i \in F'$ with $a_i \in \mathcal{O}$, then let $c = a_{k+1}^{-1} \cdots a_n^{-1}$, we get $x_i \in F = \langle cx_1, \cdots, cx_k \rangle$ for every $1 \leqslant i \leqslant n$. Hence $F' \subset M \subset F$ and $\mathrm{rank}(F) = \mathrm{rank}(F')$.

Let $p_i\colon F \to \mathcal{O}$ be the projection from F to its i-th coefficient, then $p_i(M) = \mathfrak{a}_i$ is an ideal of $\mathcal{O}$. It is then clear that $M = \mathfrak{a}_1 e_1 \cdots + \mathfrak{a}_n e_n$. □

10.7 (Grothendieck group) The isomorphic classes of projective finite modules over a ring R form an abelian monoid whose addition is defined by

$$[M] + [N] := [M \oplus N].$$

We define an equivalence relation (which is called ***stably isomorphic***) $\sim$ on this abelian monoid as follow: $M \sim M'$ when there exist finite free modules F, F' such that $M \oplus F \cong M' \oplus F'$. Under this equivalence relation we obtain another monoid denoted by $K_0(R)$. It is easy to check this $K_0(R)$ is the group completion of the above monoid, so we call it the ***Grothendieck group*** of R.

10.8 Theorem *Let M be a projective finite module over the Dedekind ring $\mathcal{O}$. Then $M \cong \mathcal{O}^{n-1} \oplus \mathfrak{a}$ with n its rank and $\mathfrak{a}$ an ideal of $\mathcal{O}$, and he association $M \mapsto \mathfrak{a}$ induces isomorphism of the Grothendieck group $K_0(\mathcal{O})$ with the ideal class group Cl_K.*

Proof: By Propositions 10.2 and 10.6, $M \cong \mathcal{O}^{n-1} \oplus \mathfrak{a}$ with n its rank and $\mathfrak{a}$ an ideal of $\mathcal{O}$, and the map $M \mapsto \mathfrak{a}$ is a homomorphism. Since every ideal is a projective finite module, the map is clearly surjective. It suffices to show that if $M \cong \mathcal{O}^n \oplus \mathfrak{a}$, $N \cong \mathcal{O}^m \oplus \mathfrak{b}$ and $[\mathfrak{a}] = [\mathfrak{b}]$ in Cl_K, then $[M] = [N]$ in $K_0(\mathcal{O})$.

$[\mathfrak{a}] = [\mathfrak{b}]$ means there exists a some $c \in K$ such that $\mathfrak{b} = c\mathfrak{a}$. Then $N \cong \mathcal{O}^m \oplus c\mathfrak{a} \cong \mathcal{O}^{m-1} \oplus c\mathcal{O} \oplus \mathfrak{a} \cong \mathcal{O}^m \oplus \mathfrak{a}$. Hence there exist free modules F and F' such that $M \oplus F \cong \mathcal{O}^r \oplus \mathfrak{a} \cong N \oplus F'$, which means $[M] = [N]$ in $K_0(\mathcal{O})$. □

§ 4 Lattices

I Review

II Exercises

1 Show that a lattice Γ in $\mathbb{R}^n$ is complete if and only if the quotient $\mathbb{R}^n/\Gamma$ is compact.

Proof: If Γ is complete, then the fundamental mesh Φ has the property that $\Phi + \Gamma = \mathbb{R}^n$. Note that the projection $\pi : \mathbb{R}^n \to \mathbb{R}^n/\Gamma$ maps compact sets to compact sets, and that the image of Φ and $\Phi + \Gamma$ under this projection are the same, thus $\mathbb{R}^n/\Gamma$ is compact.

Conversely, if Γ is not complete, let V_0 be the subspace of $\mathbb{R}^n$ generated by Γ. Then there exists some $v \in \mathbb{R}^n \setminus V_0$ and thus $\pi|_{\mathbb{R}v}$ is injective. Since π is a quotient map of topological group thus is open, $\pi|_{\mathbb{R}v}$ is an open embedding. Thus $\mathbb{R}^n/\Gamma$ must not be compact. □

2 Show that Minkowski's Lattice Point Theorem cannot be improved, by giving an example of a centrally symmetric convex set $X \subset V$ such that $\operatorname{vol}(X) = 2^n \operatorname{vol}(\Gamma)$ which does not contain any nonzero point of the lattice Γ. If X is compact, however, then the statement (4.4) does remain true in the case of equality.

Proof: For example, consider the lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$, one can see that the set $X = (-1,1) \times (-1,1)$ is centrally symmetric convex and has volume 4. However, it contains no nonzero lattice point.

For the second part, we use the same approach of Theorem (4.4). First, it suffices to show that there exists two distinct lattice points $\gamma_1, \gamma_2 \in \Gamma$ such that

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \varnothing.$$

Indeed, if so, then $\gamma_1 - \gamma_2$ will belong to $X \cap \Gamma$.

When X is compact, if the sets $\frac{1}{2}X + \gamma$ are pairwise disjoint, then we must have:

$$\operatorname{vol}(\Phi) > \sum_{\gamma\in\Gamma} \operatorname{vol}(\Phi \cap (\frac{1}{2}X + \gamma)).$$

Since the set $(\Phi - \gamma) \cap \frac{1}{2}X$ has the same volume with $\Phi \cap (\frac{1}{2}X + \gamma)$, and $\Phi - \gamma, \gamma \in \Gamma$ cover the entire space V, we obtain:

$$\operatorname{vol}(\Phi) > \sum_{\gamma\in\Gamma} \operatorname{vol}((\Phi - \gamma) \cap \frac{1}{2}X) = \operatorname{vol}(\frac{1}{2}) = \frac{1}{2^n} \operatorname{vol}(X),$$

which contradicts the hypothesis. □

3 (Minkowski's theorem on linear forms) Let

$$L_i(x_1, \cdots, x_n) = \sum_{j=1}^{n} a_{ij} x_j, \quad i = 1, \cdots, n,$$

be real linear forms such that $\det(a_{ij}) \neq 0$**, and let** $c_1, \cdots, c_n$ **be positive real numbers such that** $c_1 \cdots c_n > |\det(a_{ij})|$**. Show that there exist integers** $m_1, \cdots, m_n \in \mathbb{Z}$ **such that**

$$|L_i(m_1, \cdots, m_n)| < c_i, \quad i = 1, \cdots, n.$$

Proof: Consider the lattice $\Gamma = \mathbb{Z}^n$ in $\mathbb{R}^n$. Then we have $\operatorname{vol}(\Gamma) = 1$. Consider the following subset

$$X = \left\{(x_1, \cdots, x_n) \in \mathbb{R}^n \middle| |L_i(x_1, \cdots, x_n)| < c_i, i = 1, \cdots, n\right\}.$$

We know that the volume of $X_0 = \prod_{i=1}^{n}(-c_i, c_i)$ is $2^n c_1 \cdots c_n$ and it is obtained by applying transformation $(L_1, \cdots, L_n)$ to X, therefore

$$\operatorname{vol}(X) = \left|\det(\frac{\partial L_i}{\partial x_j})\right|^{-1} \operatorname{vol}(X_0) = |\det(a_{ij})|^{-1} 2^n c_1 \cdots c_n > 2^n = 2^n \operatorname{vol}(\Gamma).$$

Hence, by Minkowski's Lattice Point Theorem, X must contain a nonzero lattice point $(m_1, \cdots, m_n)$. □

§ 5 Minkowski Theory

I Review

II Exercises

1 Write down a constant A which depends only on K such that every integral ideal $\mathfrak{a} \neq 0$ of K contains an element $a \neq 0$ satisfying

$$|\tau a| < A(\mathcal{O}_K : \mathfrak{a})^{1/n},$$

with $n = [K : \mathbb{Q}]$ and for all $\tau \in \operatorname{Hom}(K, \mathbb{C})$.

Proof: Let $A = \sqrt[n]{(\frac{2}{\pi})^s \sqrt{|d_K|}}$, then $c_\tau = A(\mathcal{O}_K : \mathfrak{a})^{1/n}$ satisfies the conditions of Theorem (5.3), hence there exists an element $a \neq 0$ satisfying

$$|\tau a| < A(\mathcal{O}_K : \mathfrak{a})^{1/n},$$

for all $\tau \in \operatorname{Hom}(K, \mathbb{C})$. □

2 Show that the convex, centrally symmetric set

$$X = \left\{ (z_\tau) \in K_{\mathbb{R}} \middle| \sum_\tau |z_\tau| < t \right\}$$

has volume $\operatorname{vol}(X) = 2^r \pi^s \frac{t^n}{n!}$ (see chap. III, (2.15)).

Proof: The image of X in $\mathbb{R}^{r+2s}$ is

$$f(X) = \left\{ (x_\tau) \in \prod_\tau \mathbb{R} \middle| \sum_\rho |x_\rho| + 2 \sum_\sigma \sqrt{x_\sigma^2 + x_{\bar{\sigma}}^2} < t \right\}.$$

For simplify notations, we substitute $x_i, i = 1, \cdots, r$, instead of x_ρ, and $y_j, z_j, j = 1, \cdots, s$, instead of $x_\sigma, x_{\bar{\sigma}}$. Then $\operatorname{vol}(f(X))$ is computed by the integral

$$I(t) = \int_{f(X)} dx_1 \cdots dx_r dy_1 \cdots dy_s dz_1 \cdots dz_s.$$

Passing to polar coordinate $y_j = u_j \cos\theta_j, z_j = u_j \sin\theta_j$, we get

$$I(t) = \int u_1 \cdots u_s dx_1 \cdots dx_r du_1 \cdots du_s d\theta_1 \cdots d\theta_s.$$

where the integral is taken over the domain

$$\begin{cases} |x_1| + \cdots + |x_r| + 2u_1 + \cdots + 2u_s < t, & \\ 0 \leqslant u_j, & j = 1, \cdots, s, \\ 0 \leqslant \theta_j \leqslant 2\pi, & j = 1, \cdots, s. \end{cases}$$

Substituting $2u_j = w_j$, we get

$$I(t) = 2^r 4^{-s} (2\pi)^s I_{r,s}(t)$$

where the integral

$$I_{r,s}(t) = \int w_1 \cdots w_s dx_1 \cdots dx_r dw_1 \cdots dw_s$$

is taken over the domain

$$\begin{cases} x_1 + \cdots + x_r + w_1 + \cdots + w_s < t, & \\ 0 \leqslant x_i, & i = 1, \cdots, r, \\ 0 \leqslant w_j, & j = 1, \cdots, s. \end{cases}$$

Clearly $I_{r,s}(t) = t^n I_{r,s}(1)$. By Fubini's theorem, we get

$$\begin{aligned} I_{r,s}(1) &= \int_0^1 I_{r-1,s}(1 - x_1) dx_1 \\ &= \int_0^1 (1 - x_1)^{n-1} I_{r-1,s}(1) dx_1 \\ &= \frac{1}{n} I_{r-1,s}(1). \end{aligned}$$

By induction,

$$I_{r,s}(1) = \frac{1}{n(n-1)\cdots(n-r+1)} I_{0,s}(1).$$

In the same way, we get

$$I_{0,s}(1) = \int_0^1 w_1 (1 - w_1)^{2s-2} I_{0,s-1}(1) dw_1 = \frac{1}{2s(2s-1)} I_{0,s-1}(1),$$

and hence

$$I_{0,s}(1) = \frac{1}{(2s)!} I_{0,0}(1) = \frac{1}{(2s)!}.$$

Therefore, $I_{r,s}(1) = \frac{1}{n!}$ and so

$$\operatorname{vol}(X) = 2^s \operatorname{vol}(f(X)) = 2^s 2^r 4^{-s} (2\pi)^s t^n I_{r,s}(1) = \frac{2^r \pi^s}{n!} t^n. \qquad \square$$

3 Show that in every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists an $a \neq 0$ such that

$$|N_{K|\mathbb{Q}}(a)| \leqslant M(\mathcal{O}_K : \mathfrak{a}),$$

where $M = \frac{n!}{n^n}(\frac{4}{\pi})^s \sqrt{|d_K|}$ (the so-called *Minkowski bound*).

Proof: Consider the compact, convex, centrally symmetric set

$$X = \left\{ (z_\tau) \in K_\mathbb{R} \middle| \sum_\tau |z_\tau| \leqslant n(M(\mathcal{O}_K : \mathfrak{a}))^{1/n} \right\}$$

which has volume

$$\operatorname{vol}(X) = \frac{2^r \pi^s}{n!} n^n \left(\frac{n!}{n^n} (\frac{4}{\pi})^s \sqrt{|d_K|} \right) (\mathcal{O}_K : \mathfrak{a}) = 2^n \operatorname{vol}(\Gamma).$$

By Exercise 4.2, it contains a nonzero element of $\Gamma = j\mathfrak{a}$, thus there exists an $a \neq 0$ in $\mathfrak{a}$ such that

$$\begin{aligned} |N_{K|\mathbb{Q}}(a)| &= \prod_\tau |\tau(a)| \\ &\leqslant \left(\frac{1}{n} \sum_\tau |\tau(a)| \right)^n \\ &\leqslant M(\mathcal{O}_K : \mathfrak{a}). \end{aligned}$$

□

§ 6 The Class Number

I Review

II Exercises

1 How many integral ideals $\mathfrak{a}$ are there with the given norm $\mathfrak{N}(\mathfrak{a}) = n$?

Proof: If $\mathfrak{N}(\mathfrak{a}) = n$, then $(n) \subset \mathfrak{a}$, therefore $\mathfrak{a}$ is a factor of the ideal (n). Factorize (n) into primes:

$$(n) = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r},$$

and assume the *inertia degree* of $\mathfrak{p}_i$ over a prime number p_i is f_i. For an ideal containing (n), we must have

$$\mathfrak{a} = \mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_r^{\mu_r}$$

for some $\mu_i \leqslant \nu_i$ and its norm is $\mathfrak{N}(\mathfrak{a}) = p_1^{f_1\mu_1} \cdots p_r^{f_r\mu_r}$. (Warning: those p_i may be repeated.)

$\mathfrak{N}((n)) = |N_{K|\mathbb{Q}}(n)|$ is a power of n, say n^k. Assume $n = q_1^{t_1} \cdots q_s^{t_s}$. Then $\sum\limits_{\mathfrak{p}_i|(q_j)} f_i\nu_i = kt_j$ and $\sum\limits_{\mathfrak{p}_i|(q_j)} f_i\mu_i = t_j$. One can then deduce the number of such kind of ideal $\mathfrak{a}$ from above conditions. □

2 Show that the quadratic fields with discriminant 5, 8, 13, −3, −4, −7, −8, −11 have class number 1.

In the original exercise, the where I write 13 is indeed 11. But it should be a flaw since there is no quadratic field with discriminant 11.

Proof: Recall that proof of Theorem (6.3) combined with Exercise 5.3 shows that each class of Cl_K contains an integral ideal with absolute norm no greater than the *Minkowski bound* $M = \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d_K|}$.

Recall that the discriminant d_K of quadratic field $K = \mathbb{Q}(\sqrt{D})$ with square-free integer D is given by

$$\begin{aligned} d_K &= D && \text{if } D \equiv 1 \bmod 4, \\ d_K &= 4D && \text{if } D \equiv 2 \text{ or } 3 \bmod 4. \end{aligned}$$

When $d_K > 0$, K is real, thus $s = 0$ and $M = \frac{1}{2}\sqrt{|d_K|}$. When $d_K < 0$, K is not real, thus $s = 1$ and $M = \frac{2}{\pi}\sqrt{|d_K|}$.

In the case $d_K = 5, 8, 13, -3, -4, -7, -8$, $M < 2$, therefore each class of Cl_K contains an integral ideal with absolute norm 1. But the only ideal with absolute norm 1 is $\mathcal{O}_K$ itself. So the class number $h_K = 1$.

In the case $d_K = -11$, $2 < M < 3$. We know that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ in this case. But as the proof of Exercise 1 shows, the ideals with absolute norm 2 must contain (2). On the other hand, 2 is obviously invertible in $\mathcal{O}_K$, thus $(2) = \mathcal{O}_K$. Hence there are no ideal with absolute norm 2. So the class number $h_K = 1$. □

3 Show that in every ideal class of an algebraic number field K of degree n, there exists an integral ideal $\mathfrak{a}$ such that

$$\mathfrak{N}(\mathfrak{a}) \leqslant \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d_K|}.$$

Proof: This is nothing but part of the proof of Theorem (6.3) combined with Exercise 5.3. chose an arbitrary representative $\mathfrak{a}$ of the class $[\mathfrak{a}] \in Cl_K$, and a nonzero $\gamma \in \mathcal{O}_K$ such that $\mathfrak{b} = \gamma\mathfrak{a}^{-1}$ is integral. Then, by Exercise 5.3, there exists a nonzero $\alpha \in \mathfrak{b}$ such that

$$|N_{K|\mathbb{Q}}(\alpha)| \leqslant \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d_K|}\mathfrak{N}(\mathfrak{b}).$$

Then $\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$ and its absolute norm

$$\mathfrak{N}(\mathfrak{a}) \leqslant \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|d_K|}.$$

□

4 (Minkowski's theorem on the discriminant) Show that the absolute value of the discriminant $|d_K|$ is > 1 for every algebraic number field $K \neq \mathbb{Q}$. (cf. chap. III, (2.17))

Proof: Since the absolute norm $\mathfrak{N}(\mathfrak{a})$ must $\geqslant 1$, thus by Exercise 3, we must have

$$\sqrt{|d_K|} \geqslant \frac{n^n}{n!}(\frac{\pi}{4})^s \geqslant \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}.$$

Let $a_n = \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}$, then

$$\frac{a_{n+1}}{a_n} = \left(1 + \frac{1}{n}\right)^n (\frac{\pi}{4})^{1/2} > 1$$

and $a_2 = \frac{\pi}{2} > 1$. Therefore $|d_K| > 1$. □

5 Show that the absolute value of the discriminant $|d_K|$ tends to ∞ with the degree n of the field.

Proof: Same as Exercise 4, we get

$$\sqrt{|d_K|} \geqslant \frac{n^n}{n!}(\frac{\pi}{4})^{n/2} =: a_n.$$

To show $|d_K|$ tends to ∞ with the degree n of the field, we only need to show the sequences a_n tends to ∞ with n.

Indeed, we have

$$\frac{a_{n+1}}{a_n} = \left(1 + \frac{1}{n}\right)^n (\frac{\pi}{4})^{1/2} > \sqrt{\pi} > 1.$$

Hence $a_{n+1} > \pi^{n/2} a_1$, which tends to ∞ with the degree n. □

6 Let $\mathfrak{a}$ be an integral ideal of K and $\mathfrak{a}^m = (a)$. Show that $\mathfrak{a}$ becomes a principal ideal in the field $L = K(\sqrt[m]{a})$, in the sense that $\mathfrak{a}\mathcal{O}_L = (\alpha)$.

Proof: Note that in a Dedekind domain, if for two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ one have $\mathfrak{a}^m = \mathfrak{b}^m$ for some positive integer m, then the unique factorization property implies $\mathfrak{a} = \mathfrak{b}$.

In our case, it is obviously that $(\mathfrak{a}\mathcal{O}_L)^m = \mathfrak{a}^m\mathcal{O}_L = a\mathcal{O}_L = (\sqrt[m]{a}\mathcal{O}_L)^m$. Therefore $\mathfrak{a}\mathcal{O}_L = \sqrt[m]{a}\mathcal{O}_L$ is principal. □

7 (Hilbert class field) Show that, for every number field K, there exists a finite extension L such that every ideal of K becomes a principal ideal.

Proof: Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ be a system of representatives of classes of Cl_K and h be the class number of K. Then $\mathfrak{a}_1^h, \cdots, \mathfrak{a}_n^h$ are principal, say $(a_1), \cdots, (a_n)$. Then by Exercise 6, $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ becomes principal in $L = K(\sqrt[h]{a_1}, \cdots, \sqrt[h]{a_n})$.

For an ideal $\mathfrak{b} \in [\mathfrak{a}_i]$, there exists $x \in K$ such that $\mathfrak{b} = x\mathfrak{a}_i$. Then

$$\mathfrak{b}^h = x^h \mathfrak{a}_i^h = (x^h a_i),$$

and thus $\mathfrak{b}\mathcal{O}_L = x\sqrt[h]{a_i}\mathcal{O}_L$ is a principal fractional ideal. On the other hand, since $\mathfrak{b}$ is integral, so is $\mathfrak{b}\mathcal{O}_L$. This proves that every ideals of K becomes principal in L. □

§ 7 Dirichlet's Unit Theorem

I Review

II Exercises

1 Let $D > 1$ be a squarefree integer and d the discriminant of the real quadratic number field $K = \mathbb{Q}(\sqrt{D})$ (cf. Exercise 2.4). Let x_1, y_1 be the uniquely determined rational integer solution of the equation

$$x^2 - dy^2 = -4,$$

or - in case this equation has no rational integer solutions - of the equation

$$x^2 - dy^2 = 4,$$

for which $x_1, y_1 > 0$ are as small as possible. Then

$$\varepsilon_1 = \frac{x_1 + y_1\sqrt{d}}{2}$$

is a fundamental unit of K. (The pair of equations $x^2 - dy^2 = \pm 4$ is called *Pell's equation.*)

Proof: By Exercise 2.4, the ring of integers of K is $\mathcal{O}_K = \mathbb{Z} + \frac{d+\sqrt{d}}{2}\mathbb{Z}$. For $\alpha = u + v\frac{d+\sqrt{d}}{2} \in \mathcal{O}_K$, its norm is $N(\alpha) = (u + \frac{vd}{2})^2 - d(\frac{v}{2})^2$. Thus the units of $\mathcal{O}_K$ correspond to the solutions of $x^2 - dy^2 = \pm 4$ via

$$u + v\frac{d+\sqrt{d}}{2} \longleftrightarrow \begin{cases} x = 2u + vd, \\ y = v. \end{cases}$$

Therefore, ε_1 is a unit. It remains to show that it is the fundamental unit. For real quadratic field K, $r = 1, s = 0$, hence $\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}$. Hence the smallest positive unit of K greater than 1 must be a fundamental unit. A positive unit $u + v\frac{d+\sqrt{d}}{2} > 1$ corresponds the solution $x = 2u + vd, y = v$, Therefore ε_1 or ε_1^{-1} is a fundamental unit, hence so is the other one.

As for the sign of ±4, if the solution (x_1, y_1) is for equation $x^2 - dy^2 = 4$, then one can see that $x^2 - dy^2 = -4$ has no integral solutions since the norm of $\pm\varepsilon_1^n$ must be 1. □

2 Check the following table of fundamental units ε_1 for $\mathbb{Q}(\sqrt{D})$:

D	2	3	5	6	7	10
ε_1	$1+\sqrt{2}$	$2+\sqrt{3}$	$(1+\sqrt{5})/2$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$

Proof: By Exercise 1, we only need to find the smallest positive y such that $dy^2 \pm 4$ is a square number x^2, where d is the discriminant of $\mathbb{Q}(\sqrt{D})$, by Exercise 2.4, it is

$$\begin{aligned} d &= D && \text{if } D \equiv 1 \bmod 4, \\ d &= 4D && \text{if } D \equiv 2 \text{ or } 3 \bmod 4. \end{aligned}$$

For $\mathbb{Q}(\sqrt{2})$, $d = 8$. When $y = 1$, $dy^2 - 4 = 4 = 2^2$, hence $\varepsilon_1 = \frac{2+\sqrt{8}}{2} = 1 + \sqrt{2}$ is a fundamental unit.

For $\mathbb{Q}(\sqrt{3})$, $d = 12$, When $y = 1$, $dy^2 + 4 = 16 = 4^2$, hence $\varepsilon_1 = \frac{4+\sqrt{12}}{2} = 2 + \sqrt{3}$ is a fundamental unit.

For $\mathbb{Q}(\sqrt{5})$, $d = 5$, When $y = 1$, $dy^2 - 4 = 1 = 1^2$, hence $\varepsilon_1 = \frac{1+\sqrt{5}}{2}$ is a fundamental unit.

For $\mathbb{Q}(\sqrt{6})$, $d = 24$, When $y = 2$, $dy^2 + 4 = 100 = 10^2$, hence $\varepsilon_1 = \frac{10+2\sqrt{24}}{2} = 5 + 2\sqrt{6}$ is a fundamental unit.

For $\mathbb{Q}(\sqrt{7})$, $d = 28$, When $y = 3$, $dy^2 + 4 = 256 = 16^2$, hence $\varepsilon_1 = \frac{16+3\sqrt{28}}{2} = 8 + 3\sqrt{7}$ is a fundamental unit.

For $\mathbb{Q}(\sqrt{10})$, $d = 40$, When $y = 1$, $dy^2 - 4 = 36 = 6^2$, hence $\varepsilon_1 = \frac{6+\sqrt{40}}{2} = 3 + \sqrt{10}$ is a fundamental unit. □

3 The Battle of Hastings(October 14, 1066)

"The men of Harold stood well together, as their wont was, and formed thirteen squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter their redoubts; for a single blow of a Saxon war-hatched would break his lance and cut through his coat of mail... When Harold threw himself into the fray the Saxons were one mighty square of men, shouting the battle-cries, 'Ut!', 'Olicrosse!', 'Godemite!'." [Fictitious historical text, following essentially problem no. 129 in: H.E. Dundeney, *Amusements in Mathematics*, 1917 (Dover reprints 1958 and 1970).]

Question. How many troops does this suggest Harold II had at the battle of Hastings?

Proof: Let y^2 be the number of men in each square of Saxons before Harold threw himself into the fray. Then according to the text, we know the number of troops Harold had is $13y^2$ and $13y^2 + 1$ is a square, say x^2.

Consider the subring $\mathbb{Z}[\sqrt{13}]$ of the ring $\mathcal{O}$ of integers of $\mathbb{Q}(\sqrt{13})$, one can see the integral solutions (x, y) of the equation $x^2 - 13y^2 = 1$ corresponds to the units $\varepsilon = x + y\sqrt{13}$ of $\mathbb{Z}[\sqrt{13}]$ with norm 1. Those units are also units of $\mathcal{O}$. Since the group of units of $\mathcal{O}$ is isomorphic to $\{\pm 1\} \times \mathbb{Z}$, and $(\mathcal{O} : \mathbb{Z}[\sqrt{13}]) = 2$, the units of $\mathbb{Z}[\sqrt{13}]$ are also generated by a fundamental one. By the similar argument of Exercise 1, this fundamental unit $x_1 + y_1\sqrt{13}$

corresponds to the integer solution (x_1, y_1) of $x^2 - 13y^2 = \pm 1$ with $x_1, y_1 > 0$ as small as possible.

When $y = 5$, $13y^2 - 1 = 324 = 18^2$, hence $\varepsilon_1 = 18 + 5\sqrt{13}$ is a fundamental unit of $\mathbb{Z}[\sqrt{13}]$, whose norm is -1. Therefore all units of $\mathbb{Z}[\sqrt{13}]$ with norm 1 is generated by $\varepsilon_1^2 = 629 + 180\sqrt{13}$. Then the smallest possible number of men Harold had is $629^2 - 1 = 395640$. □

4 Let ζ be a primitive p-th root of unity, p an odd prime number. Show that $\mathbb{Z}[\zeta]^* = \langle\zeta\rangle\mathbb{Z}[\zeta + \zeta^{-1}]^*$. When $p = 5$, show that $\mathbb{Z}[\zeta]^* = \{\pm\zeta^k(1 + \zeta)^n | 0 \leqslant k < 5, n \in \mathbb{Z}\}$.

Proof: First, $\langle\zeta\rangle\mathbb{Z}[\zeta + \zeta^{-1}]^* \subset \mathbb{Z}[\zeta]^*$. In fact, $\mathbb{Z}[\zeta + \zeta^{-1}] \subset \mathbb{Z}[\zeta]$, hence $\mathbb{Z}[\zeta + \zeta^{-1}]^* \subset \mathbb{Z}[\zeta]^*$. On the other hand, the cyclic group $\langle\zeta\rangle$ is obviously in $\mathbb{Z}[\zeta]^*$. Therefore, $\langle\zeta\rangle\mathbb{Z}[\zeta + \zeta^{-1}]^* \subset \mathbb{Z}[\zeta]^*$.

Now, for any unit ε of $\mathbb{Z}[\zeta]$, we can write it as $\varepsilon = re^{i\theta}$ with $r, \theta \in \mathbb{R}$. We have $\varepsilon\bar{\varepsilon} = r^2$ and so $e^{i2\theta} = \varepsilon/\bar{\varepsilon} \in \mathbb{Z}[\zeta]^*$. Since all conjugates of $e^{i2\theta}$ has absolute value 1, by Proposition (7.1), it must be a root of unity, say $e^{i2\theta} = \pm\zeta^a$.

If $e^{i2\theta} = -\zeta^a$, write $\varepsilon = b_0 + \cdots + b_{p-2}\zeta^{p-2}$, we have $\bar{\varepsilon} = b_0 + \cdots + b_{p-2}\zeta^{-(p-2)} \equiv b_0 + \cdots + b_{p-2} \equiv \varepsilon = -\zeta^a\bar{\varepsilon} \equiv -\bar{\varepsilon} \bmod (1-\zeta)$. Thus $2\bar{\varepsilon} \in (1-\zeta)$. By Lemma 4.4, $(1-\zeta)$ is a prime ideal and one can see $2 \notin (1-\zeta)$, therefore $\bar{\varepsilon} \in (1-\zeta)$, which contradicts that $\bar{\varepsilon}$ is a unit. So $e^{i2\theta} = \zeta^a$.

Since p is odd, there exists a $b \in \mathbb{Z}$ such that $2b \equiv a \bmod p$, thus $e^{i\theta} = \zeta^b$. Then $r = \varepsilon\zeta^{-b} \in \mathbb{Z}[\zeta]^* \cap \mathbb{R}$ and hence $r \in \mathbb{Z}[\zeta + \zeta^{-1}]^*$ by Lemma 4.3. Therefore $\varepsilon = re^{i\theta} \in \langle\zeta\rangle\mathbb{Z}[\zeta + \zeta^{-1}]^*$.

For $K = \mathbb{Q}(\zeta)$ with ζ a primitive 5-th root of unity, $n = 4, s = 2, r = 0$, hence $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}$. By **??**, Proposition (10.2), $\mathcal{O}_K = \mathbb{Z}[\zeta]$. Therefore $\mathbb{Z}[\zeta]^* = \{\pm\zeta^k u^n | 0 \leqslant k < 5, n \in \mathbb{Z}\}$, here u is a fundamental unit of K and, by Lemma 4.3, can be chosen to be a fundamental unit of $\mathbb{Q}(\zeta + \zeta^{-1})$.

Since $\zeta + \zeta^{-1} = \frac{\pm\sqrt{5}-1}{2}$ and $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 2$, we get $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\sqrt{5})$, which has a fundamental unit $\varepsilon = \frac{1+\sqrt{5}}{2}$ by Exercise 2. Hence $\zeta + \zeta^{-1}$ is also a fundamental unit and so $\mathbb{Z}[\zeta]^* = \{\pm\zeta^k(\zeta + \zeta^{-1})^n | 0 \leqslant k < 5, n \in \mathbb{Z}\}$.

To get the required formula, first note that $(1 + \zeta)(-\zeta - \zeta^3) = 1$, so $(1 + \zeta)$ is a unit. Then since $\zeta + \zeta^{-1} = -\zeta^{-2}(1 + \zeta)^{-1}$, we also have $\mathbb{Z}[\zeta]^* = \{\pm\zeta^k(1 + \zeta)^n | 0 \leqslant k < 5, n \in \mathbb{Z}\}$ as desired. □

4.1 Lemma *The maximal real subfield K^+ of $K = \mathbb{Q}(\zeta)$ is $\mathbb{Q}(\zeta + \zeta^{-1})$.*

Proof: Let $\phi \colon K \to K$ be the complex conjugate $z \mapsto \bar{z}$, which is an element of $\mathrm{Gal}(K/\mathbb{Q})$ with order 2. The maximal real subfield of K is obviously the fixed field K^ϕ of ϕ and $[K : K^\phi] = 2$. One can see that ϕ sends ζ to ζ^{-1} and fixes $\zeta + \zeta^{-1}$. Hence $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K^\phi$. Consider the irreducible polynomial

$$X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X],$$

which is obviously the minimal polynomial of ζ over $\mathbb{Q}(\zeta+\zeta^{-1})$. Hence $[K:\mathbb{Q}(\zeta+\zeta^{-1})]=2$ and then $\mathbb{Q}(\zeta+\zeta^{-1})=K^{\phi}$. □

4.2 Lemma *$\zeta^j+\zeta^{-j}, j\geqslant 1$ contains an integral basis of $\mathbb{Z}[\zeta+\zeta^{-1}]$.*

Proof: First, $\zeta^j+\zeta^{-j}\in\mathbb{Z}[\zeta+\zeta^{-1}]$ for all $j\geqslant 1$. This follows from a conduction on j: if $\zeta^j+\zeta^{-j}\in\mathbb{Z}[\zeta+\zeta^{-1}]$ for $1\leqslant j<k$, then $\zeta^k+\zeta^{-k}=(\zeta+\zeta^{-1})^k-\sum_{j=1}^{[\frac{k-1}{2}]}\binom{k}{j}(\zeta^{k-2j}+\zeta^{2j-k})\in\mathbb{Z}[\zeta+\zeta^{-1}]$.

On the other hand, any power of $\zeta+\zeta^{-1}$ can be expressed as a $\mathbb{Z}$-liner combination of $\zeta^j+\zeta^{-j}$ by the binomial theorem. Thus $\zeta^j+\zeta^{-j}, j\geqslant 1$ must contain an integral basis of $\mathbb{Z}[\zeta+\zeta^{-1}]$. □

4.3 Lemma *$\mathbb{Z}[\zeta+\zeta^{-1}]$ is the ring of integers in $K^+=\mathbb{Q}(\zeta+\zeta^{-1})$.*

Proof: Obviously $\mathbb{Z}[\zeta+\zeta^{-1}]\subset\mathcal{O}_{K^+}$.

By §10, Proposition (10.2), $\mathbb{Z}[\zeta]$ is the ring of integers in $K=\mathbb{Q}(\zeta)$. For any $\alpha\in\mathcal{O}_{K^+}$, we have $\alpha\in\mathbb{Z}[\zeta]^{\phi}$, thus we can write it as

$$\alpha=f(\zeta)=\sum_{j=1}^{p-1}a_j\zeta^j\in\mathbb{Z}[\zeta]^{\phi}.$$

Then $f(\zeta)=\overline{f(\zeta)}=f(\bar{\zeta})$. Therefore $a_j=a_{p-j}$ and so that

$$f(\zeta)=\sum_{j=1}^{\frac{p-1}{2}}a_j(\zeta^j+\zeta^{-j}),$$

which is contained in $\mathbb{Z}[\zeta+\zeta^{-1}]$ by Lemma 4.2. □

4.4 Lemma *$(1-\zeta)$ is a prime ideal in $\mathbb{Z}[\zeta]$.*

Proof: First, we show that $1-\zeta$ is not a unit. Indeed, the all embeddings of K into $\mathbb{C}$ are $\zeta\mapsto\zeta^j, 1\leqslant j\leqslant p-1$. Therefore

$$\begin{aligned}N(1-\zeta)&=\prod_{j=1}^{p-1}(1-\zeta^j)\\&=1+1^1+\cdots+1^{p-1}=p>1.\end{aligned}$$

This shows $1-\zeta$ is not a unit.

For $\alpha\beta\in(1-\zeta)$, write $\alpha=a_0+\cdots+a_{p-2}\zeta^{p-2}$ and $\beta=b_0+\cdots+b_{p-2}\zeta^{p-2}$, we have $0\equiv\alpha\beta=(a_0+\cdots+a_{p-2}\zeta^{p-2})(b_0+\cdots+b_{p-2}\zeta^{p-2})\equiv(a_0+\cdots+a_{p-2})(b_0+\cdots+b_{p-2})\bmod(1-\zeta)$. However, $a_0+\cdots+a_{p-2}, b_0+\cdots+b_{p-2}\in\mathbb{Z}$ and $(1-\zeta)\cap\mathbb{Z}=p\mathbb{Z}$, hence $p\mid(a_0+\cdots+a_{p-2})(b_0+\cdots+b_{p-2})$. Since p is a prime number, so either $p\mid a_0+\cdots+a_{p-2}$ or $p\mid b_0+\cdots+b_{p-2}$, which implies either $\alpha\in(1-\zeta)$ or $\beta\in(1-\zeta)$ as desired. □

4.5 Remark In general case where ζ is a primitive n-th root of unity, this result doesn't hold. When n is not a prime power, $(1-\zeta)$ is actually a unit.

Reference: [Lawrence C. Washington] Introduction to Cyclotomic Fields

5 Let ζ be a primitive m-th root of unity, $m \geqslant 3$. Show that the numbers $\frac{1-\zeta^k}{1-\zeta}$ for $(k,m)=1$ are units in the ring of integers of the field $\mathbb{Q}(\zeta)$. The subgroup of the group of units they generate is called the group of *cyclotomic units*.

Proof: Since $(k,m)=1$, there exists an integer l such that $lk \equiv 1 \bmod m$. Then we have

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1-\zeta^{lk}}{1-\zeta^k} = 1+\zeta^k+\zeta^{2k}+\cdots+\zeta^{(l-1)k},$$

which is integral. Therefore $\frac{1-\zeta^k}{1-\zeta}$ is a unit. □

6 Let K be a totally real number field, i.e., $X = \mathrm{Hom}(K,\mathbb{C}) = \mathrm{Hom}(K,\mathbb{R})$, and let T be a proper nonempty subset of X. Then there exists a unit ε satisfying $0 < \tau\varepsilon < 1$ for $\tau \in T$, and $\tau\varepsilon > 1$ for $\tau \notin T$.

Proof: Consider the lattice $\Gamma = \lambda\mathcal{O}_K^*$ in the trace-zero hyperplane H. Let S be the set

$$S = \{(x_\tau) \in H | x_\tau < 0 \text{ for } \tau \in T; x_\tau > 0 \text{ for } \tau \notin T\}.$$

It is the intersection of an *orthant* and H, which contains the origin. Therefore the volume of S must be either ∞, if H across this orthant, or 0, if not. One can see the later case only happens when $T = X$ or $T = \varnothing$. Therefore, when T is a proper nonempty subset of X, vol(S) is ∞ and hence satisfying the condition of Minkowski's Lattice Point Theorem. Then there exists a unit ε such that $\lambda\varepsilon \in S$ and therefore satisfying the required properties. □

§ 8 Extensions of Dedekind Domains

I Review

II Exercises

In this section, $\mathcal{o}$ is a dedekind domain with fraction field K and $\mathcal{O}$ is its integral closure in a finite separable extension $L|K$.

1 If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathcal{o}$, then one has $\mathfrak{a} = \mathfrak{a}\mathcal{O} \cap \mathcal{o}$ and $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{a}\mathcal{O} \mid \mathfrak{b}\mathcal{O}$.

Proof: First, the result $\mathfrak{a} = \mathfrak{a}\mathcal{O} \cap \mathcal{o}$ is clear for PIDs: since for any $x \in \mathfrak{a}\mathcal{O} \cap \mathcal{o}$, it can be written as $x = ay$ with $\mathfrak{a} = a\mathcal{o}$ and $y \in \mathcal{O}$, then $y = a^{-1}x \in K$ and so $y \in \mathcal{o}$ and $x \in \mathfrak{a}$.

For a general $\mathcal{o}$, we have show that $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}\mathcal{O}_\mathfrak{p} \cap \mathcal{o}_{pp}$ for every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{o}$: by Proposition 3.5.2 of §1.3, $\mathcal{o}_\mathfrak{p}$ is a Dedekind domain, by Proposition 2.5.7 of §1.2, $\mathcal{O}_\mathfrak{p}$ is the integral closure of $\mathcal{o}_\mathfrak{p}$ in the extension $L|K$, so the result for local follows from above. Since $\mathfrak{a}_\mathfrak{p}\mathcal{O}_\mathfrak{p} \cap \mathcal{o}_\mathfrak{p} = (\mathfrak{a}\mathcal{O} \cap \mathcal{o})_\mathfrak{p}$, we get $\mathfrak{a} = \mathfrak{a}\mathcal{O} \cap \mathcal{o}$ since equality is a local property.

If $\mathfrak{a} \mid \mathfrak{b}$, then $\mathfrak{a} \supset \mathfrak{b}$ and so $\mathfrak{a}\mathcal{O} \supset \mathfrak{b}\mathcal{O}$ i.e. $\mathfrak{a}\mathcal{O} \mid \mathfrak{b}\mathcal{O}$. Conversely, if $\mathfrak{a}\mathcal{O} \mid \mathfrak{b}\mathcal{O}$, then $\mathfrak{a}\mathcal{O} \supset \mathfrak{b}\mathcal{O}$ and so $\mathfrak{a}\mathcal{O} \cap \mathcal{o} \supset \mathfrak{b}\mathcal{O} \cap \mathcal{o}$, which is $\mathfrak{a} \supset \mathfrak{b}$ i.e. $\mathfrak{a} \mid \mathfrak{b}$. □

2 For every integral ideal $\mathfrak{A}$ of $\mathcal{O}$, there exists a $\theta \in \mathcal{O}$ such that the conductor $\mathfrak{F} = \{\alpha \in \mathcal{O} | \alpha\mathcal{O} \subset \mathcal{o}[\theta]\}$ is prime to $\mathfrak{A}$ and such that $L = K(\theta)$.

The statement in this exercise is false. However, according to Serre's *Local Fields* [Ser79], Ch.III, Exercise 2 on p.59, it is true when the residue extension $\mathcal{O}/\mathfrak{A} | \mathcal{o}/(\mathfrak{A} \cap \mathcal{o})$ is *separable*.

Proof: In the case $\mathcal{O}$ is local, the statement follows from Proposition 2.1 immediately. In general case, let □

2.1 Proposition ([Ser79, III, Proposition 12]) *Suppose that $\mathcal{O}$ (hence also $\mathcal{o}$) is a discrete valuation ring. If the residue field extension is separable, then there exists a $\theta \in \mathcal{O}$ such that $\mathcal{O} = \mathcal{o}[\theta]$.*

Proof: Let e be the ramification index and f the inertia degree, so that $n = ef$. Let π be a uniformizing parameter of $\mathcal{O}$, and let $\theta \in \mathcal{O}$ represent a primitive element for the residue field extension.

We claim that $\theta^i\pi^j, 0 \leqslant i \leqslant f, 0 \leqslant j \leqslant e$ form a $\mathcal{o}$-basis of $\mathcal{O}$. Indeed, by *Nakayama's Lemma*, it suffices to show that their classes span $\mathcal{O}/\mathfrak{p}\mathcal{O}$.

Since $\mathfrak{p}\mathcal{O} = \mathfrak{P}^e = \pi^e\mathcal{O}$, it suffices to show that their classes span $\mathcal{O}/\pi^n\mathcal{O}$ by induction on $1 \leqslant n \leqslant e$.

Further, the element θ can be chosen so that there exists a monic polynomial $f(X) \in \mathcal{o}[X]$ of degree f such that $f(\theta)$ is a uniformizing parameter of $\mathcal{O}$. Indeed, let f be a monic polynomial over $\mathcal{o}$ whose reduction $\overline{f}$ is the minimal polynomial of $\overline{\theta}$, let v denote the normalized valuation of $\mathcal{O}$, then $v(f(\theta)) \geqslant 1$. If $v(f(\theta)) = 1$, then θ satisfies the requirement. If $v(f(\theta)) \geqslant 2$, choose any $h \in \mathcal{O}$ of valuation 1, and apply *Taylor's formula*, one has

$$f(\theta + h) \equiv f(\theta) + f'(\theta)h \bmod h^2.$$

Since the residue field extension is *separable*, $\overline{f}'(\overline{\theta}) \neq 0$, thus $f'(\theta)$ is a unit. Then $v(f(\theta + h)) = 1$ and $\overline{\theta + h} = \overline{\theta}$. □

2.2 Remark Note that the above proof shows, if $\mathcal{O} = \mathcal{o}[\theta]$ and $v(\theta' - \theta) \geqslant 2$, then $\mathcal{O} = \mathcal{o}[\theta']$.

2.3 Proposition *Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}$ whose corresponding residue field extension is separable. Then there exists a $\theta \in \mathcal{O}$ such that the conductor $\mathfrak{F} = \{\alpha \in \mathcal{O} | \alpha\mathcal{O} \subset \mathcal{o}[\theta]\}$ is prime to $\mathfrak{P}$ and such that $L = K(\theta)$.*

Proof: Note that the prime ideal $\mathfrak{P}$ induces discrete valuations on $\mathcal{O}$ and $\mathcal{o}$. Let $\widehat{\mathcal{O}}$ and $\widehat{\mathcal{o}}$ denote the completion of $\mathcal{O}$ and $\mathcal{o}$ respectively. Then $\widehat{\mathcal{O}}$ and $\widehat{\mathcal{o}}$ are discrete valuation rings and $\widehat{\mathcal{O}}$ is the integral closure of $\widehat{\mathcal{o}}$ in the fraction field $\widehat{L}$. Then, by Proposition 2.1, there exists a $\theta \in \widehat{\mathcal{O}}$ such that $\widehat{\mathcal{O}} = \widehat{\mathcal{o}}[\theta]$. Shrinking θ so that $\theta \in \mathcal{O}$ and let $f(X)$ be the minimal polynomial of θ. Then $\widehat{\mathfrak{F}} = \widehat{\mathcal{O}}$. Therefore $\mathfrak{F}/\mathfrak{P} \cong \widehat{\mathfrak{F}}/\widehat{\mathfrak{P}} = \widehat{\mathcal{O}}/\widehat{\mathfrak{P}} = \mathcal{O}/\mathfrak{P}$. □

2.4 Remark (conductor) Let A be a domain with integral closure $\overline{A}$ in its fraction field K, then the ***conductor*** of A is defined to be

$$\mathfrak{f}_A := \{x \in K | x\overline{A} \subset A\}.$$

This is a generalization of the conductors defined in this section and **??**. One can see it is a common ideal of A and $\overline{A}$. Moreover, it is the largest common ideal.

More generally, let B be an A-subalgebra, then the ***conductor*** of B in A is defined to be the largest common ideal of A and B, or equivalently,

$$\mathfrak{f}(B/A) := \{x \in A | xB \subset A\}.$$

More generally, let M, N be two A-modules, then the ***conductor*** is defined to be

$$(N :_A M) := \{x \in A | xM \subset N\}.$$

If M, N are further to be A-submodules of K, then we can also define

$$(N :_K M) := \{x \in K | xM \subset N\}.$$

The examples of conductor contain:

1. The conductor $\mathfrak{F} = \mathfrak{f}_{\mathcal{O}[\theta]}$;
2. The ***annihilator*** $\operatorname{Ann}(M) = (0 :_A M)$.

Note that $(N :_A M) = \operatorname{Ann}((M+N)/N)$, therefore we have the following formula for any multiplicative subset S of A:

$$S^{-1}(N :_A M) = (S^{-1}N :_{S^{-1}A} S^{-1}M).$$

2.5 Proposition *Let M, N be two A-submodules of K, then there exists a natural isomorphism $\operatorname{Hom}_A(M,N) \cong (N :_K M)/\operatorname{Ann}(M)$. Especially, $\mathfrak{f}_A$ can be naturally identified with $\operatorname{Hom}_A(\overline{A}, A)$.*

Proof: The canonical map $(N :_K M) \to \operatorname{Hom}_A(M,N)$ can be constructed as follow: for any $x \in (N :_K M)$, the map $v \mapsto xv$ defines a homomorphism from M to N. It is easy to check this is a natural homomorphism with kernel $\operatorname{Ann}(M)$. It is surjective since for any homomorphism $f\colon M \to N$, we can choose an $x \in M \cap A$, then for any $\frac{s}{t} \in M$, we have $xtf(\frac{s}{t}) = f(xs) = sf(x)$ and so $f(\frac{s}{t}) = \frac{f(x)}{x}\frac{s}{t}$, which shows $\frac{f(x)}{x} \in (N :_K M)$ is a required preimage.□

3 If a prime ideal $\mathfrak{p}$ of K is totally split in two separable extensions $L|K$ and $L'|K$, then it is also totally split in the composite extension.

In this Exercise, We denote the integral closure of $\mathcal{O}$ in L by $\mathcal{O}_L$ to emphasize the field.

Proof: It follows immediately from Proposition 3.1 and Proposition 3.2. □

3.1 Proposition *Let $\mathfrak{p}$ be a prime ideal of K, and $L|K, N|L$ two separable extensions. Then $\mathfrak{p}$ is totally split in N if and only if it is totally split in L and every prime ideal above $\mathfrak{p}$ is totally split in N.*

Proof: Since prime ideals above distinct prime ideals are distinct, the "only if" is then obvious. Conversely, let $[L : K] = n, [N : L] = m$ and

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$
$$\mathfrak{P}_i\mathcal{O}_N = \mathfrak{Q}_{i1}^{e_{i1}} \cdots \mathfrak{Q}_{ir_i}^{eir_i} (1 \leqslant i \leqslant r).$$

Then

$$\mathfrak{p}\mathcal{O}_N = \prod_{i=1}^{r}\prod_{j=1}^{r_i} \mathfrak{Q}_{ij}^{e_i e_{ij}}.$$

Since $\mathfrak{p}$ is totally split in N, one must have $r_1 + \cdots + r_r = nm$. However, $r \leqslant n$ and $r_i \leqslant m$. Thus $r = n$ and $r_i = m$, which shows that $\mathfrak{p}$ is totally split in L and $\mathfrak{P}_i$ are totally split in N. □

3.2 Proposition *Let $\mathfrak{p}$ be a prime ideal of K, and $L|K, L'|K$ two separable extensions. If $\mathfrak{p}$ is totally split in L, then every prime ideal of L' above $\mathfrak{p}$ is totally split in LL'.*

Proof: By Exercise 2, we may assume $L = K(\theta)$ and $\mathfrak{p}$ is relative prime to the conductor $\mathfrak{F} = \{\alpha \in \mathcal{O}_L | \alpha\mathcal{O}_L \subset \mathcal{o}[\theta]\}$. Then by Proposition (8.3), the minimal polynomial $f(x)$ of θ on K can be factored into

$$f(x) \equiv (x - a_1) \cdots (x - a_n) \operatorname{mod} \mathfrak{p}.$$

For $\mathfrak{P}$ a prime ideal of L' above $\mathfrak{p}$, we claim that it is relative prime to the conductor $\mathfrak{F}' = \{\alpha \in \mathcal{O}_{LL'} | \alpha\mathcal{O}_{LL'} \subset \mathcal{O}_{L'}[\theta]\}$. Since $LL' = L'(\theta)$ and the minimal polynomial of θ on L' divides $f(x)$, by Proposition (8.3) again, $\mathfrak{P}$ is totally split in LL'. □

4 A prime ideal $\mathfrak{p}$ of K is totally split in the separable extension $L|K$ if and only if it is totally split in the Galois closure $N|K$ of $L|K$.

Proof: This follows immediately from Exercise 3 since the Galois closure of a separable extension is just the composite of all its conjugates. □

5 For a number field K the statement of proposition (8.3) concerning the prime decomposition in the extension $K(\theta)$ holds for all prime ideals $\mathfrak{p} \nmid (\mathcal{O} : \mathcal{o}[\theta])$.

Proof: We only need to show $\mathfrak{p} \nmid (\mathcal{O} : \mathcal{o}[\theta])$ implies $\mathfrak{p}$ is relative prime to the conductor $\mathfrak{F}$. Indeed, let $d = (\mathcal{O} : \mathcal{o}[\theta])$, then $\mathfrak{p} \nmid d$ implies $\mathfrak{p} + d\mathcal{o} = \mathcal{o}$ and so $\mathfrak{p}\mathcal{O} + d\mathcal{O} = \mathcal{O}$. However, $d\mathcal{O} \subset \mathfrak{F}$, therefore $\mathfrak{p}\mathcal{O} + \mathfrak{F} = \mathcal{O}$. □

6 Given a positive integer $b > 1$, an integer a relatively prime to b is a quadratic residue $\operatorname{mod} b$ if and only if it is a quadratic residue modulo each prime divisor p of b, and if $a \equiv 1 \operatorname{mod} 4$ when $4 \mid b, 8 \nmid b$, resp. $a \equiv 1 \operatorname{mod} 8$ when $8 \mid b$.

Proof: Let $b = 2^e p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition of b, then by the *Chinese Remainder Theorem* the congruence $x^2 \equiv a \operatorname{mod} b$ is equivalent to the system

$$\begin{aligned} x^2 &\equiv a \operatorname{mod} 2^e, \\ x^2 &\equiv a \operatorname{mod} p_1^{e_1}, \\ &\cdots \\ x^2 &\equiv a \operatorname{mod} p_r^{e_r}. \end{aligned}$$

Consider $x^2 \equiv a \bmod 2^e$. Since the only quadratic residue mod 4 or mod 8 is 1, the congruence has solutions only if $a \equiv 1 \bmod 4$ when $4 \mid b, 8 \nmid b$, resp. $a \equiv 1 \bmod 8$ when $8 \mid b$. If this is the case, we can construct a solution x' of the congruence $x^2 \equiv a \bmod 2^{m+1}$ from a solution x of the congruence $x^2 \equiv a \bmod 2^m$ by taking $x' = x + 2^{-1}(a - x^2)$.

Now, consider $x^2 \equiv a \bmod p_i^{e_i}$. If it has solutions, then so is $x^2 \equiv a \bmod p$. Then converse follows from the following *Hensel's lemma.* □

6.1 Lemma (Hensel's lemma) *Let $f(X)$ be a a polynomial with integer coefficients, and let m, k be positive integers such that $m \leqslant k$. If r is an integer such that*

$$f(r) \equiv 0 \bmod p^k \quad \textit{and} \quad f'(r) \not\equiv 0 \bmod p,$$

then there exists an integer s such that

$$f(s) \equiv 0 \bmod p^{k+m} \quad \textit{and} \quad r \equiv s \bmod p^k.$$

Furthermore, this s is unique $\bmod\, p^{k+m}$*, and can be computed explicitly as*

$$s = r + tp^k,$$

where the integer t is the solution of the congruence $f'(r)t + \frac{f(r)}{p^k} \equiv 0 \bmod p^m$.

Proof: The lemma derives from the following Taylor expansion:

$$f(r + tp^k) = f(r) + tp^k f'(r) + O(p^{2k}).$$ □

Proof: Also, this Hensel's lemma can be viewed as a special case of the *Hensel's lemma* (II.4.6). Consider the p-adic ring $\mathbb{Z}_p$. Since $f(r) \equiv 0 \bmod p^k$, $f(X) \bmod p$ has a root r and so admit a factorization

$$f(X) \equiv (X - r)g(X) \bmod p.$$

Since $f'(r) \not\equiv 0 \bmod p$, $f(X)$ is a primitive polynomial and $X - r, g(X)$ are relative prime. Then, $f(X)$ admit a factorization

$$f(X) = (X - s)h(X),$$

whit $s \equiv r \bmod p$ and $h(X) \equiv g(X) \bmod p$. □

7 Let $(a, p) = 1$ and $a\nu \equiv r_\nu \bmod p$, $\nu = 1, \cdots, p-1$, $0 < r_\nu < p$. Then the r_ν give a permutation π of the numbers $1, \cdots, p-1$. Show that $\operatorname{sgn} \pi = \left(\frac{a}{p}\right)$**.**

Proof (cf. Lemma 1.7.3): Fix an ordering on $\mathbb{F}_p$, we have the following equation in $\mathbb{F}_p$:

$$\operatorname{sgn}\pi = \frac{\prod_{i<j}(\pi(i) - \pi(j))}{\prod_{i<j}(i-j)}.$$

Therefore $\operatorname{sgn}\pi = a^{\frac{p(p-1)}{2}} = a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ in $\mathbb{F}_p$. □

There is another proof:

Proof: Denote the permutation defined by a as π_a. If $\left(\frac{a}{p}\right) = 1$, then we may write $a \equiv b^2 \bmod p$, then $\pi_a = \pi_b \circ \pi_b$ and must be a even permutation, so $\operatorname{sgn}\pi = 1$. However, the number of quadratic residues is $\frac{p-1}{2}$, which is the same as the number of even permutations, so the even permutations are precisely given by the quadratic residues. □

We explain the two claims in the proof as two lemmas.

7.1 Lemma *The number of quadratic residues is* $\frac{p-1}{2}$*.*

Proof: Since $x^2 \equiv (p-x)^2 \bmod p$, this number $\leqslant \frac{p-1}{2}$. On the other hand, $1^2, 2^2, \cdots, (\frac{p-1}{2})^2$ are distinct $\bmod p$, so this number is $\frac{p-1}{2}$. □

7.2 Lemma *The numbers of odd and even permutations defined by multiplication are the same.*

Proof: If there exists an odd permutation defined by multiplication, then it induces a bijection between the set of odd and even permutations defined by multiplication and thus the numbers are the same.

As for the existence of the odd permutation, just consider the generator a of the multiplication group $\mathbb{F}_p^*$. Multiplying by a is a translation of length $p-1$, thus is an odd permutation. □

By more careful considering on this type of permutations, *Zhang Hanbin* provide the following proof.

7.3 Lemma *Let* $\operatorname{inv}(a_1, \cdots, a_n)$ *denote the* **inversion number** *of the sequence* $(a_1, \cdots, a_n)$ *and let* π *be a permutation on* $1, 2, \cdots, n$*. Then one have*

$$\operatorname{sgn}\pi = (-1)^{\operatorname{inv}(\pi(1),\cdots,\pi(k))+\operatorname{inv}(\pi(k+1),\cdots,\pi(n))+\pi(1)+\cdots+\pi(k)+\frac{k(k+1)}{2}}.$$

Proof: First, using s times transportation to transform $\pi(1), \cdots, \pi(k)$ to $\tau\pi(1), \cdots, \tau\pi(k)$ with $\tau\pi(1) < \cdots < \tau\pi(k)$, i.e. $\operatorname{inv}(\tau\pi(1), \cdots, \tau\pi(k)) = 0$. Therefore

$$\begin{aligned}\operatorname{sgn}\pi &= (-1)^{\operatorname{inv}(\pi(1),\cdots,\pi(k))}\operatorname{sgn}\tau\pi \\ &= (-1)^{\operatorname{inv}(\pi(1),\cdots,\pi(k))+\sum_{i=1}^{k}(\tau\pi(i)-i)+\operatorname{inv}(\pi(k+1),\cdots,\pi(n))} \\ &= (-1)^{\operatorname{inv}(\pi(1),\cdots,\pi(k))+\operatorname{inv}(\pi(k+1),\cdots,\pi(n))+\pi(1)+\cdots+\pi(k)+\frac{k(k+1)}{2}}\end{aligned}$$ □

7.4 Lemma (Eisenstein's lemma) *Let $C = \{2, 4, \cdots, p-1\}$ and $(a, p) = 1$. If $r_i \in C$ and $ar_i \equiv t_i \bmod p$, then we have*

$$\left(\frac{a}{p}\right) = (-1)^{t_1 + \cdots + t_{\frac{p-1}{2}}}.$$

Proof: First note that the set $\left\{(-1)^{t_i} t_i \middle| i = 1, \cdots, \frac{p-1}{2}\right\}$ is a rearrangement of C. Indeed, if

$$(-1)^{t_i} t_i \equiv (-1)^{t_j} t_j \bmod p,$$

then

$$(-1)^{t_i} ar_i \equiv (-1)^{t_j} ar_j \bmod p,$$

which implies $r_i \equiv \pm r_j \bmod p$, a contradiction.

Therefore, we have

$$a^{\frac{p-1}{2}} r_1 \cdots r_{\frac{p-1}{2}} \equiv t_1 \cdots t_{\frac{p-1}{2}} \bmod p.$$

Thus

$$a^{\frac{p-1}{2}} (-1)^{t_1 + \cdots + t_{\frac{p-1}{2}}} t_1 \cdots t_{\frac{p-1}{2}} \equiv t_1 \cdots t_{\frac{p-1}{2}} \bmod p.$$

Since $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$ (Lemma 1.7.3), the result follows. □

8 Let $a_n = \frac{\varepsilon^n - \varepsilon'^n}{\sqrt{5}}$, where $\varepsilon = \frac{1+\sqrt{5}}{2}, \varepsilon' = \frac{1-\sqrt{5}}{2}$ (a_n is the n-th Fibonacci number). If p is a prime number $\neq 2, 5$, then one has

$$a_p \equiv \left(\frac{p}{5}\right) \bmod p.$$

Proof: The ***Frobenius automorphism*** $\varphi \colon x \mapsto x^p$ induces a permutation of the roots of a separable polynomial on $\mathbb{F}_p$. Since ε and ε' are the two roots of the polynomial $f(X) = X^2 - X - 1$. By $\bmod p$, we have

$$a_p = \frac{\varepsilon^p - \varepsilon'^p}{\varepsilon - \varepsilon} \equiv \frac{\varphi(\varepsilon) - \varphi(\varepsilon')}{\varepsilon - \varepsilon'} = \begin{cases} 1 & \text{if } F \text{ fixes } \varepsilon \text{ and } \varepsilon', \\ -1 & \text{if } F \text{ interchanges } \varepsilon \text{ and } \varepsilon'. \end{cases}$$

Note that F fixes ε and ε' if and only if the polynomial $f(X) \bmod p$ splits.

The discriminant of f is $\Delta(f) = 5$ and splitting field is $\mathbb{Q}(\sqrt{5})$. By Exercise 2.4, the discriminant of $\mathbb{Q}(\sqrt{5})$ is again 5, thus the two roots form an integral basis. Then we have $\mathcal{O} = \mathbb{Z}[\varepsilon]$ and the condition of Proposition (8.3) is trivially satisfied by our case. So f it splits $\bmod p$ if and only if p is totally split in $\mathbb{Q}(\sqrt{5})$, if and only if $\left(\frac{5}{p}\right) = 1$ by Proposition (8.5). Since $\frac{5-1}{2}\frac{p-1}{2}$ is even, by the *Gauss's Reciprocity Law*, we conclude that

$$a_p \equiv \left(\frac{p}{5}\right) \bmod p.$$

□

8.1 Remark Form the above proof, one can see that for the *Lucas sequence* $a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ where α, β are roots of polynomial $X^2 - X - \frac{q-1}{4}$ with q a prime number congruent to $1 \bmod 4$, we have

$$a_p \equiv \left(\frac{q}{p}\right) \bmod p,$$

and the *Gauss's Reciprocity Law* for p, q is equivalent to

$$a_p \equiv \left(\frac{p}{q}\right) \bmod p.$$

For the general case, let $q^* = \left(\frac{-1}{q}\right) q$, then $q^* \equiv 1 \bmod 4$ and so

$$a_p \equiv \left(\frac{q^*}{p}\right) \bmod p.$$

Since we have

$$\left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

the *Gauss's Reciprocity Law* is then equivalent to

$$a_p \equiv \left(\frac{p}{q}\right) \bmod p.$$

8.2 Remark (Frobenius automorphism) The ***Frobenius automorphism*** $\varphi \colon x \mapsto x^p$ defined an automorphism on a finite field with characteristic p. For a field isomorphic to $\mathbb{F}_{p^n}$, its automorphism group is cyclic of degree n and generated by φ. Consequently, for the two fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$, one can see $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ if and only if $n \mid m$, say $m = dn$. If this is the case, then this is a Galois extension and the Galois group is cyclic of degree d and generated by φ^n.

9 Study the Legendre symbol $\left(\frac{3}{p}\right)$ as a function of $p > 3$. Show that the property of 3 being a quadratic residue or nonresidue $\bmod p$ depends only on the class of $p \bmod 12$.

Proof: One have

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \bmod 3, \\ -1 & p \equiv 2 \bmod 3. \end{cases}$$

Therefore, by *Gauss's Reciprocity Law*, one get

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1, 11 \bmod 12, \\ -1 & p \equiv 5, 7 \bmod 12. \end{cases}$$ □

10 Show that the number of solutions of $x^2 \equiv a \bmod p$ equals $1 + \left(\frac{a}{p}\right)$.

Proof: It suffices to show there are exact two solutions of $x^2 \equiv a \bmod p$ when a is a quadratic residue $\bmod\, p$. Indeed, this quadratic equation has at most two solutions, but since $x^2 \equiv (p-x)^2 \bmod p$, there exist at least two solutions. □

11 Show that the number of solutions of the congruence $ax^2 + bx + c \equiv 0 \bmod p$, where $(a,p) = 1$, equals $1 + \left(\frac{b^2-4ac}{p}\right)$.

Proof: Since $(a,p) = 1$, the congruence is equivalent to the congruence $(2ax+b)^2 \equiv b^2 - 4ac \bmod p$ and therefore the number of its solutions equals $1 + \left(\frac{b^2-4ac}{p}\right)$ by Exercise 10. □

§ 9 Hilbert's Ramification Theory

I Review

II Exercises

In this section, $\mathcal{o}$ is a dedekind domain with fraction field K and $\mathcal{O}$ is its integral closure in a finite separable extension $L|K$.

1 If $L|K$ is a Galois extension of algebraic number fields with noncyclic Galois group, then there are at most finitely many nonsplit prime ideals of K.

Proof: By Proposition (8.4), there are only finitely many ramified primes. Thus it suffices to show that all nonsplit prime ideals are ramified.

Let $\mathfrak{p}$ be an unramified and nonsplit prime ideal of $\mathcal{o}$. Since it is nonsplit, the decomposition group is isomorphic to the Galois group, which is noncyclic. Since it is unramified, the inertia group is trivial and so the decomposition group is isomorphic to the Galois group of the residue fields, which must be cyclic. This is a contradiction. □

2 If $L|K$ is a Galois extension of algebraic number fields, and $\mathfrak{P}$ a prime ideal which is unramified over K (i.e., $\mathfrak{p} = \mathfrak{P} \cap K$ is unramified in L), then there is one and only one automorphism $\varphi_{\mathfrak{P}} \in \mathrm{Gal}(L|K)$ such that

$$\varphi_{\mathfrak{P}} a \equiv a^q \bmod \mathfrak{P} \quad \textbf{for all } a \in \mathcal{O},$$

where $q = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$. It is called the *Frobenius automorphism.* The decomposition group $G_{\mathfrak{P}}$ is cyclic and $\varphi_{\mathfrak{P}}$ is a generator of $G_{\mathfrak{P}}$.

There is a typo: the q should be $|\kappa(\mathfrak{p})|$.

Proof: Since $\mathfrak{p}$ is unramified, the decomposition group $G_{\mathfrak{P}}$ is isomorphic to the Galois group of the reside fields $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$, which is cyclic and generated by the *Frobenius automorphism* $x \mapsto x^q$. The corresponding generator in $G_{\mathfrak{P}}$ is the required Frobenius automorphism. □

3 (F. K. Schmidt's theorem) Let $L|K$ be a solvable extension of prime degree p (not necessarily Galois). If the unramified prime ideal $\mathfrak{p}$ in L has two prime factors $\mathfrak{P}$ and $\mathfrak{P}'$ of degree 1, then it is already totally split.

Proof: Let $N|K$ be the Galois closure of $L|K$. By Exercise 8.4, it suffices to show $\mathfrak{p}$ is totally split in N. □

II

The Theory of Valuations

§ 1 The p-adic Numbers

I Review

(1.1) Definition Fix a prime number p. A ***p-adic integer*** is a formal infinite series

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

where $0 \leqslant a_i < p$, for all $i = 0, 1, 2, \cdots$. The set of all p-adic integers is denoted by $\mathbb{Z}_p$.

The ***p-adic expansion*** of positive integers is computed by successively dividing by p.

(1.2) Proposition *The residue classes $a \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$ can be uniquely represented in the form*

$$a \equiv a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \bmod p^n,$$

where $0 \leqslant a_i < p$, for $i = 0, 1, 2, \cdots, n-1$.

Every rational number $f \in \mathbb{Z}_{(p)}$ defines a sequence of residue classes

$$\overline{s_n} = f \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad , n = 1, 2, \cdots$$

By (1.2), they can be written as

$$\overline{s_n} = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} \bmod p^n, \quad , n = 1, 2, \cdots$$

with uniquely determined coefficients $a_0, a_1, \cdots \in \{0, 1, \cdots, p-1\}$. Then the p-adic integer

$$a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$$

is called the ***p-adic expansion*** of f. In this way, one has:

$$\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p.$$

(1.3) Proposition *Associating to every p-adic integer*

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu$$

the sequence $(\overline{s_n})$ of residue classes

$$\overline{s_n} = \sum_{\nu=0}^{n-1} a_\nu p^\nu \bmod p^n \in \mathbb{Z}/p^n\mathbb{Z}$$

yields a bijection

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

This identification translates the ring structure of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}_p$. One can view elements in the later set as ***p*-adic expansion** of the former one.

Under this identification, $\mathbb{Z} \subset \mathbb{Z}_p$ is the subring of $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ consisting of tuples

$$(a \bmod p, a \bmod p^2, a \bmod p^3, \cdots) \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Remark: The fraction field of $\mathbb{Z}_p$ is denoted by $\mathbb{Q}_p$ and its elements are called ***p*-adic numbers**. Note that $\mathbb{Z}_p$ is not the integral closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ since $\mathbb{Z}_p$ is uncountable.

(1.4) Proposition *Let $F(x_1, \cdots, x_n)$ be a polynomial with integer coefficients, and fix a prime number p. The congruence*

$$F(x_1, \cdots, x_n) \equiv 0 \bmod p^\nu$$

is solvable for arbitrary $\nu \geqslant 1$ if and only if the equation

$$F(x_1, \cdots, x_n) = 0$$

is solvable in p-adic integers.

Assume one has a solution $\{x_\nu\}$ of the congruence

$$F(x) \equiv 0 \bmod p^\nu.$$

Then a solution $y = (y_k) \in \mathbb{Z}_p$ of the equation

$$F(x) = 0$$

is given by the following process.

$$\begin{tikzcd}
\{x_\nu^{(k)}\} \arrow[r, equal] & y_k \bmod p^k \arrow[dd, dotted] & \in & \mathbb{Z}/p^k\mathbb{Z} \arrow[dd] \\
\cap & & & \\
\vdots & \vdots \arrow[dd, dotted] & & \vdots \arrow[dd] \\
\cap & & & \\
\{x_\nu^{(2)}\} \arrow[r, equal] & y_2 \bmod p^2 \arrow[dd, dotted] & \in & \mathbb{Z}/p^2\mathbb{Z} \arrow[dd] \\
\cap & & & \\
\{x_\nu^{(1)}\} \arrow[r, equal] & y_1 \bmod p & \in & \mathbb{Z}/p\mathbb{Z}
\end{tikzcd}$$

II Exercises

1 A p-adic number $a = \sum_{\nu=-m}^{\infty} a_\nu p^\nu \in \mathbb{Q}_p$ is a rational number if and only if the sequence of digits is periodic (possibly with a finite string before the first period).

Proof: After multiplying by a power of p, it suffices to prove this proposition for p-adic integers. Let $a = \sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p$.

If the sequence (a_ν) is periodic, say $a_{\nu+k} = a_\nu$ for all $\nu \geqslant n_0$. Then

$$\sum_{\nu=0}^{N-1} a_\nu p^\nu \equiv \sum_{\nu=0}^{n_0-1} a_\nu p^\nu + \left(\sum_{\nu=0}^{k-1} a_{n_0+\nu} p^\nu\right) \left(\sum_{\nu=0}^{[\frac{N-n_0}{k}]} p^{n_0+k\nu}\right) \operatorname{mod} p^N$$

for large N. Thus

$$a = \sum_{\nu=0}^{n_0-1} a_\nu p^\nu + \left(\sum_{\nu=0}^{k-1} a_{n_0+\nu} p^\nu\right) \frac{p^{n_0}}{1-p^k} \in \mathbb{Z}_{(p)}.$$

Conversely, if $a = \frac{x}{y} \in \mathbb{Z}_{(p)}$, we need to show its p-adic expansion is periodic.

First, the p-adic expansions of integers are periodic byLemmas 1.1 and 1.2.

If $-1 < a < 0$, then there exists $z \in \mathbb{N}$ such that $yz = p^r - 1$ for some r. Let $d = -ac$, then $0 < d < p^r - 1$, thus the p-adic expansion of $a = \frac{d}{1-p^r}$ is

$$\sum_{\nu=0}^{\infty} dp^{r\nu},$$

which is obviously periodic.

As for positive rational number a with nontrivial denominator, there exists a positive integer b such that $-1 < a - b < 0$. Then a is the sum of a positive integer, whose p-adic expansion terminates, and a rational number with periodic p-adic expansion. Thus the p-adic expansion of a is periodic.

As for negative rational number a with nontrivial denominator, there exists a positive integer b such that $a + b$ is a positive rational number. Let $\sum_{\nu=0}^{\infty} b_\nu p^\nu$ and $\sum_{\nu=0}^{\infty} c_\nu p^\nu$ be the p-adic expansions of b and $a + b$. By Lemma 1.2, there exists a $N \in \mathbb{N}$ such that $c_N \neq 0$ and $p^N > b$. Now a is the sum of a positive integer $\sum_{\nu=0}^{N} c_\nu p^\nu - b$ and a rational number with periodic p-adic expansion $\sum_{\nu=N+1}^{\infty} c_\nu p^\nu$. Therefore the p-adic expansion of a is periodic. □

1.1 Lemma *If $a \in \mathbb{Q}_p$ has p-adic expansion $\sum_{\nu=-m}^{\infty} a_\nu p^\nu$, then the p-adic expansion of $-a$ is $\sum_{\nu=-m}^{\infty} b_\nu p^\nu$, where $b_{-m} = p - a_{-m}$ and $b_\nu = p - 1 - a_\nu$ for all $\nu > -m$.*

1.2 Lemma *A p-adic number $a = \sum_{\nu=-m}^{\infty} a_\nu p^\nu \in \mathbb{Q}_p$ terminates (i.e., $a_\nu = 0$ for large ν) if and only if a is a positive rational number whose denominator is a power of p.*

Proof: The "if" follows immediately from Definition (1.1). Conversely, if a p-adic number $a = \sum_{\nu=-m}^{\infty} a_\nu p^\nu$ terminates, say $a_\nu = 0$ for all $\nu \geqslant N$. Then consider $a' = \sum_{\nu=-m}^{N-1} a_\nu p^\nu$, which is a positive rational number whose denominator is a power of p. One can see that the p-adic expansion of a' is nothing but a. □

2 A p-adic integer $a = a_0 + a_1 p + a_2 p^2 + \cdots$ is a unit in the ring $\mathbb{Z}_p$ if and only if as $a_0 \neq 0$.

Proof: This follows form the fact that a sequence $(\overline{s_1}, \overline{s_2}, \cdots)$ is a unit in the inverse limit $\varprojlim A/I^n$ if and only if $\overline{s_1}$ is a unit in A/I. This fact follows from the following lemma. □

2.1 Lemma *Let A be a ring, I a nilpotent ideal. Then an element $x \in A$ is a unit if and only if its reduction in A/I is a unit.*

Proof: It suffices to prove the "if". If the reduction of x in A/I is a unit. Then there exists a $y \in A$ and $z \in I$ such that $xy = 1 + z$. However, since I is nilpotent, $1 + z$ has an inverse

$$(1+z)^{-1} = 1 + z + z^2 + \cdots \in A.$$

Therefore x has an inverse $y(1+z)^{-1}$ and is a unit. □

3 Show that the equation $x^2 = 2$ has a solution in $\mathbb{Z}_7$.

Proof: It suffices to show that the congruence $x^2 \equiv 2 \bmod 7^\nu$ is solvable for arbitrary $\nu \geqslant 1$. First, the congruence $x^2 \equiv 2 \bmod 7$ has a solution $x \equiv 3 \bmod 7$. Then follows from the following Proposition 3.1. □

3.1 Proposition *If p is an odd prime, $p \nmid a$, and $p \nmid n$, then if $x^n \equiv a \bmod p$ is solvable, so is $x^n \equiv a \bmod p^\nu$ for all $\nu \geqslant 1$.*

Proof: We use induction on $\nu \geqslant 1$. Assume the congruence $x^n \equiv a \bmod p^\nu$ has a solution x_ν. Let $x_{\nu+1} = x_\nu + bp^\nu$. Then

$$x_{\nu+1}^n \equiv x_\nu^n + nbp^\nu x_\nu^{n-1} \bmod p^{\nu+1}.$$

Then $x_{\nu+1}$ is a solution of the congruence $x^n \equiv a \bmod p^{\nu+1}$ if there exists an integer b such that

$$nbx_\nu^{n-1} \equiv p^{-\nu}(a - x_\nu^n) \bmod p.$$

Since $p^{-\nu}(a - x_\nu^n)$ is an integer and $p \nmid nx_\nu^{n-1}$, such an integer b exists. □

4 Write the numbers 3 and -3 as 5-adic numbers.

Proof: The 5-adic expansion of 3 is $3 + 0 \cdot 5 + 0 \cdot 5^2 + \cdots$. By Lemma 1.1, the 5-adic expansion of -3 is $2 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots$. □

5 The field $\mathbb{Q}_p$ of p-adic numbers has no automorphisms except the identity.

Proof: Let σ be an automorphism of $\mathbb{Q}_p$. Then it must be trivial on $\mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, it remains to show σ is continuous.

First, σ maps units of $\mathbb{Z}_p$ to units of $\mathbb{Z}_p$ by Lemma 5.1. Then for any $x \in \mathbb{Q}_p^*$, writing $x = p^{v_p(x)}u$ with u a unit, one has

$$\sigma(x) = \sigma(p^{v_p(x)}u) = p^{v_p(x)}\sigma(u),$$

and thus $v_p(\sigma(x)) = v_p(x)$, which shows σ is continuous. □

5.1 Lemma *For any $\alpha \in \mathbb{Q}_p^*$, the followings are equivalent*

1. *α is a unit, i.e. $\alpha \in \mathbb{Z}_p^*$;*
2. *α has n-th roots in $\mathbb{Q}_p$ for infinitely many n.*

Proof: *1.⇒2.*. Let α be a unit. Then, by Hensel's Lemma, if $p \nmid n$ and $x^n - \alpha$ has a solution $\bmod p$, then it has a solution $x \in \mathbb{Z}_p$. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$, thus for any n relative prime to $p-1$, $x^n - \alpha$ has a solution $\bmod p$. Therefore, for any n relative prime to $p(p-1)$, $x^n - \alpha$ has a solution $x \in \mathbb{Z}_p$.

Conversely, if $x^n - \alpha$ has a solution in $\mathbb{Q}_p$, then $v_p(\alpha) = v_p(x^n) = nv_p(x)$. Since there are only finitely many n divides a nonzero integer, $v_p(\alpha)$ must equals 0. □

Recall how one proves the similar result for real numbers.

5.2 Proposition *The only automorphism of the field $\mathbb{R}$ of real numbers is the identity.*

Proof: Let σ be an automorphism of $\mathbb{R}$, then it must be trivial on $\mathbb{Q}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, it remains to show σ is continuous.

For any $x \geqslant 0$, there exists y such that $x = y^2$, thus $\sigma(x) = \sigma(y)^2 \geqslant 0$. Therefore, for any $x \geqslant y$, one has $\sigma(x) \geqslant \sigma(y)$. This shows that σ preserves the order on $\mathbb{R}$ and hence σ is continuous. □

As squares are important step in the proof, we introduce the following lemma.

5.3 Lemma *Let $p > 2$, then $x \in \mathbb{Z}_p$ if and only if $1 + px^2$ is a square in $\mathbb{Q}_p$. $x \in \mathbb{Z}_2$ if and only if $1 + 8x^2$ is a square in $\mathbb{Q}_2$.*

Proof: If $x \notin \mathbb{Z}_p$, then $v_p(1 + px^2) = 1 + 2v_p(x)$ is odd, thus $1 + px^2$ can not be a square. Conversely, if $x \in \mathbb{Z}_p$, then $\alpha = 1 + px^2 \in \mathbb{Z}_p$. Consider the polynomial $f(y) = y^2 - \alpha$. When $\bmod p$, it has a solution $y \equiv 1 \bmod p$. Therefore, by Hensel's Lemma, there exists a $y \in \mathbb{Z}_p$ such that $y^2 - \alpha = 0$, which shows that $1 + px^2$ is a square.

The above argument fails when $p = 2$ since in this case $f'(y) \equiv 0 \bmod 2$, thus the Hensel's lifting fails. So we consider $1+8x^2$ instead. If $x \notin \mathbb{Z}_2$, then either $v_2(x) \leqslant -2$ and thus $v_2(1 + 8x^2) = 3 + 2v_2(x)$ is odd, or $v_2(x) = -1$ and thus $1 + 8x^2$ is an odd 2-adic integer $\not\equiv 1 \bmod 4$. In either case, $1 + 8x^2$ can not be a square. If $x \in \mathbb{Z}_2$, then $\beta = 1 + 8x^2 \in \mathbb{Z}_2$. Consider the polynomial $g(y) = y^2 - \beta$. When $\bmod 8$, it has a solution $y \equiv 1 \bmod 8$. Note that $g'(y) = 2y$. Therefore, by Hensel's Lemma, there exists a $y \in \mathbb{Z}_2$ such that $y^2 - \beta = 0$, which shows that $1 + 8x^2$ is a square. □

Proof (of Exercise 5): Let σ be an automorphism of $\mathbb{Q}_p$, it remains to show σ is continuous.

First σ maps p-adic integers to p-adic integers. Indeed, if $1 + px^2 = y^2$ or $1 + 8x^2 = y^2$, then $1 + p\sigma(x)^2 = \sigma(y)^2$ or $1 + 8\sigma(x)^2 = \sigma(y)^2$. Then, by Lemma 5.3, $\sigma(\mathbb{Z}_p) = \mathbb{Z}_p$. Then $\sigma(p^k\mathbb{Z}_p) = p^k\mathbb{Z}_p$, which shows σ is continuous. □

6 How is the addition, subtraction, multiplication and division of rational numbers reflected in the representation by p-adic digits?

Proof: The addition, subtraction, multiplication and division of p-adic expansions are like the corresponding operations on decimals except the order is from left to right instead of from right to left. □

§ 2 The p-adic Absolute Value

I Review

For any nonzero $a \in \mathbb{Q}$, write $a = p^m \frac{b}{c}$ such that $(bc, p) = 1$. Denote m by $v_p(a)$ and set $v_p(0) = \infty$, this defines a function

$$v_p \colon \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\},$$

the ***p-adic exponential valuation***. The ***p-adic absolute value*** is given by

$$\begin{aligned} |\ |_p \colon \mathbb{Q} &\longrightarrow \mathbb{R} \\ a &\longmapsto p^{-v_p(a)}. \end{aligned}$$

(2.1) Proposition *For every rational number $a \neq 0$, one has*

$$\prod_p |a|_p = 1,$$

where p varies over all prime numbers as well as the symbol ∞.

The notation $|\ |_\infty$ for the ordinary absolute value is motivated by the analogy of the field of rational numbers $\mathbb{Q}$ with the rational function field $k(t)$.

For any prime ideal $\mathfrak{p}$ of $k[t]$, which is given by a monic irreducible polynomials $p(t) \in k[t]$, one has $\mathfrak{p}$-*adic exponential valuation* defined as follows. For any $f(t) \in k(t)$, write $f(t) = p(t)^m \frac{g(t)}{h(t)}$ with $g(t), h(t) \in k[t]$ and $(gh, p) = 1$. Denote this m by $v_\mathfrak{p}(f)$. Further, $v_\mathfrak{p}(0) = \infty$.

The $\mathfrak{p}$-*adic absolute value* is defined by

$$\begin{aligned} |\ |_\mathfrak{p} \colon k(t) &\longrightarrow \mathbb{R} \\ f &\longmapsto q_\mathfrak{p}^{-v_\mathfrak{p}(f)}. \end{aligned}$$

where $q_\mathfrak{p} = q^{d_\mathfrak{p}}$, $d_\mathfrak{p}$ being the degree of the residue class field of $\mathfrak{p}$ over k and q a fixed real number > 1.

One more exponential valuation v_∞ defined as follows. For any nonzero $f(t) \in k(t)$, $v_\infty(f) = \deg(h) - \deg(g)$, where $f(t) = \frac{g(t)}{h(t)}$ with $g(t), h(t) \in k[t]$. One can see $v_\infty(f)$ is the difference of the order of zero, resp. pole, of $f(t)$ at the point at infinity.

This is also the $\mathfrak{p}$-adic exponential valuation associated to the prime ideal $\mathfrak{p} = (\frac{1}{t})$ of the ring $k[\frac{1}{t}]$. Indeed, if $f(t) = \frac{g(t)}{h(t)}$ with $g(t), h(t) \in k[t]$, then

$$f(t) = (\frac{1}{t})^{\deg(h) - \deg(g)} \frac{\widetilde{g}(\frac{1}{t})}{\widetilde{h}(\frac{1}{t})},$$

where $\widetilde{g}(\frac{1}{t}) = (\frac{1}{t})^{\deg(g)} g(t) \in k[\frac{1}{t}]$ and $\widetilde{h}(\frac{1}{t}) = (\frac{1}{t})^{\deg(h)} h(t) \in k[\frac{1}{t}]$. One can check that $(\widetilde{gh}, \frac{1}{t}) = 1$. Then $v_{\mathfrak{p}}(f) = \deg(h) - \deg(g)$.

Putting $|f|_\infty = q^{-v_\infty(f)}$, one has:

$$\prod_{\mathfrak{p}} |a|_{\mathfrak{p}} = 1,$$

where $\mathfrak{p}$ varies over the prime ideals of $k[t]$ as well as the symbol ∞.

(2.2) Proposition *The field $\mathbb{Q}_p$ of p-adic numbers is complete with respect to the absolute value $|\ |_p$, i.e., every Cauchy sequence in $\mathbb{Q}_p$ converges with respect to $|\ |_p$.*

Here the analytic definition of $\mathbb{Q}_p$ is the quotient $R/\mathfrak{m}$, where R is the ring of all Cauchy sequences and $\mathfrak{m}$ is the maximal ideal consisting of all nullsequences.

(2.3) Proposition *The set*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x|_p \leqslant 1\}$$

is a subring of $\mathbb{Q}_p$. It is the closure with respect to $|\ |_p$ of the ring $\mathbb{Z}$ in the field $\mathbb{Q}_p$.

(2.4) Proposition *The nonzero ideals of the ring $\mathbb{Z}_p$ are the principal ideals*

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p | v_p(x) \geqslant n\},$$

with $n \geqslant 0$, and one has

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

This gives the projections $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ and thus the canonical homomorphism $\mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

(2.5) Proposition *The homomorphism*

$$\mathbb{Z}_p \longrightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

is an isomorphism.

Via p-adic expansions, one has

(2.6) Proposition *There is a canonical isomorphism*

$$\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X - p).$$

II Exercises

1 $|x-y|_p \geqslant ||x|_p - |y|_p|$.

Proof: It is equivalent to show $|x+y|_p \leqslant |x|_p + |y|_p$. One can see $v_p(x+y) \geqslant \min\{v_p(x), v_p(y)\}$, therefore $|x+y|_p \leqslant \max\{|x|_p, |y|_p\} \leqslant |x|_p + |y|_p$. □

2 **Let n be a natural number, $n = a_0 + a_1 p + \cdots + a_{r-1}p^{r-1}$ its p-adic expansion, with $0 < a_i < p$, and $s = a_0 + a_1 + \cdots + a_{r-1}$. Show that $v_p(n!) = \frac{n-s}{p-1}$.**

Proof: One can see that

$$\begin{aligned} v_p(n!) &= v_p(1) + v_p(2) + \cdots + v_p(n) \\ &= \left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2\left(\left[\frac{n}{p^2}\right] - \left[\frac{n}{p^3}\right]\right) + \cdots \\ &= \sum_{k=1}^{\infty} k \left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right) \\ &= \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]. \end{aligned}$$

On the other hand, one has

$$\begin{aligned} \left[\frac{n}{p}\right] &= a_1 + a_2 p + \cdots + a_{r-1}p^{r-2}, \\ \left[\frac{n}{p^2}\right] &= \qquad a_2 + \cdots + a_{r-1}p^{r-3}, \\ &\vdots \\ \left[\frac{n}{p^{r-1}}\right] &= \qquad\qquad a_{r-1}. \end{aligned}$$

Therefore

$$\begin{aligned} v_p(n!) &= a_1 + a_2(p+1) + \cdots + a_{r-1}(p^{r-2} + p^{r-3} + \cdots + 1) \\ &= \frac{a_1(p-1) + a_2(p^2-1) + \cdots + a_{r-1}(p^{r-1}-1)}{p-1} \\ &= \frac{n-s}{p-1}. \end{aligned}$$

□

3 **The sequence $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \cdots$ does not converge in $\mathbb{Q}_p$. for any p.**

Proof: It suffices to show $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \cdots$ is not a Cauchy sequence.

Since $v_2(\frac{1}{10^m} - \frac{1}{10^n}) = v_5(\frac{1}{10^m} - \frac{1}{10^n}) = -\max\{m, n\} \leqslant 0$. The sequence is obviously not a Cauchy sequence in $\mathbb{Q}_2$ or $\mathbb{Q}_5$. As for $p \neq 2, 5$, note that $v_p(\frac{1}{10^{n+1}} - \frac{1}{10^n}) = v_p(9)$ is a constant for all n, thus the sequence is not a Cauchy sequence. □

4 Lets $\varepsilon \in 1 + p\mathbb{Z}_p$, and let $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots$ be a p-adic integer, and write $s_n = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$. Show that the sequence ε^{s_n} converges to a number ε^α in $1 + p\mathbb{Z}_p$. Show furthermore that $1 + p\mathbb{Z}_p$ is thus turned into a multiplicative $\mathbb{Z}_p$-module.

Proof: To show the sequence ε^{s_n} converges to a number ε^α in $\mathbb{Z}_p$, it suffices to show it is a Cauchy sequence. Let $\varepsilon = 1 + px$. For any $m \geqslant n$, one has

$$\begin{aligned}\varepsilon^{s_m} - \varepsilon^{s_n} &= \varepsilon^{s_n}(\varepsilon^{s_m - s_n} - 1) \\ &= \varepsilon^{s_n}\left((s_m - s_n)(px) + \cdots + (px)^{s_m - s_n}\right).\end{aligned}$$

Therefore

$$\begin{aligned}\left|\varepsilon^{s_m} - \varepsilon^{s_n}\right|_p &= \left|(s_m - s_n)(px)\right|_p \\ &= \left|s_m - s_n\right|_p |px|_p.\end{aligned}$$

Here s_n is a Cauchy sequence and $|px|_p$ is a constant. Thus ε^{s_n} is a Cauchy sequence.

To show $\varepsilon^\alpha \in 1 + p\mathbb{Z}_p$, we need to show $|\varepsilon^\alpha - 1|_p < 1$. For large n, one has

$$|\varepsilon^{s_n} - 1|_p = |s_n|_p |px|_p = |\alpha|_p |px|_p,$$

which is a constant. Thus $|\varepsilon^\alpha - 1|_p = |\alpha|_p |px|_p < 1$. □

5 For every $a \in \mathbb{Z}$, $(a, p) = 1$, the sequence $\{a^{p^n}\}_{n \in \mathbb{N}}$ converges in $\mathbb{Q}_p$.

Proof: It suffices to show $\{a^{p^n}\}_{n \in \mathbb{N}}$ is a Cauchy sequence. Since $(a, p) = 1$, one has $a^{p-1} \equiv 1 \bmod p$. Asssume $a^{p-1} = 1 + px$. For any $m > n$, one has

$$\begin{aligned}a^{p^m} - a^{p^n} &= a^{p^n}(a^{p^m - p^n} - 1) \\ &= a^{p^n}\left(\left(a^{p-1}\right)^{\frac{p^m - p^n}{p-1}} - 1\right) \\ &= a^{p^n}\left(\frac{p^m - p^n}{p-1}(px) + \cdots + (px)^{\frac{p^m - p^n}{p-1}}\right).\end{aligned}$$

Therefore, for any $\varepsilon > 0$ and $m > n > -\log_p \varepsilon$, one has

$$\begin{aligned} |a^{p^m} - a^{p^n}|_p &= \left| \frac{p^m - p^n}{p-1} px \right|_p \\ &= |p^{n+1}x|_p < p^{-n} < \varepsilon, \end{aligned}$$

which shows a^{p^n} is a Cauchy sequence. □

6 The fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$. are not isomorphic, unless $p = q$.

Proof: If there exists an isomorphism $\phi\colon \mathbb{Q}_p \to \mathbb{Q}_q$, then it must be identity on $\mathbb{Q}$. Furthermore, $\sqrt{n} \in \mathbb{Q}_p$ if and only if $\sqrt{n} \in \mathbb{Q}_q$, which is wrong when $p \neq q$. Indeed, $\sqrt{n} \in \mathbb{Q}_p$ if and only if n is quadratic residue modulo p. However, we have the following Lemma 6.1. □

6.1 Lemma *If p, q are distinct prime numbers, then there exists some integer n such that $\left(\frac{n}{p}\right) = 1$ and $\left(\frac{n}{q}\right) = -1$.*

Proof: Let a and b be integers satisfying $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{b}{q}\right) = -1$. Since $(p, q) = 1$, there exists integers x and y such that $xp + yq = a - b$. Then let $n = a - xp = b + yq$, one has $\left(\frac{n}{p}\right) = 1$ and $\left(\frac{n}{q}\right) = -1$. □

Another approach uses the following lemma

6.2 Proposition *When $p \neq 2$, $\mathbb{Q}_p^*$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/(p-1) \times \mathbb{Z}_p$, while $\mathbb{Q}_2^*$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}_2$.*

Proof: It is obvious that $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p^*$. Consider the short exact sequence

$$0 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^* \longrightarrow \mathbb{F}_p^* \longrightarrow 0.$$

By Hensel's lemma, the projection $\mathbb{Z}_p^* \to \mathbb{F}_p^*$ has a section which maps $\mathbb{F}_p^*$ to the subgroup $\mu_{p-1} = \{x \in \mathbb{Q}_p | x^{p-1} = 1\}$ of $\mathbb{Z}_p^*$. Therefore

$$\mathbb{Z}_p^* \cong (1 + p\mathbb{Z}_p) \times \mathbb{Z}/(p-1).$$

It remains to show $1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$ when $p \neq 2$ and $1 + 2\mathbb{Z}_2 \cong \mathbb{Z}/2 \times \mathbb{Z}_2$.

To do this, consider the series

$$\begin{aligned} \exp(x) &:= \sum_{n=0}^{\infty} \frac{x^n}{n!}, \\ \log(1+x) &:= \sum_{n=1}^{\infty} \frac{(-1)^{n-1}x^n}{n}. \end{aligned}$$

One can verify that $\exp(x)$ converges when $v_p(x) > \frac{1}{p-1}$, $\log(1+x)$ converges when $v_p(x) > 0$ and that $\exp(\log(x)) = x, \log(\exp(x)) = x$ when they converge.

In this way, one has

$$\begin{tikzcd} p\mathbb{Z}_p \arrow[r, shift left, "\exp"] & 1 + p\mathbb{Z}_p \arrow[l, shift left, "\log"] \end{tikzcd}$$

when $p \neq 2$, and

$$\begin{tikzcd} 4\mathbb{Z}_2 \arrow[r, shift left, "\exp"] & 1 + 4\mathbb{Z}_2. \arrow[l, shift left, "\log"] \end{tikzcd}$$

Note that $1 + 4\mathbb{Z}_2$ is precisely the kernel of the surjection

$$\begin{aligned} 1 + 2\mathbb{Z}_2 &\longrightarrow \mathbb{F}_2 \\ 1 + 2a &\longmapsto a \bmod 2. \end{aligned}$$

Therefore $1 + 2\mathbb{Z}_2 \cong \mathbb{Z}/2 \times (1 + 4\mathbb{Z}_2)$. □

6.3 Proposition *When $p \neq 2$, $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, while $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.*

Proof: Follows from Proposition 6.2 or Lemma 1.5.3. □

Proof (Exercise 6): If there exists an isomorphism $\phi\colon \mathbb{Q}_p \to \mathbb{Q}_q$, then it must be identity on $\mathbb{Q}$. Furthermore, ϕ will preserve the torsion subgroup of the multiplicative subgroup. By Proposition 6.2, this shows that $\mathbb{Q}_p \ncong \mathbb{Q}_q$ whenever $\{p, q\} \neq \{2, 3\}$. The remaining case follows from Proposition 6.3.□

7 The algebraic closure of $\mathbb{Q}_p$ has infinite degree.

Proof: It suffices to show there exists algebraic extension of $\mathbb{Q}_p$ of degree n for any natural number n. This follows immediately from the fact that $X^n - p$ is irreducible over $\mathbb{Q}_p$ for all integers $n > 1$. Indeed, $X^n - p$ is reducible over $\mathbb{Q}_p$ if and only if it is reducible over $\mathbb{Z}_p$. But p is a prime element in $\mathbb{Z}_p$, thus $X^n - p$ is irreducible by Proposition 7.1. □

7.1 Proposition (Eisenstein's criterion) *Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a monic polynomial over a domain R and $\mathfrak{p}$ is a prime ideal of R. Then if $f(X)$ is an* **Eisenstein polynomial with respect to $\mathfrak{p}$** *(cf.I.2.5.1), that menas $a_i \in \mathfrak{p}$ for $1 \leqslant i \leqslant n-1$ and $a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $f(X)$ is irreducible.*

Proof: Suppose there exists a nontrivial factorization $f(X) = g(X)h(X)$ over R. Then, modulo $\mathfrak{p}$, one gets a nontrivial factorization $X^n = \overline{g}(X)\overline{h}(X)$ over $R/\mathfrak{p}$. Let g_0, h_0 be the constant terms of $g(X)$ and $h(X)$ respectively, then $g_0h_0 = a_0$ and thus one of them and only one of them belongs to $\mathfrak{p}$, say $g_0 \in \mathfrak{p}$ and $h_0 \notin \mathfrak{p}$. Then $\overline{h}(X)$ has nontrivial constant term, which contradicts with $X^n = \overline{g}(X)\overline{h}(X)$. □

8 In the ring $\mathbb{Z}_p[[X]]$ of formal power series $\sum_{\nu=0}^{\infty} a_\nu X^\nu$ over $\mathbb{Z}_p$, one has the following *division with remainder*. Let $f, g \in \mathbb{Z}_p[[X]]$ and let $f(X) = a_0 + a_1 X + \cdots$ such that $p \mid a_\nu$ for $\nu = 0, \cdots, n-1$, but $p \nmid a_n$. Then one may write in a unique way

$$g = qf + r,$$

where $q \in \mathbb{Z}_p[[X]]$, and $r \in \mathbb{Z}_p[X]$ is a polynomial of degree $\leqslant n-1$.

This result holds for general complete local ring, see [Lan02].

Proof: Let τ be the operator $\tau(\sum_{\nu=0}^{\infty} b_\nu X^\nu) = \sum_{\nu=n}^{\infty} b_\nu X^{\nu-n}$. It suffices to show there exists a unique $q \in \mathbb{Z}_p[[X]]$ such that $\tau(g) = \tau(qf)$.

First, $U(X) = \tau(f(X)) = a_n + a_{n+1}X + \cdots$ is a unit in $\mathbb{Z}_p[[X]]$. This follows from the fact that $p \nmid a_n$, i.e. $a_n \in \mathbb{Z}_p^*$ and Lemma 1.2.1.

Write $f(X) = pP(X) + X^n U(X)$ with a polynomial $P(X)$ of degree $\leqslant n-1$. If $\tau(g) = \tau(qf)$, then

$$\begin{aligned}
\tau(g) &= \tau(pqP) + \tau(qX^nU) \\
&= p\tau(qP) + qU \\
&= \left(p + (\tau \circ \frac{P}{U})^{-1}\right)(\tau(qP)).
\end{aligned}$$

Furthermore,

$$\begin{aligned}
p(\tau \circ \frac{P}{U})(\tau(g)) &= \left(p^2(\tau \circ \frac{P}{U}) + p\right)(\tau(qP)), \\
p^2(\tau \circ \frac{P}{U})^2(\tau(g)) &= \left(p^3(\tau \circ \frac{P}{U})^2 + p^2(\tau \circ \frac{P}{U})\right)(\tau(qP)), \\
&\cdots
\end{aligned}$$

Hence

$$\begin{aligned}
&\left(\sum_{i=0}^{\infty}(-1)^i p^i (\tau \circ \frac{P}{U})^i\right)(\tau(g)) \\
=&\left(\sum_{i=0}^{\infty}(-1)^i p^{i+1}(\tau \circ \frac{P}{U})^i + (-1)^i p^i (\tau \circ \frac{P}{U})^{i-1}\right)(\tau(qP)) \\
=&(\tau \circ \frac{P}{U})^{-1}(\tau(qP)) = qU.
\end{aligned}$$

Therefore

$$q = \frac{1}{U}\left(\sum_{i=0}^{\infty}(-1)^i p^i (\tau \circ \frac{P}{U})^i\right)(\tau(g)).$$

Conversely, it is easy to see for such a q, $\tau(qf) = \tau(g)$. □

9 (p-adic Weierstrass Preparation Theorem) Every nonzero power series

$$f(X) = \sum_{\nu=0}^{\infty} a_\nu X^\nu \in \mathbb{Z}_p[[X]]$$

admits a unique representation

$$f(X) = p^\mu P(X)U(X),$$

where $U(X)$ is a unit in $\mathbb{Z}_p[[X]]$ and $P(X) \in \mathbb{Z}_p[X]$ is a monic polynomial satisfying $P(X) = X^n \bmod p$.

This result holds for general complete local ring, see [Lan02].

Proof: First of all, divided by a power of p, we may assume there exists an integer n such that $p \nmid a_n$ and $p \mid a_\nu$ for $\nu = 0, \cdots, n-1$. It remains to show $f(X)$ admits a unique representation $f(X) = P(X)U(X)$.

By Exercise 8, there exists a unique factorization

$$X^n = qf + r,$$

where $q \in \mathbb{Z}_p[[X]]$, and $r \in \mathbb{Z}_p[X]$ is a polynomial of degree $\leqslant n-1$. Note that $r \in \mathfrak{p}[X]$.

Assume $q(X) = b_0 + b_1 X + \cdots$, then $1 \equiv b_0 a_n \bmod p$. Thus q is a unit in $\mathbb{Z}_p[[X]]$. We obtain

$$f = (X^n - r)q^{-1},$$

where $X^n - r$ is a monic polynomial satisfying $X^n - r = X^n \bmod p$. □

§ 3 Valuations

I Review

(3.1) Definition A ***valuation*** of a field K is a function

$$|\ |\colon K \to \mathbb{R}$$

enjoying the properties

(i) $|x| \geqslant 0$ and $|x| = 0 \iff x = 0$,

(ii) $|xy| = |x||y|$,

(iii) "***triangle inequality***": $|x + y| \leqslant |x| + |y|$.

Remark: Besides the term ***valuation***, the terms ***absolute value***, ***norm*** and ***magnitude*** are also used.

An ***exponential valuation*** of K is a function

$$v\colon K \to \mathbb{R} \cup \{\infty\}$$

enjoying the properties

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x + y) \geqslant \min\{v(x), v(y)\}$.

Remark: The term ***valuation*** is also used to refer v, in this case, $|\ |$ is usually called ***absolute value***, ***norm*** or ***magnitude***.

(3.2) Definition Two valuations of K are called *equivalent* if they define the same topology on K.

The topology on K defined by a valuation $|\ |$ is the metric topology induced by the distance

$$d(x, y) := |x - y|.$$

(3.3) Proposition *Two valuations $|\ |_1$, and $|\ |_2$ on K are equivalent if and only if there exists a real number $s > 0$ such that one has*

$$|x|_1 = |x|_2^s$$

for all $x \in K$.

Remark: Another equivalent condition arises from the proof:

$$|x|_1 < 1 \Longrightarrow |x|_2 < 1.$$

(3.4) Approximation Theorem *Let $|\ |_1, \cdots, |\ |_n$ be pairwise inequivalent valuations of the field K and let $a_1, \cdots, a_n \in K$ be given elements. Then for every $\varepsilon > 0$ there exists an $x \in K$ such that*

$$|x - a_i|_i < \varepsilon, \quad \forall i = 1, \cdots, n.$$

(3.5) Definition The valuation $|\ |$ is called ***nonarchimedean*** if $|n|$ is bounded, for all $n \in \mathbb{N}$. Otherwise it is called ***archimedean***.

(3.6) Proposition *The valuation $|\ |$ is nonarchimedean if and only if it satisfies the* **strong triangle inequality**

$$|x + y| \leqslant \max\{|x|, |y|\}.$$

Remark: The strong triangle inequality immediately implies that

$$|x| \neq |y| \Longrightarrow |x + y| = \max\{|x|, |y|\}.$$

One may extend the nonarchimedean valuation $|\ |$ of K to a valuation of the function field $K(t)$ in a canonical way by setting, for a polynomial $f(t) = a_0 + a_lt + \cdots + a_nt^n$,

$$|f| = \max\{|a_0|, \cdots, |a_n|\}.$$

A.1 Proposition (On archimedean norm) *A*

(3.7) Proposition *Every valuation of $\mathbb{Q}$ is equivalent to one of the valuations $|\ |_p$ or $|\ |_\infty$.*

Let $|\ |$ be a nonarchimedean valuation of the field K. Putting

$$v(x) = -\log|x| \quad \text{for } x \neq 0, \quad \text{and } v(0) = \infty,$$

we obtain an *exponential valuation* of K.

Conversely, for every exponential valuation v we obtain a valuation by putting

$$|x| = q^{-v(x)}$$

for some fixed real number $q > 1$.

(3.8) Proposition *The subset*

$$\mathcal{O} = \{x \in K | v(x) \geqslant 0\} = \{x \in K | |x| \leqslant 1\}$$

is a ring with group of units

$$\mathcal{O}^* = \{x \in K | v(x) = 0\} = \{x \in K | |x| = 1\}$$

and the unique maximal ideal

$$\mathfrak{p} = \{x \in K | v(x) > 0\} = \{x \in K | |x| > 1\}.$$

$\mathcal{O}$ is an integral domain with field of fractions K and has the property that, for every $x \in K$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. Such a ring is called a ***valuation ring***. Its only maximal ideal is $\mathfrak{p} = \{x \in \mathcal{O} | x^{-1} \notin \mathcal{O}\}$. The field $\mathcal{O}/\mathfrak{p}$ is called the residue class field of $\mathcal{O}$. A valuation ring is always integrally closed.

An exponential valuation v is called ***discrete*** if it admits a smallest positive value s. It is called ***normalized*** if $s = 1$.

For a normalized valuation v, a ***prime element***, or ***uniformizing parameter*** is an element $\pi \in \mathcal{O}$ such that $v(\pi) = 1$. Every element $x \in K^*$ admits a unique representation

$$x = u\pi^{v(x)}$$

with $u \in \mathcal{O}^*$.

(3.9) Proposition *Let v be a discrete exponential valuation of K, then*

$$\mathcal{O} = \{x \in K | v(x) \geqslant 0\}$$

is a principal ideal domain, hence a discrete valuation ring (cf. I,(11.3)).

Suppose v is normalized. Then the nonzero ideals of $\mathcal{O}$ are given by

$$\mathfrak{p}^n = \pi^n \mathcal{O} = \{x \in K | v(x) \geqslant n\}$$

where π is a prime element. One has

$$\mathfrak{p}^n / \mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}.$$

In a discretely valued field K the chain

$$\mathcal{O} \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots$$

forms a basis of neighbourhoods of 0.

As a basis of neighbourhoods of 1 in K^*, there is a descending chain

$$\mathcal{O}^* = U^{(0)} \supset U^{(1)} \supset U^{(2)} \supset \cdots$$

with

$$U^{(n)} = 1 + \mathfrak{p}^n = \left\{ x \in K^* \middle| |1 - x| < \frac{1}{q^{n-1}} \right\}, \quad n > 0.$$

$U^{(n)}$ is called the n-th ***higher unit group*** and $U^{(1)}$ the group of ***principal units***.

(3.10) Proposition $\mathcal{O}^*/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^*$ *and* $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$, *for* $n \geqslant 1$.

II Exercises

1 Show that $|z| = (z\bar{z})^{1/2} = \sqrt{|N_{\mathbb{C}|\mathbb{R}}(z)|}$ is the only valuation of $\mathbb{C}$ which extends the absolute value $|\ |$ of $\mathbb{R}$.

Proof: Let $|\ |$ be a valuation of $\mathbb{C}$ which extends the absolute value of $\mathbb{R}$. It suffices to show that $|z| = 1$ for all $z \in S^1$, where $S^1 = \{e^{i\theta} | \theta \in \mathbb{R}\}$ denotes the unit circle of $\mathbb{C}$.

First of all $i^4 = 1$ implies $|i| = |1|^{\frac{1}{4}} = 1$. Then for any $\theta \in \mathbb{R}$, one has

$$|e^{i\theta}| \leqslant |\cos\theta| + |\sin\theta| \leqslant 2.$$

If $|e^{i\theta}| \neq 1$ for some $\theta \in \mathbb{R}$, then there must exists an integer n such that $|e^{i\theta}|^n > 2$. Then $|e^{in\theta}| = |e^{i\theta}|^n > 2$, which contradicts with the above inequality. □

2 What is the relation between the Chinese remainder theorem and the approximation theorem (3.4)**?**

Proof: Let $\mathcal{O}$ be a Dedekind domain with fraction field K. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be distinct prime ideals of $\mathcal{O}$. Putting

$$|x|_i = q^{-\operatorname{ord}_{\mathfrak{p}_i}(x)},$$

one gets pairwise inequivalent valuations $|\ |_1, \cdots, |\ |_n$ of the field K. Let $a_1, \cdots, a_n \in K$ be given elements. For $\varepsilon = q^{-m} > 0$, $|x - a_i|_i < \varepsilon$ means

$$x \equiv a_i \bmod \mathfrak{p}_i^m.$$

In this way, the approximation theorem can be viewed as a variant of the Chinese remainder theorem. □

3 Let k be a field and $K = k(t)$ the function field in one variable. Show that the valuations $v_{\mathfrak{p}}$ associated to the prime ideals $\mathfrak{p} = (p(t))$ of $k[t]$, together with the degree valuation v_∞, are the only valuations of K, up to equivalence. What are the residue class fields?

The statement is not correct since there may be nontrivial valuation on k. One should assume the valuation v is trivial on k. For instance, when k is a finite field, by Lemma 3.1, any valuation of K must be trivial on k.

Proof: Since a valuation of K which is trivial on k must be nonarchimedean, thus one can consider exponential valuations instead of valuations.

Let v be an exponential valuation of K with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{p}$.

If v is $k[t]$-***regular***, i.e. $k[t] \subset \mathcal{O}$. Then $\mathfrak{p} \cap k[t]$ is a non-zero prime ideal of $k[t]$, thus of the form $\mathfrak{p} = (p(t))$ for some monic irreducible polynomial $p(t)$. Consider the localization $k[t]_{\mathfrak{p}}$. Obviously, $k[t]_{\mathfrak{p}} \subset \mathcal{O}$. Conversely, any element of K can be written as a fraction f/g with $f, g \in k[t]$ and $(f, g) = 1$. Then $v(f/g) \geqslant 0$ implies $g \notin \mathfrak{p}$, which implies $p \nmid g$ and thus $\mathcal{O} \subset k[t]_{\mathfrak{p}}$.

If v is not $k[t]$-regular, since v is trivial on k, one must have $v(t) < 0$. We may assume $v(t) = -1$. For any polynomial $f(t) = a_n t^n + \cdots + a_0$, since $v(a_\nu t^\nu) = v(a_\nu) + \nu v(t) = -\nu$ for $0 \leqslant \nu \leqslant n$, one has $v(f) = -n = -\deg f$. Therefore $v = v_\infty$. □

3.1 Lemma *If k is a finite field, then there is no nontrivial valuation of k.*

Proof: Let $k = \mathbb{F}_q$, then for any $x \in k^*$, $x^{q-1} = 1$. Let $|\ |$ be a valuation of k, then $|x|^{q-1} = |x^{q-1}| = |1| = 1$. Since $|x| \geqslant 0$, one must have $|x| = 1$ for all $x \in k^*$. Thus $|\ |$ is trivial. □

4 Let $\mathcal{O}$ be an arbitrary valuation ring with field of fractions K, and let $\Gamma = K^*/\mathcal{O}^*$. Then Γ becomes a totally ordered group if we define $x \bmod \mathcal{O}^* \geqslant y \bmod \mathcal{O}^*$ to mean $x/y \in \mathcal{O}$.

Write Γ additively and show that the function

$$v\colon K \longrightarrow \Gamma \cup \{\infty\},$$

$v(0) = \infty$, $v(x) = x \bmod \mathcal{O}^*$ for $x \in K^*$, satisfies the conditions

1) $v(x) = \infty \Longrightarrow x = 0$,

2) $v(xy) = v(x) + v(y)$,

3) $v(x + y) \geqslant \min\{v(x), v(y)\}$.

v is called a *Krull valuation*.

Proof: Since for $x \in K^*$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$, Γ is a totally ordered group. 1), 2) are obvious. As for 3), assume $v(x) \geqslant v(y)$, which means $x/y \in \mathcal{O}$. Thus $(x + y)/y = x/y + 1 \in \mathcal{O}$, which means $v(x + y) \geqslant v(y)$ as desired. □

§ 4 Completions

I Review

(4.1) Definition valued field $(K, |\ |)$ is called ***complete*** if every Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$ in K converges to an element $a \in K$.

The ***completion*** $\widehat{K}$ of K is obtained by the quotient of the ring R of all Cauchy sequences on K by the maximal ideal $\mathfrak{m}$ of all nullsequences. The completion is the smallest extension of K which is complete. Consequently, K is dense in $\widehat{K}$.

(4.2) Ostrowski's Theorem *Let K be a field which is complete with respect to an archimedean valuation $|\ |$. Then there is an isomorphism σ from K to $\mathbb{R}$ or $\mathbb{C}$ satisfying*

$$|a| = |\sigma a|^s \quad \forall a \in K,$$

for some fixed $s \in (0, 1]$.

The extension of v on $\widehat{K}$ is given by

$$\widehat{v}(a) := \lim_{n\to\infty} v(a_n)$$

where $a = \lim a_n$ with $a_n \in K$. The sequence $v(a_n)$ for nonzero a has to become stationary, thus

$$v(K^*) = \widehat{v}(\widehat{K}^*),$$

and if v is discrete and normalized, then so is the extension $\widehat{v}$.

(4.3) Proposition *If $\mathcal{O} \subset K$, resp. $\widehat{\mathcal{O}} \subset \widehat{K}$, is the valuation ring of v, resp. of $\widehat{v}$, and $\mathfrak{p}$, resp. $\widehat{\mathfrak{p}}$, is the maximal ideal, then one has*

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p},$$

and, if v is discrete, one has furthermore

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n \quad for \quad n \geqslant 1.$$

p-adic expansion of an arbitrary discrete valuation v of the field K:

(4.4) Proposition *Let $R \subset \mathcal{O}$ be a system of representatives for $\kappa = \mathcal{O}/\mathfrak{p}$ such that $0 \in R$, and let $\pi \in \mathcal{O}$ be a prime element. Then every $x \neq 0$ in $\widehat{K}$ admits a unique representation as a convergent series*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$$

whereat $a_i \in R, a_0 \neq 0, m \in \mathbb{Z}$.

The following proposition shows that the valuation ring $\widehat{\mathcal{O}}$ of the completion $\widehat{K}$ is the $\mathfrak{p}$-*adic completion* of the valuation ring $\mathcal{O}$ of K.

(4.5) Proposition *Let K be complete with respect to a discrete valuation and $\mathcal{O}$ be the valuation ring with the maximal ideal $\mathfrak{p}$. Then, the canonical mapping*

$$\mathcal{O} \longrightarrow \varprojlim_n \mathcal{O}/\mathfrak{p}^n$$

is an isomorphism and a homeomorphism. The same is true for the mapping

$$\mathcal{O}^* \longrightarrow \varprojlim_n \mathcal{O}^*/U^{(n)}.$$

Valuation of a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{O}[x]$:

$$|f| := \max\{|a_0|, \cdots, |a_n|\}.$$

A polynomial is called ***primitive*** if $|f| = 1$.

(4.6) Hensel's Lemma *If a primitive polynomial $f(x) \in \mathcal{O}[x]$ admits modulo $\mathfrak{p}$ a factorization*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \bmod \mathfrak{p}$$

into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[x]$, then $f(x)$ admits a factorization

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

into polynomials $g, h \in \mathcal{O}[x]$ such that $\deg(g) = \deg(\overline{g})$ and

$$\overline{g}(x) \equiv g(x) \bmod \mathfrak{p} \quad \textit{and} \quad \overline{h}(x) \equiv h(x) \bmod \mathfrak{p}.$$

(4.7) Corollary *Let the field K be complete with respect to the nonarchimedean valuation $|\ |$. Then, for every irreducible polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ such that $a_0a_n \neq 0$, one has*

$$|f| = \max\{|a_0|, |a_n|\}.$$

In particular, $a_n = 1$ and $a_0 \in \mathcal{O}$ imply that $f \in \mathcal{O}[x]$.

(4.8) Theorem *Let K be complete with respect to the valuation $|\ |$. Then $|\ |$ may be extended in a unique way to a valuation of any given algebraic extension $L|K$. This extension is given by the formula*

$$|\alpha| = \sqrt[n]{N_{L|K}(\alpha)},$$

when $L|K$ has finite degree n. In this case L is again complete.

(4.9) Proposition *Let K be complete with respect to the valuation $|\ |$ and let V be an n-dimensional nonmed vector space over K. Then, for any basis $v_1, \cdots, v_n$ of V the maximum norm*

$$||x_1v_1 + \cdots + x_nv_n|| := \max\{|x_1|, \cdots, |x_n|\}$$

is equivalent to the given norm on V. In particular, V is complete and the isomorphism

$$K^n \longrightarrow V, \quad (x_1, \cdots, x_n) \mapsto x_1v_1 + \cdots + x_nv_n,$$

is a homeomorphism.

II Exercises

1 An infinite algebraic extension of a complete field K is never complete.

The following proof comes from [BGR84], but only works for algebraic extensions having infinite separable degree.

Proof: Let L be an infinite algebraic extension of a complete field K and have infinite separable degree. Then, we have a sequence of linearly independent elements $\{\alpha_n\}_{n\in\mathbb{N}}$ of L separable over K. Then one can find a sequence $\{c_n\}_{n\in\mathbb{N}}$ of nonzero constants in K such that

(i) $|c_n\alpha_n|$ is decreasing and $\lim_n |c_n\alpha_n| = 0$,

(ii) $|c_n\alpha_n| < r(\sum_{i=1}^{n-1} c_i\alpha_i)$.

Here r is defined as

$$r(\alpha) := \min_{\sigma\alpha\neq\alpha} |\alpha - \sigma\alpha|.$$

We claim that $\sum_{i=1}^{\infty} c_i\alpha_i$ has no limit in L, which contradicts the completeness of L. If such a limit exists, say α. Then

$$\left|\alpha - \sum_{i=1}^{n-1} c_i\alpha_i\right| \leqslant |c_n\alpha_n| < r(\sum_{i=1}^{n-1} c_i\alpha_i)$$

Thus, by *Krasner's lemma* (cf. Exercise 6.2), $\sum_{i=1}^{n-1} c_i\alpha_i \in K(\alpha)$. Since all coefficients c_i are non-zero, we get $\alpha_n \in K(\alpha)$ for all n. Therefore, $[K(\alpha) : K]$ is infinite which is impossible. □

Another approach is using the *Baire category theorem*. However, this only works for some special case.

Proof: Let L be an infinite algebraic extension of a complete field K satisfying conditions in Lemma 1.4. Then, its algebraic dimension is countable. This contradicts Theorem 1.2. □

Recall: A ***Baire space*** is a topological space in which the union of every countable collection of closed sets with empty interior has empty interior. This equals to say every intersection of countably many dense open sets is dense.

For a topological vector space V, its ***Hamel basis*** is a linearly independent subset spanning whole V. The ***algebraic dimension*** of V is the cardinality of the Hamel basis.

1.1 Lemma (Baire Category Theorem) *Every complete metric space is a Baire space.*

Proof: Let $\{U_n\}$ be a family of countably many dense open sets. It suffices to show that any nonempty open set V in X has a point x in common with all of the U_n.

First, since U_1 is dense, there exists an $x_1 \in X$ and $r_1 < 1$ such that

$$\overline{B}(x_1, r_1) \subset V \cap U_1,$$

where

$$\begin{aligned} B(x_1, r_1) &:= \{x \in X | |x - x_1| < r_1\}, \\ \overline{B}(x_1, r_1) &:= \{x \in X | |x - x_1| \leqslant r_1\}. \end{aligned}$$

Whenever $x_{n-1} \in X$ and $r_{n-1} < \frac{1}{n-1}$ are given, since U_n is dense, there exists an $x_n \in X$ and $r_n < \frac{1}{n}$ such that

$$\overline{B}(x_n, r_n) \subset B(x_{n-1}, r_{n-1}) \cap U_n.$$

As $\overline{B}(x_n, r_n) \subset B(x_{n-1}, r_{n-1})$, the sequence $\{x_n\}_{n\in\mathbb{N}}$ is Cauchy. Since X is complete, the sequence converges to a limit $x \in X$. By closeness of $\overline{B}(x_n, r_n)$, $x \in V \cap U_n$ for all n. □

1.2 Theorem *The algebraic dimension of an infinite-dimensional Banach Space over a complete field is uncountable.*

Proof: Let X be an infinite-dimensional Banach Space over a complete field K. Suppose X has countable Hamel basis $\{x_n\}_{n\in\mathbb{N}}$. Let

$$X_n := \operatorname{span}\{x_1, \cdots, x_n\}.$$

Then we have

- $X = \bigcup_n X_n$.
- X_n are finite-dimensional, hence closed (cf. (4.9));
- X_n are proper subspace, hence has empty interior (Lemma 1.3).

Therefore, X is not a Baire space, which contradicts the *Baire category theorem* (Lemma 1.1). □

1.3 Lemma *Proper subspace of a normed vector space must has empty interior.*

Proof: Let V be a proper subspace of a normed vector space X. If V has nonempty interior, it must contains a ball $B(x, r) := \{y \in X | |y - x| < r\}$. Then for any $z \in X$, putting $y = x + \frac{r}{2|z|}z$, one has $y \in B(x, r) \subset V$. Therefore $X = V$, a contradiction. □

1.4 Lemma *The algebraic dimension of an infinite algebraic extension of a field K satisfying one of the following condition is countable.*

- *The cardinal of K is countable.*
- *K is complete and has a countable dense subfield.*
- *K is a global field.*
- *K is a local field.*

Proof: First, if the cardinal of K is countable, then so is $\overline{K}$, *a fortior* its dimension.

If K is complete and has a countable dense subfield F, so the algebraic closure $\overline{F}$ is obtained by adjoining roots of countable many separable polynomials over F. Then, so is $\overline{K}$ and hence $\overline{K}$ has a countable basis over K. Indeed, for any $\alpha \in \overline{K}$ separable over K with minimal polynomial f, since F is dense in K, there exists a polynomial $g \in F[t]$ near to f. Then $|g(\alpha)| = |g(\alpha) - f(\alpha)|$ is small. The $|\alpha - \beta|$ is small for some root of g. In particular, we can choose g and β such that $|\alpha - \beta| < r(\alpha)$. Then, by *Krasner's lemma* (cf. Exercise 6.2), $\alpha \in K(\beta)$.

It is well-known that $\mathbb{Q}$ is countable, thus so is its finite extensions. As for $K = \mathbb{F}_p(t)$, the result follows from the fact that $\mathbb{F}_p[t]$ has a countable basis hence is countable.

Finally, local fields are completion of global fields , thus they have global fields as their countable dense subfield. □

1.5 Remark The exist uncountable-dimensional algebraic extensions. For instance, let $K = k(t_i | i \in I)$, then $L = k(\sqrt{t_i} | i \in I)$ is algebraic and of degree $[L : K] \geqslant \mathrm{Card}(I)$ because the elements $\sqrt{t_i}$ are linearly independent over K. Thus by taking I to be uncountable, one obtains an algebraic extension $L|K$ of uncountable degree. (cf. this post)

1.6 Lemma *Let K be an infinite field, then the algebraic closure $\overline{K}$ has the same cardinal with K.*

Proof: First, $K[t]$ has a countable basis $1, t, t^2, \cdots$, thus has the same cardinal with K. Let $\chi \colon \overline{K} \to K[t]$ denotes the map which maps an algebraic element to its minimal polynomial. This map has finite fibers, thus $\overline{K}$ has the same cardinal with $K[t]$, hence K. □

1.7 Remark $[\mathbb{R} : \mathbb{Q}] = \mathrm{Card}(\mathbb{R})$ (see this MO post). How about $[\mathbb{Q}_p : \mathbb{Q}]$?

I also heard that $[\overline{\mathbb{C}((t))} : \mathbb{C}((t))] = \aleph_0$, how about general $[\overline{K((t))} : K]$ with K an algebraic closed field?

2 Let $X_0, X_1, \cdots$ be an infinite sequence of unknowns, p a fixed prime number and $W_n = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n, n \geqslant 0$. Show that there exist polynomials $S_0, S_1, \cdots ; P_0, P_1, \cdots \in \mathbb{Z}[X_0, X_1, \cdots ; Y_0, Y_1, \cdots]$ such that

$$\begin{aligned} W_n(S_0, S_1, \cdots) &= W_n(X_0, X_1, \cdots) + W_n(Y_0, Y_1, \cdots), \\ W_n(P_0, P_1, \cdots) &= W_n(X_0, X_1, \cdots) \cdot W_n(Y_0, Y_1, \cdots). \end{aligned}$$

Proof: Obviously, $S_0, S_1, \cdots ; P_0, P_1, \cdots$ can be obtained inductively from the above equalities. It remains to show $S_0, S_1, \cdots ; P_0, P_1, \cdots$ are integral. To simplify the notations, we use X instead of the sequence $X_0, X_1, \cdots$ and Y, S, P similarly. We also use X^p instead of the sequence obtained by replacing each X_i by X_i^p.

Note that

$$W_n(X) \equiv W_{n-1}(X^p) \bmod p,$$

hence

$$W_n(X) + W_n(Y) \equiv W_{n-1}(X^p) + W_{n-1}(Y^p) = W_{n-1}(S(X^p; Y^p)) \bmod p.$$

On the other hand, for any polynomials $f(X) \in \mathbb{Z}[X]$, one has

$$f(X^p) \equiv f(X)^p \bmod p.$$

Hence, by the obversion that $a \equiv b \bmod p^r \Rightarrow a^p \equiv b^p \bmod p^{r+1}$, one has

$$f(X^p)^{p^n} \equiv f(X)^{p^{n+1}} \bmod p^{n+1}.$$

Use this fact, one has

$$p^i S_i(X^p; Y^p)^{p^{n-i-1}} \equiv p^i S_i(X; Y)^{p^{n-i}} \bmod p^n.$$

Therefore,

$$\begin{aligned} W_{n-1}(S(X^p; Y^p)) &\equiv \sum_{i=0}^{n-1} p^i S_i(X^p; Y^p)^{p^{n-1-i}} \\ &\equiv \sum_{i=0}^{n-1} p^i S_i(X; Y)^{p^{n-i}} \bmod p^n. \end{aligned}$$

On the other hand, one has

$$W_n(X) + W_n(Y) = W_n(S(X; Y)) = \sum_{i=0}^{n} p^i S_i(X; Y)^{p^{n-i}}.$$

Therefore,

$$p^n S_n(X; Y) \equiv 0 \bmod p^n,$$

which means $S_n(X; Y)$ is integral. The proof of integrality of $P_n(X; Y)$ is similar. □

Similar argument shows the following general proposition.

2.1 Proposition *For any polynomials $\Phi(X;Y;\cdots)$ over $\mathbb{Z}$, there exists are unique polynomials $\varphi_n(X;Y;\cdots)$ for all $n=0,1,2,\cdots$ such that*

$$W_n(\varphi_0,\varphi_1,\cdots)=\Phi(W_n(X);W_n(Y);\cdots).$$

For example, when $\Phi=X+Y$, $\varphi_n(X;Y)=S_n(S;Y)$; when $\Phi=XY$, $\varphi_n(X;Y)=P_n(S;Y)$. We further point out that

1. when $\Phi=0$, $\varphi_n=0$;
2. when $\Phi=1$, $\varphi_0=1$, $\varphi_n=0$ for $n>0$;
3. when $\Phi=X$, $\varphi_n=X_n$;
4. the case $\Phi=-X$ is not as simple as it looks like: when $p\neq 2$, one has $\varphi_n=-X_n$ as desired, while when $p=2$, $\varphi_n\neq -X_n$ in general. We denote this φ_n by ι_n.

3 Let A be a commutative ring. For $a=(a_0,a_1,\cdots),b=(b_0,b_1,\cdots)$, $a_i,b_i\in A$, put

$$a+b=(S_0(a,b),S_1(a,b),\cdots),\quad a\cdot b=(P_0(a,b),P_1(a,b),\cdots).$$

Show that with these operations the vectors $a=(a_0,a_l,\cdots)$ form a commutative ring $W(A)$ with 1. It is called the *ring of Witt vectors* over A.

Proof: The proof is straightforward.

1. $(W(A),+,0)$ *is an abelian group.* Here 0 denotes the vector $(0,0,\cdots)$.

   1.1 *For any $a\in W(A)$, $a+0=a$.* This equals to say $S_n(a,0)=a_n$ for all $n\in\mathbb{N}$, which follows from the equality of polynomials:

   $$S_n(X;0)=X_n,$$

   which follows from Proposition 2.1 in the case $\Phi(X)=X$ and the fact that $W_n(0)=0$.

   1.2 *For any $a\in W(A)$, $a+\iota(a)=0$.* This equals to say $S_n(a,\iota(a))=0$ for all $n\in\mathbb{N}$, which follows from the equality of polynomials:

   $$S_n(X;\iota(X))=0,$$

   which follows from Proposition 2.1 in the case $\Phi(X)=0$ and the fact that $W_n(\iota(X))=-W_n(X)$.

1.3 *For any $a, b \in W(A)$, $a+b = b+a$.* This equals to say $S_n(a, b) = S_n(b, a)$ for all $n \in \mathbb{N}$, which follows from the equality of polynomials:

$$S_n(X;Y) = S_n(Y;X),$$

which follows from $\Phi(X;Y) = X + Y = Y + X$.

1.4 *For any $a, b, c \in W(A)$, $(a + b) + c = a + (b + c)$.* This equals to say $S_n(S(a, b), c) = S_n(a, S(b, c))$ for all $n \in \mathbb{N}$, which follows from the equality of polynomials:

$$S_n(S(X;Y);Z) = S_n(X;S(Y;Z)),$$

which follows from $\Phi(X;Y;Z) = (X + Y) + Z = X + (Y + Z)$.

2. $(W(A), +, \cdot, 0, 1)$ *is a commutative ring.* Here 1 denotes the vector $(1, 0, \cdots)$.

2.1 *For any $a \in W(A)$, $a \cdot 1 = a$.* This equals to say $P_n(a, 1) = a_n$ for all $n \in \mathbb{N}$, which follows from the equality of polynomials:

$$P_n(X;1) = X_n,$$

which follows from Proposition 2.1 in the case $\Phi(X) = X$ and the fact that $W_n(1) = 1$.

2.2 *For any $a, b \in W(A)$, $a \cdot b = b \cdot a$.* This equals to say $P_n(a, b) = P_n(b, a)$ for all $n \in \mathbb{N}$, which follows from the equality of polynomials:

$$P_n(X;Y) = P_n(Y;X),$$

which follows from $\Phi(X;Y) = XY = YX$.

2.3 *For any $a, b, c \in W(A)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.* This equals to say $P_n(P(a, b), c) = P_n(a, P(b, c))$ for all $n \in \mathbb{N}$, which follows from the equality of polynomials:

$$P_n(P(X;Y);Z) = P_n(X;P(Y;Z)),$$

which follows from $\Phi(X;Y;Z) = (XY)Z = X(YZ)$.

2.4 *For any $a, b, c \in W(A)$, $(a+b) \cdot c = a \cdot c + b \cdot c$.* This equals to say $P_n(S(a, b), c) = S_n(P(a, c), P(b, c))$ for all $n \in \mathbb{N}$, which follows from the equality of polynomials:

$$P_n(S(X;Y);Z) = S_n(P(X;Z);P(Y;Z)),$$

which follows from $\Phi(X;Y;Z) = (X + Y)Z = XY + XZ$. □

Another approach is the follows

Proof: We first prove the statement for $\mathbb{Q}$-algebras. Define $\psi\colon W(A) \to A^{\mathbb{N}}$ by $a = (a_0, a_1, \cdots) \mapsto (W_0(a), W_1(a), \cdots)$. This is a bijection and there is a standard ring structure on $A^{\mathbb{N}}$, therefore ψ translate the ring structure of $A^{\mathbb{N}}$ to $W(A)$. Specially, $\psi(0, 0, \cdots) = (0, 0, \cdots)$ shows that $(0, 0, \cdots)$ is the additive identity; $\psi(1, 0, 0, \cdots) = (1, 1, 1, \cdots)$ shows that $(1, 0, 0, \cdots)$ is the multiplicative identity; and $\psi(\iota_1(a), \iota_2(a), \cdots) = (-a_1, -a_2, \cdots)$ shows that $(\iota_1(a), \iota_2(a), \cdots)$ is the additive inverse.

Next, if A is ***$\mathbb{Z}$-torsion-free***, which means there exists no nonzero $a \in A$ such that $na = 0$ for some $n \in \mathbb{Z}$, we consider the embedding $A \to A \otimes \mathbb{Q}$, which induces an injective map $W(A) \to W(A \otimes \mathbb{Q})$. This map preserves $S, P, 0, 1$ and ι as they are polynomials over $\mathbb{Z}$, then it gives $W(A)$ a ring structure by identify it with a subring of $W(A \otimes \mathbb{Q})$.

Lastly, we need to prove this for general case. This follows from that every ring is a quotient of a $\mathbb{Z}$-torsion-free ring. □

The Witt vectors for different primes p are special cases of universal Witt vectors.

3.1 (The universal Witt vectors) Let $X_1, X_2, \cdots$ be infinite many indeterminates. Define

$$W_n = \sum_{d \mid n} d X_d^{n/d}.$$

A ***universal Witt vector*** is a sequence $a = (a_1, a_2, \cdots)$ of elements of a ring A. The ***ghost components*** of a is the elements $a^{(n)} = W_n(a)$.

3.2 Lemma *Each a_n can be expressed in terms of $a^{(d)}$ for $d \mid n$, with rational coefficients.*

Proof: We prove this for X_n and W_n by induction on n. First, $X_1 = W_1$. Suppose X_r has been expressed in terms of W_d for $d \mid r$ and $r \leqslant n$, with rational coefficients. Then since

$$W_n = \sum_{d \mid n} d X_d^{n/d},$$

we have

$$X_n = \frac{1}{n} \left(W_n - \sum_{d \mid n, d \neq n} d X_d^{n/d} \right),$$

where each monomial of right side can be expressed in terms of W_d for $d \mid n$, with rational coefficients as desired. □

One may further want to write down the explicit formula for X_n. This suggests the theory of Dirichlet convolution on $\Omega(\mathbb{Q})$ (cf. Example A.15). Although the problem here is in fact different from the *Möbius inversion formula*, I still post it here.

3.3 (Arithmetic functions and Dirichlet convolution) A map from the set of positive integral numbers to some ring R is called an ***arithmetic function*** over R. The set of arithmetic functions over R is denoted by $\mathcal{A}(R)$. Of course $\mathcal{A}(R)$ can be made into a ring by setting

$$(f+g)(n) := f(n)+g(n) \quad \text{and} \quad (fg)(n) = f(n)g(n),$$

with additive identity 0 and multiplicative identity $u(n) = 1$. However, there exists another multiplication on $\mathcal{A}(R)$.

Let f, g be two arithmetic functions over R, we define the ***Dirichlet convolution*** of them by

$$(f * g)(n) := \sum_{d|n} f(d)g(\frac{n}{d}).$$

Then one can verify that $(\mathcal{A}(R), +, *, 0, \delta)$ is a ring, where δ is the multiplicative identity under the Dirichlet convolution and is given by $\delta(1) = 1$ and $\delta(n) = 0$ for $n > 1$.

Define the ***Möbius function*** μ as

- $\mu(1) = 1$;
- $\mu(n) = 0$ if n is not square-free;
- $\mu(n) = (-1)^k$ if n has k distinct prime divisors.

One can see $\mu \in \mathcal{A}(R)$ and further,

3.4 Proposition (Möbius Inversion Formula) *Let f, g be two arithmetic functions over R, then*

$$f(n) = \sum_{d|n} g(d)$$

if and only if

$$g(n) = \sum_{d|n} f(d)\mu(\frac{n}{d}).$$

Proof: It suffices to show

$$u * \mu = \delta.$$

Indeed, we have $(u*\mu)(1) = \mu(1) = 1 = \delta(1)$ and for $n = p_1^{\nu_1}\cdots p_r^{\nu_r} > 1$,

$$\begin{aligned}(u*\mu)(n) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_r) + \mu(p_1p_2) + \cdots + \mu(p_1p_2\cdots p_r)\\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + (-1)^r\\ &= (1-1)^r = 0.\end{aligned}$$

□

Now, go back to the topic.

3.5 Lemma *Let $a = (a_1, a_2, \cdots)$ be a universal Witt vector and*

$$f_a(t) = \prod_{n=1}^{\infty} (1 - a_n t^n)^{-1},$$

then one has

$$t \frac{\mathrm{d}}{\mathrm{d\,t}} \log\left(f_a(t)\right) := t \frac{f_a'(t)}{f_a(t)} = \sum_{n=1}^{\infty} a^{(n)} t^n.$$

Proof: Straight forward calculation shows

$$\begin{aligned} t\frac{f_a'(t)}{f_a(t)} &= \sum_{n=1}^{\infty} \frac{n a_n t^n}{1 - a_n t^n} \\ &= \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} n (a_n t^n)^m \\ &= \sum_{n=1}^{\infty} \sum_{d|n} d a_d^{n/d} t^n = \sum_{n=1}^{\infty} a^{(n)} t^n. \end{aligned}$$

□

The ghost components induces a map from the set $W(A)$ of universal Witt vectors over A to the product $A^{\mathbb{N}^*}$ of countable many copies of A:

$$\begin{aligned} \varpi \colon W(A) &\longrightarrow A^{\mathbb{N}^*} \\ a = (a_1, a_2, \cdots) &\longmapsto (a^{(1)}, a^{(2)}, \cdots). \end{aligned}$$

Note that $A^{\mathbb{N}^*}$ has a standard ring structure. We further point out that

3.6 Proposition *Let a, b be two universal Witt vectors over A, then we have*

$$(a+b)_n, (ab)_n \in \mathbb{Z}[a_1, \cdots, a_n; b_1, \cdots, b_n].$$

Proof: First note that we may assume $a_1, a_2, \cdots, b_1, b_2, \cdots$ are algebraic independent over $\mathbb{Z}$ and $A = \mathbb{Z}[a_1, a_2, \cdots; b_1, b_2, \cdots]$.

Straight forward calculation shows

$$\begin{aligned} t \frac{\mathrm{d}}{\mathrm{d\,t}} \log\left(f_{a+b}(t)\right) &= \sum_{n=1}^{\infty} (a+b)^{(n)} t^n = \sum_{n=1}^{\infty} a^{(n)} + b^{(n)} t^n \\ &= t \frac{\mathrm{d}}{\mathrm{d\,t}} \log\left(f_a(t)\right) + t \frac{\mathrm{d}}{\mathrm{d\,t}} \log\left(f_b(t)\right) \\ &= t \frac{\mathrm{d}}{\mathrm{d\,t}} \left(\log f_a(t) + \log f_b(t)\right) \\ &= t \frac{\mathrm{d}}{\mathrm{d\,t}} \log\left(f_a(t) f_b(t)\right). \end{aligned}$$

By Lemma 3.7, $f_a(t)f_b(t) = f_{a+b}(t)$. Therefore $(a+b)_n$ can be written as integral polynomial of $a_1, \cdots, a_n, b_1, \cdots, b_n$.

Straight forward calculation shows

$$\begin{aligned}
\log f_{ab}(t) &= \oint \frac{t \frac{\mathrm{d}}{\mathrm{d}\,t} \log\left(f_{ab}(t)\right)}{t} \,\mathrm{d}\,t \\
&= \oint \frac{1}{t} \sum_{n=1}^{\infty} (ab)^{(n)} t^n \,\mathrm{d}\,t \\
&= \oint \sum_{n=1}^{\infty} a^{(n)} b^{(n)} t^{n-1} \,\mathrm{d}\,t \\
&= \sum_{n=1}^{\infty} \frac{a^{(n)} b^{(n)}}{n} t^n \\
&= \sum_{n=1}^{\infty} \sum_{d|n} \sum_{e|n} \frac{de}{n} a_d^{n/d} b_e^{n/e} t^n \\
&= \sum_{d,e \geqslant 1} \sum_{\substack{n \geqslant 1 \\ d|n, e|n}} \frac{de}{n} a_d^{n/d} b_e^{n/e} t^n \\
&= \sum_{d,e \geqslant 1} \sum_{\nu=1}^{\infty} \frac{1}{\nu} \left(\frac{de}{m} a_d^{m/d} b_e^{m/e} t^m \right)^{\nu} \\
&= \sum_{d,e \geqslant 1} \log(1 - a_d^{m/d} b_e^{m/e} t^m)^{-de/m}.
\end{aligned}$$

Here m denotes the least common multiple of d, e and d, e range over all integers $\geqslant 1$. Then, by Lemma 3.7,

$$f_{ab}(t) = \prod_{d,e \geqslant 1} (1 - a_d^{m/d} b_e^{m/e} t^m)^{-de/m}.$$

Thus $(ab)_n \in \mathbb{Z}[a_1, \cdots, a_n; b_1, \cdots, b_n]$. □

3.7 Lemma *Let A be a $\mathbb{Z}$-torsion-free ring. Then the maps* $\log$ *and* $t \frac{\mathrm{d}}{\mathrm{d}\,t} \log$ *on* $\Lambda(A)$ *are injective.*

Proof: When A is a $\mathbb{Q}$-algebra, the inverse of log is exp, while the inverse of $t \frac{\mathrm{d}}{\mathrm{d}\,t} \log$ is $f(t) \mapsto \exp \oint \frac{f(t)}{t} \,\mathrm{d}\,t$. See the followings for details.

If A is $\mathbb{Z}$-torsion-free, then $A \otimes \mathbb{Q}$ is a $\mathbb{Q}$-algebra and the maps log and $t \frac{\mathrm{d}}{\mathrm{d}\,t} \log$ for A can be identified with restrictions of those for $A \otimes \mathbb{Q}$ on A, hence are injective. □

Remark: One may find that the image of $t \frac{\mathrm{d}}{\mathrm{d}\,t} \log$ lies in $tA[[t]]$. However, the similar results do not hold for log, exp and $\exp \oint \frac{}{t} \,\mathrm{d}\,t$.

Recall (Operations on formal power series): Here we recall some operations on formal power series. First, let

$$f(t) = \sum_{\nu=1}^{\infty} f_\nu t^\nu \in tA[[t]],$$
$$g(t) = \sum_{\nu=0}^{\infty} g_\nu t^\nu \in A[[t]].$$

Then, we can ***composite*** them by setting

$$g(f(t)) := \sum_{\nu=0}^{\infty} (g \circ f)_\nu t^\nu,$$

where $(g \circ f)_0 = g_0$ and for $\nu \geqslant 1$,

$$(g \circ f)_\nu := \sum_{k \in \mathbb{N}, j_1 + \cdots + j_k = \nu} g_k f_{j_1} \cdots f_{j_k}.$$

Here the sum is extended over all partitions $j = (j_1, j_2, \cdots, j_k)$ of ν.

Given a formal power series $f(t) = \sum_{\nu=0}^{\infty} f_\nu t^\nu \in A[[t]]$, we define its ***formal derivative*** by

$$\frac{\mathrm{d}}{\mathrm{d}\,\mathrm{t}} f(t) := \sum_{\nu=1}^{\infty} \nu f_\nu t^{\nu-1}.$$

This linear map is of course not injective. But its kernel is A, thus $\frac{\mathrm{d}}{\mathrm{d}\,\mathrm{t}}$ induces a bijective linear map

$$tA[[t]] \xrightarrow{\frac{\mathrm{d}}{\mathrm{d}\,\mathrm{t}}} A[[t]].$$

Denote its inverse by I.

Given a formal power series $f(t) = \sum_{\nu=0}^{\infty} f_\nu t^\nu \in A[[t]]$, we define its ***formal indefinite integral*** by

$$\int f(t)\,\mathrm{d}\,t := \sum_{\nu=1}^{\infty} \frac{f_{\nu-1}}{\nu} t^\nu + A.$$

By fix the constant term to be 0, we obtain the ***formal definite integral***

$$\oint f(t)\,\mathrm{d}\,t := \sum_{\nu=1}^{\infty} \frac{f_{\nu-1}}{\nu} t^\nu.$$

This induces a bijective linear map, which is precisely the inverse I of $\frac{\mathrm{d}}{\mathrm{d}\,\mathrm{t}}$.

Let $\Lambda(A) = 1 + A[[t]]$ denote the principal unit group of formal power series over A and suppose A is a $\mathbb{Q}$-algebra. Consider the following two series:

$$\begin{aligned}\exp(t) &= \sum_{\nu=0}^{\infty} \frac{1}{\nu!} t^{\nu},\\ \log(1+t) &= \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} t^{\nu}.\end{aligned}$$

Then exp induces a map from $tA[[t]]$ to $\Lambda(A)$ by $f(t) \mapsto \exp(t) \circ f(t)$, while log induces a map from $\Lambda(A)$ to $tA[[t]]$ by $f(t) \mapsto \log(1+t) \circ (f(t)-1)$. Furthermore, one can verify that they are mutual inverse group homomorphisms.

$$\begin{tikzcd} tA[[t]] \arrow[r, shift left, "\exp"] & \Lambda(A). \arrow[l, shift left, "\log"] \end{tikzcd}$$

We point out that

3.8 Proposition *$W(A)$ is a ring.*

Proof: We first prove the statement for $\mathbb{Q}$-algebras. In this case, Lemma 3.2 implies that ϖ is injective, while Proposition 3.6 implies that the image of ϖ in $A^{\mathbb{N}^*}$ is a subring. Therefore, the embedding ϖ translate the ring structure of $A^{\mathbb{N}^*}$ to $W(A)$.

Next, for any ring A with characteristic 0, we consider the embedding $A \to A \otimes \mathbb{Q}$, which induces an injective map $W(A) \to W(A \otimes \mathbb{Q})$. By Proposition 3.6, this map gives $W(A)$ a ring structure by identify it with a subring of $W(A \otimes \mathbb{Q})$.

Lastly, we need to prove this for positive characteristic rings. This follows from that every ring is a quotient of a ring with characteristic 0. □

One can see the above proof is similar with that of Exercise 3. Recall the notion of *λ-rings* (cf. A.4), we can give another proof which further points out that

3.9 Proposition *$W(A)$ is a λ-ring.*

Proof: Consider the map

$$\begin{aligned} W(A) &\longrightarrow \Lambda(A)\\ a = (a_1, a_2, \cdots) &\longmapsto f_a(t). \end{aligned}$$

By Lemmas 3.5 and 3.10, this map is bijective. Thus we can identify $W(A)$ with $\Lambda(A)$ and translate the λ-ring structure of $\Lambda(A)$ to $W(A)$. □

Remark: The calculations in the proof of Proposition 3.6 show that this ring structure of $W(A)$ does not coincide with that we give in Proposition 3.8. To correct this, one need modify the definitions.

3.10 Lemma *Let $U^{(n)}$ denotes the ideal $1 + t^n A[[t]]$ of $A[[t]]$, one has*

$$U^{(n)}/U^{(n+1)} \cong A$$

as $A[[t]]$-modules.

Proof: This follows from the shot exact sequence:

$$1 \longrightarrow U^{(n+1)} \longrightarrow U^{(n)} \xrightarrow{\alpha_n} A \longrightarrow 0$$

where α_n is defined by $\alpha_n(\sum_{\nu=0}^{\infty} a_\nu t^\nu) \mapsto a_n$. □

In this way, we obtain the universal property of W from that of Λ.

3.11 Theorem *The functor*

$$\begin{aligned} W\colon \mathbf{CRing} &\longrightarrow \Lambda\,\mathbf{Ring} \\ A &\longmapsto W(A) \end{aligned}$$

is the right adjoint of the forgetful functor $F\colon \lambda\,\mathbf{Ring} \to \mathbf{CRing}$.

4 Assume $pA = 0$. For every Witt vector $a = (a_0, a_1, \cdots) \in W(A)$ consider the "ghost components"

$$a^{(n)} = W_n(a) = a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n$$

as well as the mappings $V, F\colon W(A) \to W(A)$ defined by

$$Va = (0, a_0, a_1, \cdots) \quad \textbf{and} \quad Fa = (a_0^p, a_l^p, \cdots),$$

called respectively "transfer" ("Verschiebung" in German) and "Frobenius". Show that

$$(Va)^{(n)} = pa^{(n-1)} \quad \textbf{and} \quad a^{(n)} = (Fa)^{(n)} + p^n a_n.$$

5 Let k be a field of characteristic p. Then V is a homomorphism of the additive group of $W(k)$ and F is a ring homomorphism, and one has

$$VFa = FVa = pa.$$

6 If k is a perfect field of characteristic p, then $W(k)$ is a complete discrete valuation ring with residue class field k.

III Appendix: λ-rings

Here is a survey of λ-rings following nLab. One can think this is an expanding of it.

Motivation from representation theory

Typically one can form direct sums of representations of some algebraic structure. The decategorification to isomorphism classes of such representations then inherits the structure of a commutative monoid. But nobody likes commutative monoids: we all have an urge to subtract. So, we throw in formal negatives and get an abelian group – the ***Grothendieck group***.

In many situations, we can also take tensor products of representations. Then the Grothendieck group becomes something better than an abelian group. It becomes a ring: the ***representation ring***. Moreover, in many situations we can also take exterior and symmetric powers of representations; indeed, we can often apply any *Young diagram* to a representation and get a new representation. Then the representation ring becomes something better than a ring: it becomes a *λ-ring*.

More generally, the Grothendieck group of a monoidal abelian category is always a ring, called a ***Grothendieck ring***. If we start with a braided monoidal abelian category, this ring is commutative. But if we start with a symmetric monoidal abelian category, we get a *λ-ring*.

So, *λ-rings* are all about getting the most for your money when you decategorify a symmetric monoidal abelian category – for example the category of representations of a group, or the category of vector bundles on a topological space.

Unsurprisingly, the Grothendieck group of the free symmetric monoidal abelian category on one generator is the free λ-ring on one generator. This category is very important in representation theory. Objects in this category are called ***Schur functors***, because for obvious reasons they act as functors on any symmetric monoidal abelian category. The irreducible objects in this category are called "***Young diagrams***". Elements of the free λ-ring on one generator are called ***symmetric functions***.

1 Preliminaries

A.1 (pre-$\boldsymbol{\lambda}$-ring) A ***pre-λ-structure*** on a commutative ring R is a sequence of maps

$$\lambda^n \colon R \to R$$

for each $n \geqslant 0$ satisfying the relations for all $x \in R$:

$$\lambda^0(x) = 1, \quad \lambda^1(x) = x.$$

and for all integers $n \geqslant 0$, and $x, y \in R$,

$$\lambda^n(x+y) = \sum_{k=0}^{n} \lambda^k(x)\lambda^{n-k}(y).$$

A ***pre-λ-ring*** is a commutative ring equipped with a pre-λ-structure on it.

For a pre-λ-ring (R, λ), we define the formal power series

$$\lambda_t(x) = \sum_{n=0}^{\infty} \lambda^n(x)t^n = 1 + xt + \text{higher terms},$$

called the ***generating function*** of the pre-λ-structure $\lambda^\bullet$. One can see the map $x \mapsto \lambda_t(x)$ induces a homomorphism from the additive group of R into the principal unit group $1 + tR[[t]]$ of power series over R. Conversely, any such a homomorphism such that $\lambda_t(x) = 1 + xt+$ higher terms gives rise to a pre-λ-structure on R.

When $\lambda_t(x)$ is a polynomial of degree n, we say x is of ***degree*** n, write $\deg_\lambda(x) = n$. From $\lambda_t(x+y) = \lambda_t(x)\lambda_t(y)$, one has

$$\deg_\lambda(x+y) \leqslant \deg_\lambda(x) + \deg_\lambda(y).$$

To further define the notion of λ-rings, we need some knowledge from symmetric polynomials.

Recall (Symmetric polynomial): The n-th symmetric group $\mathfrak{S}_n$ acts on $R[x_1, \cdots, x_n]$ by

$$\sigma.f(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

A polynomial is called ***symmetric*** if $\sigma.f = f$ for all $\sigma \in \mathfrak{S}_n$. The ***weight*** of a monomial $x_1^{\nu_1}x_2^{\nu_2}\cdots x_n^{\nu_n}$ is $\nu_1 + 2\nu_2 + \cdots + n\nu_n$. The weight of a polynomial is the maximum of the weights of its monomials. One has

A.2 Lemma (Fundamental Theorem of Symmetric Polynomials) *Let f be a symmetric polynomial of indeterminates $x_1, x_2, \cdots, x_n$ and of degree d. Then there exists a polynomial $g(X_1, \cdots, X_n)$ of weight $\leqslant d$ such that*

$$f(t) = g(s_1, s_2, \cdots, s_n).$$

Here s_i is the i-th elementary symmetric polynomial of $x_1, x_2, \cdots, x_n$.

Proof: Refer [Lan02, IV, Theorem 6.1]. □

For any positive integers m and n, consider the polynomial

$$g(t) = \prod_{1 \leqslant i_1 < \cdots < i_m \leqslant nm} (1 + x_{i_1} \cdots x_{i_m} t).$$

One can see that the coefficient of each t^j in $g(t)$ is a symmetric polynomial of $x_1, \cdots, x_{nm}$ over $\mathbb{Z}$. Specially, the coefficient of t^n is such a symmetric polynomial. Hence by Lemma A.2, there exists a polynomial $P_{n,m}$ in nm indeterminates with integer coefficients such that the coefficient of t^n in $g(t)$ is $P_{n,m}(s_1, \cdots, s_{nm})$.

Recall (Symmetric polynomials in two sets of variables): The result of Lemma A.2 can be generalized to multi sets of variables. A polynomial $f(x; y) \in R[x_1, \cdots, x_n; y_1, \cdots, y_m]$ is said to be ***symmetric*** if

$$f(x; y) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}; y_{\tau(1)}, \cdots, y_{\tau(m)}), \quad \forall \sigma \in \mathfrak{S}_n, \tau \in \mathfrak{S}_m.$$

Let s_i, σ_i denote the i-th elementary symmetric polynomial of $x_1, x_2, \cdots, x_n$ and $y_1, y_2, \cdots, y_m$ respectively, one has

A.3 Corollary *Every symmetric polynomial $f(x; y) \in R[x_1, \cdots, x_n; y_1, \cdots, y_m]$ can be written uniquely as a polynomial of $s_1, s_2, \cdots, s_n; \sigma_1, \sigma_2, \cdots, \sigma_m$ with coefficients in R.*

For any positive integer n, consider the polynomial

$$h(t) = \prod_{i,j=1}^{n} (1 + x_i y_j t).$$

One can see that the coefficient of each t^k in h is a symmetric polynomial in $\mathbb{Z}[x_1, \cdots, x_n; y_1, \cdots, y_n]$. Specially, the coefficient of t^n is such a symmetric polynomial. Hence by Corollary A.3, there exists a polynomial $P_n \in \mathbb{Z}[X_1, \cdots, X_n; Y_1, \cdots, Y_n]$ such that the coefficient of t^n in $h(t)$ is $P_n(s_1, s_2, \cdots, s_n; \sigma_1, \sigma_2, \cdots, \sigma_n)$.

2 The "orthodox" definition of λ-rings

Now, we can give the "orthodox" definition of λ-rings.

A.4 A ***(special)*** $\boldsymbol{\lambda}$***-structure*** on a commutative ring R is a pre-λ-structure $\lambda^\bullet$ satisfying

(i) $\lambda^n(1) = 0$, for $n \geqslant 1$;

(ii) $\lambda^n(xy) = P_n(\lambda^1(x), \ldots, \lambda^n(x); \lambda^1(y), \ldots, \lambda^n(y))$ for all $x, y \in R$;

(iii) $\lambda^m(\lambda^n(x)) := P_{m,n}(\lambda^1(x), \ldots, \lambda^{mn}(x))$, for all $x \in R$.

Here, the polynomials $P_n, P_{m,n}$ have been given in the above recalls on symmetric polynomials. A commutative ring equipped with a λ-structure on it is called a ***(special)*** $\boldsymbol{\lambda}$***-ring***.

The following is a useful lemma in the theory of λ-rings.

A.5 Lemma *Let (R, λ) be a λ-ring, and let x and y be elements in R. If both x and y are of degree* 1*, then so is xy.*

Proof: Consider the polynomial for $n \geqslant 2$

$$h(t) = \prod_{i,j=1}^{n} (1 + x_i y_j t).$$

set $x_2, \cdots, x_n, y_2, \cdots, y_n$ to 0. Then one can see the coefficient of t^n is 0. This implies that

$$P_n(s_1, 0, 0, \cdots; \sigma_1, 0, 0, \cdots) = 0.$$

Thus

$$\lambda^n(xy) = P_n(\lambda^1(x), 0, 0, \cdots; \lambda^1(y), 0, 0, \cdots) = 0,$$

which shows $\deg_\lambda(xy) = 1$. □

The usual properties and constructions of rings extend in an obvious way to λ-rings.

A.6 Let R, S be two (pre-)λ-rings, then

- a ***(pre-)***$\boldsymbol{\lambda}$***-homomorphism*** is a ring homomorphism $f : R \to S$ such that $f \circ \lambda^n = \lambda^n \circ f$ for all n;
- a ***(pre-)***$\boldsymbol{\lambda}$***-ideal*** of R is an ideal I of R such that $\lambda^n(x) \in I$ for $n \geqslant 1$ and $x \in I$;
- a ***(pre-)***$\boldsymbol{\lambda}$***-subring*** of R is a subring R' of R such that $\lambda^n(x) \in R'$ for all n and $x \in R'$.

A.7 Proposition *Let $f\colon R \to S$ be a λ-homomorphism between λ-rings, then*

(i) The kernel of f is a λ-ideal in R;

(ii) The image of f is a λ-subring in S;

(iii) The quotient R/I of R by a λ-ideal I is naturally a λ-ring, and the projection map $R \to R/I$ is a λ-homomorphism.

(iv) An ideal I of R is a λ-ideal if and only if $\lambda^n(z_j) \in I$ holds for $n \geqslant 1$ and every element of a set of generators $\{z_j\}$ of I;

(v) The direct product $R \times S$ is a λ-ring, in which

$$\lambda_t(r,0) = (1,1) + \sum_{n=1}^{\infty} (\lambda^n(r), 0)t^n,$$
$$\lambda_t(0,s) = (1,1) + \sum_{n=1}^{\infty} (0, \lambda^n(s))t^n.$$

(vi) The tensor product $R \otimes S$ is a λ-ring, in which

$$\lambda^n(r \otimes 1) = \lambda^n(r) \otimes 1,$$
$$\lambda^n(1 \otimes s) = 1 \otimes \lambda^n(s).$$

(vii) If $\{R_i\}$ is an inverse system of λ-rings, then the inverse limit $\varprojlim R_i$ is naturally a λ-ring.

Given a λ-ring R, it is convenient to know how to put a λ-structure on the polynomial ring $R[x]$ or the power series ring $R[[x]]$. This is illustrated by the following result.

A.8 Proposition *Let R be a λ-ring. Then there exists a unique λ-structure on the polynomial ring $R[x]$ such that $\lambda_t(x) = 1 + xt$, i.e., $\deg_\lambda(x) = 1$. If R is augmented, then so is $R[x]$ with $\varepsilon(x) = 0$ or 1. The same holds for the power series ring $R[[x]]$.*

Proof: It suffices to extend $\lambda_t(x) = 1 + xt$ to all of $R[x]$ or $R[[x]]$. First, λ^n can be extended to the powers x^k using the axiom for $\lambda^n(xy)$ repeatedly. Then, use this axiom again we extend λ^n to monomials of the form ax^k. Finally, we extend λ^n to polynomials (or formal power series) $f = \sum a_k x^k$ by setting

$$\lambda_t(f) = \prod \lambda_t(a_k x^k).$$

The same reasoning shows that the λ-structure is uniquely determined by the condition $\lambda_t(x) = 1 + xt$. The assertion about the augmentation is clear. □

Apply Proposition A.8 repeatedly, one obtains

A.9 Corollary *Let R be a λ-ring. Then there exists a unique λ-structure on the polynomial ring $R[x_1, \cdots, x_n]$ such that $\lambda_t(x_i) = 1 + x_i t$, i.e., $\deg_\lambda(x_i) = 1$ for $i = 1, 2, \cdots, n$. If R is augmented, then so is $R[x_1, \cdots, x_n]$ with $\varepsilon(x_i) = 0$ or 1 for each i. The same holds for the power series ring $R[[x_1, \cdots, x_n]]$.*

3 Examples

The followings are typical examples.

A.10 Example (The initial $\boldsymbol{\lambda}$-ring) The simplest λ-ring is the ring of integers $\mathbb{Z}$ with the λ-structure

$$\lambda^n(m) = \binom{m}{n}.$$

Or, in other words, its λ-structure is given by the generating function

$$\lambda_t(m) = (1+t)^m.$$

In fact, this is the unique λ-structure on $\mathbb{Z}$. Indeed, in any λ-ring R, one has $\lambda_t(1) = 1 + t$, hence

$$\lambda_t(m) = (1+t)^m, \quad \forall m \in \mathbb{Z}.$$

This also shows that Every λ-ring has characteristic 0 and contains a λ-subring that is isomorphic to $\mathbb{Z}$ as λ-rings. If conversely R comes equipped with a λ-homomorphism $\varepsilon \colon R \to \mathbb{Z}$, then we say R is an ***augmented λ-ring*** and ε is an ***augmentation***.

A.11 Proposition *A λ-ring R is augmented if and only if there exists a λ-ideal I such that $R = \mathbb{Z} \oplus I$ as an abelian group.*

Proof: Taking I to be $\ker \varepsilon$. □

A.12 Example (The cofree $\boldsymbol{\lambda}$-ring $\boldsymbol{\Lambda}$) It is not obvious that the principal unit group $1 + tR[[t]]$ of formal power series is a λ-ring:

- *addition* on $1 + tR[[t]]$ is defined to be multiplication of power series,
- *multiplication* is defined by

  $$(1 + \sum_{n=1}^{\infty} r_n t^n) * (1 + \sum_{n=1}^{\infty} s_n t^n) := 1 + \sum_{n=1}^{\infty} P_n(r_1, \ldots, r_n; s_1, \ldots, s_n) t^n,$$

  with identity $1 + t$;
- the λ-*structure* is defined by

  $$\lambda^n(1 + \sum_{m=1}^{\infty} r_m t^m) = 1 + \sum_{m=1}^{\infty} P_{m,n}(r_1, \ldots, r_{mn}) t^m.$$

One should notice that to verify properties about the multiplication, it suffices to prove equalities of the integral polynomials P_n, which is enough to verify the equalities in the case the indeterminates are taking to be elementary symmetric polynomials. For instance, the associativity of multiplication follows from considering the coefficient of t^n of both sides of the equalities

$$\prod(1+x_iy_jt)*\prod(1+z_kt)=\prod(1+x_iy_jz_kt)=\prod(1+x_it)*\prod(1+y_jz_kt).$$

In similar way, one can show that $1+tR[[t]]$ is a λ-ring. This λ-ring is denoted by $\Lambda(R)$.

The following proposition gives another definition of λ-rings.

A.13 Proposition *A pre-λ-ring is a λ-ring if and only if*

$$\lambda_t\colon R\longrightarrow\Lambda(R)=1+tR[[t]]$$

is a pre-λ-homomorphism. If this is the case, λ_t is a split monomorphism in both categories **CRing** *and* λ **Ring**.

Proof: We have seen λ_t is always a homomorphism of additive groups. Then λ_t is a ring homomorphism if and only if

$$\lambda_t(1)=1+t,\quad \lambda_t(xy)=\lambda_t(x)*\lambda_t(y).$$

Furthermore, λ_t is a pre-λ-homomorphism if and only if

$$\lambda_t(\lambda^n(x))=\lambda^n(\lambda_t(x)).$$

Expanding all the three conditions, one obtain (i)-(iii) in A.4.

To show that λ_t is a split monomorphism, we give its retraction by

$$\begin{aligned}\alpha_1\colon \Lambda(R)&\longrightarrow R\\ 1+\sum_{n=1}^{\infty}r_nt^n&\longmapsto r_1.\end{aligned}$$

One can see that this is the retraction of λ_t in **Ab**. Moreover, α_1 is a ring homomorphism, thus λ_t is a split monomorphism in **CRing**. To show α_1 is a λ-homomorphism when R is a λ-ring, one only need to prove the corresponding equalities of symmetric polynomials. In our case, it is

$$P_{1,n}(s_1,\cdots,s_n)=s_n,$$

where the symmetric polynomials are in n indeterminates. Consider the polynomial $g(t)$ after Lemma A.2, this is obvious. Thus λ_t is a split monomorphism in λ **Ring**. □

The following theorem gives the universal property of the functor Λ.

A.14 Theorem *The functor* $\Lambda\colon \mathbf{CRing} \to \lambda\,\mathbf{Ring}$ *is the right adjoint of the forgetful functor* $F\colon \lambda\,\mathbf{Ring} \to \mathbf{CRing}$.

Proof: Given λ-ring R and a ring S, we need to show

$$\mathrm{Hom}_{\mathbf{CRing}}(R, S) \cong \mathrm{Hom}_{\lambda\,\mathbf{Ring}}(R, \Lambda(S)).$$

Any ring homomorphism $f\colon R \to S$ induces a canonical λ-homomorphism $\Lambda(f)\colon \Lambda(R) \to \Lambda(S)$ by mapping t to t. By Proposition A.13, $\lambda_t\colon R \to \Lambda(R)$ is a λ-homomorphism, thus we get a canonical λ-homomorphism $\Lambda(f) \circ \lambda_t$. Note that the following diagram is commutative.

$$\begin{tikzcd}
\Lambda(R) \arrow[r, "\Lambda(f)"] & \Lambda(S) \arrow[d, "\alpha_1"] \\
R \arrow[u, "\lambda_t"] \arrow[r, "f"] & S
\end{tikzcd}$$

We now show that $f \mapsto \Lambda(f) \circ \lambda_t$ is injective. Considering two ring homomorphisms f and g, if $\Lambda(f) \circ \lambda_t = \Lambda(g) \circ \lambda_t$, then, $\alpha_1 \circ \Lambda(f) \circ \lambda_t = \alpha_1 \circ \Lambda(g) \circ \lambda_t$, i.e., $f = g$.

Finally, we show that $f \mapsto \Lambda(f) \circ \lambda_t$ is surjective. Let $\widehat{f}\colon R \to \Lambda(S)$ be a λ-homomorphism, then $\alpha_1 \circ \widehat{f}\colon R \to S$ is a ring homomorphism. Apply the mapping $f \mapsto \Lambda(f) \circ \lambda_t$ on it, we have

$$\begin{aligned}
\Lambda(\alpha_1 \circ \widehat{f}) \circ \lambda_t(x) &= \Lambda(\alpha_1 \circ \widehat{f})(1 + \sum_{n=1}^{\infty} \lambda^n(x) t^n) \\
&= 1 + \sum_{n=1}^{\infty} (\alpha_1 \circ \widehat{f})(\lambda^n(x)) t^n \\
&= 1 + \sum_{n=1}^{\infty} \alpha_1(\lambda^n(\widehat{f}(x))) t^n.
\end{aligned}$$

Let $\widehat{f}(x) = 1 + \sum_{n=1}^{\infty} f_n(x) t^n$, then we have

$$\begin{aligned}
\alpha_1(\lambda^n(\widehat{f}(x))) &= \alpha_1 \left(1 + \sum_{m=1}^{\infty} P_{m,n}(f_1(x), \ldots, f_{mn}(x)) t^m \right) \\
&= P_{1,n}\left(f_1(x), \ldots, f_n(x)\right) \\
&= f_n(x).
\end{aligned}$$

Therefore

$$\Lambda(\alpha_1 \circ \widehat{f}) \circ \lambda_t(x) = 1 + \sum_{n=1}^{\infty} f_n(x) t^n = \widehat{f}(x).$$

Now, $f \mapsto \Lambda(f) \circ \lambda_t$ is bijective and the naturality is obvious, thus Λ is right adjoint to F. □

Remark: Recall that a ***comonad*** on a category $\mathcal{C}$ is a *comonoid* in the category of endofunctors of $\mathcal{C}$. In other words, a ***comonad*** is a functor $T\colon \mathcal{C} \to \mathcal{C}$ together with two natural transformations $\delta\colon T \to T^2 := T \circ T$ and $\varepsilon\colon T \to \mathrm{id}$ such that the following diagrams commute.

$$\begin{tikzcd}
T^2 \arrow[r, "\delta T"] & T^3 \\
T \arrow[u, "\delta"] \arrow[r, "\delta"'] & T^2 \arrow[u, "T\delta"']
\end{tikzcd}
\qquad
\begin{tikzcd}
T^2 \arrow[r, "\varepsilon T"] & T \\
T \arrow[u, "\delta"] \arrow[ur, equal] \arrow[r, "\delta"'] & T^2 \arrow[u, "T\varepsilon"']
\end{tikzcd}$$

A ***coalgebra*** over a comonad (T, δ, ε) on a category $\mathcal{C}$ is an object A in $\mathcal{C}$ together with a morphism $\alpha\colon A \to TA$ such that the following diagrams commute.

$$\begin{tikzcd}
T(A) \arrow[r, "\delta_A"] & T^2(A) \\
A \arrow[u, "\alpha"] \arrow[r, "\alpha"'] & T(A) \arrow[u, "T(\alpha)"']
\end{tikzcd}
\qquad
\begin{tikzcd}
TA \arrow[r, "\varepsilon_A"] & A \\
A \arrow[u, "\alpha"] \arrow[ur, equal] &
\end{tikzcd}$$

The category of *coalgebras* over a comonad is called its ***co-Eilenberg-Moore category*** and denoted by $T\,\mathbf{Alg}$.

Given a pair $L \dashv R\colon \mathcal{C} \to \mathcal{D}$ of *adjoint functors*, with *counit* ε and *unit* η, then there is a natural comonad $T = (L \circ R, L\eta R, \varepsilon)$ and a natural *comparison functor*

$$K\colon \mathcal{C} \longrightarrow T\,\mathbf{Alg}$$
$$A \longmapsto (L(A), L(A) \overset{L(\eta_A)}{\longrightarrow} LRL(A)).$$

The adjunction $L \dashv R$ is said to be a ***comonadic adjunction*** if K is an equivalence of categories.

By, Theorem A.14, $(F \circ \Lambda, \lambda_t, \alpha_1)$ is a comonad on $\mathbf{CRing}$. Moreover, from the proof, one can see that $F \dashv \Lambda$ is a comonadic adjunction.

A.15 Example ($\boldsymbol{\Omega}$) Let $\Omega_n(R)$ denote the ring $R[x_1, \cdots, x_n]$ of polynomials in n indeterminates over R. For every n there is a surjective ring homomorphism

$$\rho_n\colon \Omega_{n+1}(R) \longrightarrow \Omega_n(R),$$

defined by setting the last indeterminate x_{n+1} to 0.

The, we have an inverse system

$$R = \Omega_0(R) \xleftarrow{\rho_0} \Omega_1(R) \xleftarrow{\rho_1} \Omega_2(R) \longleftarrow \cdots$$

Its inverse limit is denoted by $\Omega(R)$.

Let ϕ_n denote the structure map $\Omega(R) \to \Omega_n(R)$. An element of $\Omega(R)$ is then a power series f in infinite indeterminates $x_1, x_2, \cdots$ such that for any $n \geqslant 1$,

$$\phi_n(f) = f(x_1, \cdots, x_n, 0, 0, \cdots)$$

is a polynomial of $x_1, \cdots, x_n$.

Let $s_k(x_1, \cdots, x_n)$ denote the k-th elementary symmetric polynomial of $x_1, \cdots, x_n$. Since

$$\phi_n(s_k(x_1, \cdots, x_{n+1})) = s_k(x_1, \cdots, x_n, 0) = s_k(x_1, \cdots, x_n),$$

the sequence $\{s_k(x_1, \cdots, x_n)\}_{n \geqslant 0}$ determines an element

$$s_k := \varprojlim_n s_k(x_1, \cdots, x_n)$$

in $\Omega(R)$, called the k-th ***elementary symmetric function*** over R. The sub R-algebra $\mho(R)$ of $\Omega(R)$ generated by all the elementary symmetric functions is called the ***ring of symmetric functions*** over R.

Now let R be a λ-ring. By Corollary A.9, $\Omega_n(R)$ are λ-rings. Straight forward calculation shows ρ_n are λ-homomorphisms. Therefore, by (vii) of Proposition A.7, $\Omega(R)$ is a λ-ring and ϕ_n are λ-homomorphisms.

A.16 Lemma *$\lambda^n(s_1) = s_n$ for all $n \geqslant 1$.*

Proof: For any $k \geqslant n$, we have

$$\begin{aligned}\phi_k \lambda^n(s_1) &= \lambda^n(\phi_k(s_1)) \\ &= \lambda^n(x_1 + \cdots + x_k) \\ &= \sum_{1 \leqslant i_1 < \cdots < i_n \leqslant k} x_{i_1} \cdots x_{i_n} \\ &= \phi_k(s_n).\end{aligned}$$

Therefore $\lambda^n(s_1) = s_n$. □

In the case $R = \mathbb{Z}$, all the λ-structures are uniquely determined. The λ-rings $\Omega(\mathbb{Z}), \mho(\mathbb{Z})$ are simply denoted by Ω and $\mho$. The above lemma implies that $\mho$ is the smallest λ-subring of Ω which contains s_1.

A.17 Example (The free λ-ring $\mho$) We now give the universal property of $\mho$: it is the *free λ-ring on one generator* s_1. That means for any λ-ring R and an element $x \in R$, there exists a unique λ-homomorphism $u_x \colon \mho \to R$ such that $x = u_x(s_1)$. This follows immediately from Lemma A.16 and the fact that $\mho$ is generated by $\{s_n\}_{n \geqslant 1}$.

There is another approach to the ***ring of symmetric functions*** $\mho(R)$ as follows.

First, let $\mho_n(R)$ denote the ring $\Omega_n(R)^{\mathfrak{S}_n}$ of symmetric polynomials in n indeterminates over R. It is not difficult to see that it is the smallest λ-sub-R-algebra of $\Omega_n(R)$ containing s_1. For every n the surjective λ-homomorphism $\rho_n \colon \Omega_{n+1}(R) \to \Omega_n(R)$ induces the surjective λ-homomorphism

$$\rho_n \colon \mho_{n+1}(R) \longrightarrow \mho_n(R).$$

Then, we have

$$\mho(R) = \varprojlim_{\rho_n} \mho_n(R).$$

On the other hand, we can interpret this inverse limit as a direct limit as follows. First note that the nonzero elements of the kernel of ρ_n have degree at least $n+1$ (in fact, they are multiples of $x_1 x_2 \cdots x_{n+1}$). Therefore the restriction of ρ_n to elements of degree at most n is a bijective linear map, and we have

$$\rho_n(s_k(x_1, \cdots, x_{n+1})) = s_k(x_1, \cdots, x_n),$$

for all $k \leqslant n$. Thus, by Lemma A.2, the inverse of this restriction can be extended uniquely to a ring homomorphism

$$\varphi_n \colon \mho_n(R) \longrightarrow \mho_{n+1}(R).$$

Since the images $\varphi_n(s_k(x_1, \cdots, x_n)) = s_k(x_1, \cdots, x_{n+1})$ for $k = 1, \cdots, n$ are still algebraically independent over R, the homomorphisms φ_n are injective. Applying φ_n to a polynomial amounts to adding all monomials containing the new indeterminate obtained by symmetry from monomials already present.

The ring $\mho(R)$ is then the direct limit

$$\mho(R) := \varinjlim_{\varphi_n} \mho_n(R).$$

As a direct limit of monomorphisms, an element F of $\mho(R)$ can be uniquely determined by an element, denoted by $F(x_1, \cdots, x_n)$, of $\mho_n(R)$ for enough large n. Note that φ_n are compatible with the total degree of polynomials, hence one can define the ***degree*** of F as the total degree of $F(x_1, \cdots, x_n)$. This gives $\mho(R)$ the structure of a graded ring

$$\mho(R) = \bigoplus_{n=1}^{\infty} \mho(R)_n.$$

The following are fundamental examples of symmetric functions.

- The ***monomial symmetric functions*** m_ν. Let $\nu = (\nu_1, \nu_2, \cdots)$ be a sequence of non-negative integers, only finitely many of which are non-zero. Then we can consider the monomial defined by ν:

  $$x^\nu := x_1^{\nu_1} x_2^{\nu_2} \cdots .$$

  Then m_ν is the symmetric function determined by x^ν, i.e. the sum of all monomials obtained from x^ν by symmetry. A formal definition of this is

  $$m_\nu = \sum_{\sigma \in \mathfrak{S}} x^{\sigma\nu}.$$

Since any symmetric function containing any of the monomials of some m_ν must contain all of them with the same coefficient, the distinct monomial symmetric functions therefore form a basis of $\mho(R)$ as graded R-module.

- The ***elementary symmetric functions*** s_k, for any natural number k. They are $s_k = m_\nu$ where $x^\nu = \prod_{i=1}^k x_i$.
- The ***power sum symmetric functions*** p_k, for any positive integer k. They are $p_k = m_\nu$, where $\nu = (k, 0, 0, \cdots)$.
- The ***complete homogeneous symmetric functions*** h_k, for any natural number k. They are the sum of all monomial symmetric functions m_ν where ν varies over all partitions of k.
- The ***Schur functions*** $s_\nu := m_\nu$ for any partition ν. Note that the set of Schur functions also form a basis of $\mho(R)$ as graded R-module.

The following are examples of expressions, which provide symmetric polynomials for all n but do not define symmetric functions.

- $p_0(x_1, \cdots, x_n) = \sum_{k=1}^n x_k^0 = n$.
- The "discriminant" $d(x_1, \cdots, x_n) = \prod\limits_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2$.

Important properties of $\mho(R)$ include the following.

A.18 Theorem (Fundamental Theorem of Symmetric Functions) *There is a canonical isomorphism of graded R-algebras:*

$$\begin{aligned} \mho(R) &\longrightarrow R[y_1, y_2, \cdots] \\ s_k &\longmapsto y_k. \end{aligned}$$

Proof: Follows from Lemma A.2. □

A.19 Corollary *Theorem A.18 implies the following.*

(i) The subring of $\mho(R)$ generated by its elements of degree $\leqslant n$ is isomorphic to the ring $\mho_n(R)$.

(ii) For every $n > 0$, $\mho(R)_n$ modulo its intersection with the subring generated by its elements of degree $< n$, is free of rank 1, and is generated by the image of s_n.

(iii) The **Hilbert–Poincaré series** *of $\mho(R)$ is*

$$P_{\mho(R)}(t) := \sum_{n=0}^{\infty} \dim_R(\mho(R)_n) t^n = \prod_{k=1}^{\infty} \frac{1}{1 - t^k},$$

the generating function of the integer partitions.

Proof: (i),(ii) are obvious. As for (iii), just notice that the Hilbert–Poincaré series is additive, hence

$$P_{R[y_1,y_2,\cdots]}(t) = \prod_{k=1}^{\infty} P_{R[y_k]}(t).$$

In our case y_k are algebraic independent and $\deg(y_k) = \deg(s_k) = k$. Note that a the only monomials in $R[y_k]$ are those of the form y_k^n, thus we have

$$P_{R[y_k]}(t) = \sum_{n=0}^{\infty} t^{kn} = \frac{1}{1-t^k}.$$

The statement then follows. Note that $P_{\mho(R)}(t)$ is the generating function of the integer partitions since the set of Schur functions form a basis of $\mho(R)$ as graded R-module. □

Remark: Theorem A.18 and hence Corollary A.19 still hold if one replace the family $\{s_n\}_{n>0}$ by any family $\{f_n\}_{n>0}$ of symmetric functions satisfying $\deg(f_n) = n$ and the above (ii). The set of complete homogeneous symmetric functions $\{h_n\}_{n>0}$, for instance, is such a family.

A.20 Corollary *There is an involutory automorphism ω of $\mho(R)$ such that*

(i) it interchanges the elementary symmetric functions s_k and the complete homogeneous symmetric function h_k for all k;

(ii) it sends each power sum symmetric function p_k to $(-1)^{k-1}p_k$;

(iii) it permutes the Schur functions among each other: interchanging s_ν and s_{ν^t} where ν^t is the transpose partition of ν.

Proof: The composite $s_k \mapsto y_k \mapsto h_k$ gives the automorphism ω. To prove the properties of ω, one only need to show the following identities.

- The *symmetry between elementary and complete homogeneous symmetric functions*:

$$\sum_{i=0}^{k}(-1)^i s_i h_{k-i} = 0 = \sum_{i=0}^{k}(-1)^i h_i s_{k-i}, \quad \forall k > 0.$$

- The *Newton identities*:

$$ks_k = \sum_{i=1}^{k}(-1)^{i-1} p_i s_{k-i}, \quad \forall k > 0,$$

$$kh_k = \sum_{i=1}^{k} p_i h_{k-i}, \quad \forall k > 0.$$

They can be proved by, for instance, using generating functions. □

A.21 Remark The generating functions.

- for the elementary symmetric functions:

$$S(t) = \sum_{k=0}^{\infty} s_k(x)t^k = \prod_{i=1}^{\infty}(1 + x_i t).$$

- for complete homogeneous symmetric functions

$$H(t) = \sum_{k=0}^{\infty} h_k(x)t^k = \prod_{i=1}^{\infty}\left(\sum_{k=0}^{\infty}(x_i t)^k\right) = \prod_{i=1}^{\infty}\frac{1}{1 - x_i t}.$$

- for the power sum symmetric functions

$$P(t) = \sum_{k=1}^{\infty} p_k(x)t^k = \sum_{k,i=1}^{\infty}(x_i t)^k = \sum_{i=1}^{\infty}\frac{x_i t}{1 - x_i t}.$$

One has

$$P(-t) = t\,\frac{\mathrm{d}}{\mathrm{d}\,\mathrm{t}}\log\left(S(t)\right) = t\frac{S'(t)}{S(t)}, \qquad P(t) = t\,\frac{\mathrm{d}}{\mathrm{d}\,\mathrm{t}}\log\left(H(t)\right) = t\frac{H'(t)}{H(t)}.$$

The generating functions are related to Hirzebruch polynomials as follows. Let $\phi(t)$ be a integral power series, then we may form the power series (we assume that $\phi(0) = 0$ in the first case, resp. that $\phi(0) = 1$ in the second):

$$ch_{\phi}(t) := \sum_{k=1}^{\infty}\phi(x_i t), \qquad td_{\phi}(t) := \prod_{k=1}^{\infty}\phi(x_i t).$$

The coefficient of t^n in $ch_{\phi}(t)$ (resp. $td_{\phi}(t)$) is a symmetric function $H^{+}_{\phi,n}$ (resp. $H^{\times}_{\phi,n}$) and is called the (n-th) additive (resp. multiplicative) ***Hirzebruch polynomial*** associated to ϕ.

A.22 Theorem *The functor* $\Lambda\colon$ $\mathbf{CRing} \to \lambda\,\mathbf{Ring}$ *is representable by* $\mho$.

Proof: Given a ring R, we need to show

$$\Lambda(R) \cong \mathrm{Hom}_{\mathbf{CRing}}(\mho, R).$$

Consider the mapping $f \mapsto 1 + \sum_{n=1}^{\infty} f(s_n)t^n$. It is obviously bijective since $\mho \cong \mathbb{Z}[s_1, s_2, \cdots]$.

Note that this identification gives $\mathrm{Hom}_{\mathbf{CRing}}(\mho, R)$ a λ-ring structure, which is different from the obvious one. Since $\mho \cong \mathbb{Z}[s_1, s_2, \cdots]$, one can identify $\mathrm{Hom}_{\mathbf{CRing}}(\mho, R)$ with the set $\mathcal{A}(R)$ of arithmetic functions over R (cf. 3.3). □

4 Verification Principle and Splitting Principle

A.23 (Natural operation on $\boldsymbol{\lambda}$-rings) A natural operation on λ-rings is a rule that assigns to each λ-ring R a function $\mu_R\colon R \to R$ such that, for any λ-homomorphism $f\colon R \to S$, the following square commutes.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\mu_R"'] & S \arrow[d, "\mu_S"] \\
R \arrow[r, "f"] & S
\end{tikzcd}$$

The addition and multiplication of natural operations on λ-rings are:

$$\begin{aligned}(\mu+\nu)_R &= \mu_R + \nu_R,\\ (\mu\nu)_R &= \mu_R\nu_R.\end{aligned}$$

Then, one can verify that the set of all natural operations on λ-rings is a ring, which is denoted by Op^λ.

For instance, each λ^n is a natural operation. Thus so is any polynomial of them. Then we get a homomorphism

$$\alpha\colon \mathbb{Z}[\lambda^1, \lambda^2, \lambda^3, \cdots] \longrightarrow Op^\lambda$$

by setting $\alpha(f(\lambda^1, \cdots, \lambda^n))_R(x) = f(\lambda^1(x), \cdots, \lambda^n(x))$ for an element x in a λ-ring R.

A.24 Theorem (Verification Principle) *The homomorphism α is an isomorphism. Moreover, one has*

$$\mu = f(\lambda^1, \cdots, \lambda^n)$$

if and only if this equality holds when applied to finite sums of elements of degree 1.

Proof: Obviously, α is a ring homomorphism.

α is injective. Indeed, if $\alpha(f(\lambda^1, \cdots, \lambda^n)) = 0$, then we have

$$\begin{aligned}0 &= \alpha(f(\lambda^1, \cdots, \lambda^n))_{\mho}(s_1)\\ &= f(\lambda^1(s_1), \cdots, \lambda^n(s_1))\\ &= f(s_1, \cdots, s_n).\end{aligned}$$

But $s_1, \cdots, s_n$ are algebraically independent, thus $f = 0$.

α is surjective. Let μ be a natural operation, then $\mu_{\mho}(s_1)$, as an element of $\mho$, is of the form $g(s_1, \cdots, s_n)$ for some integral polynomial g. We claim that $\mu = \alpha(g(\lambda^1, \cdots, \lambda^n))$.

Let x be an arbitrary element of a λ-ring R. Then, by the universal property (cf. A.17) of $\mho$, there exists a unique λ-homomorphism $u_x\colon \mho \to R$ such that $u_x(s_1) = x$. Therefore, we have

$$\begin{aligned}\mu_R(x) &= \mu_R(u_x(s_1))\\ &= u_x(\mu_{\mho}(s_1))\\ &= u_x(g(s_1, \cdots, s_n))\\ &= g(u_x(s_1), \cdots, u_x(s_n))\\ &= g(\lambda^1(x), \cdots, \lambda^n(x)).\end{aligned}$$

Consequently, α is an isomorphism.

As for the second statement, note that the above argument shows that to prove $\mu = f(\lambda^1, \cdots, \lambda^n)$, it suffices to show $\mu_{\mho}(s_1) = f(s_1, \cdots, s_n)$. This can be done by checking it on Ω, which is the inverse limit of Ω_k. Thus it suffices to show

$$\mu_{\Omega_k}(s_1(x_1, \cdots, x_k)) = f(s_1(x_1, \cdots, x_k), \cdots, s_n(x_1, \cdots, x_k))$$

for all k. Note that $s_1(x_1, \cdots, x_k) = x_1 + \cdots + x_k$ and each x_i is of degree 1, the above equalities are precisely the conditions. □

Remark: We may also consider a verification principle for more than one variable. The notion of a natural map in two variables is evident and the proof of the verification principle is similar.

We have seen the important of elements of degree 1, the following is a splitting principle which allows one to write a element of finite degree in a λ-ring as a sum of elements of degree 1 in a possibly larger λ-ring.

A.25 Theorem (Splitting Principle) *Let x be an element of degree n in a λ-ring R. Then there exists a λ-ring S containing R such that*

$$x = x_1 + \cdots + x_n$$

in S, in which each x_i is of degree 1. Moreover, if R is augmented with $\varepsilon(x) = m$, then the augmentation can be extended to S in such a way that

$$\varepsilon(x_i) = \begin{cases} 1 & \text{if } 1 \leqslant i \leqslant m,\\ 0 & \text{if } m < i \leqslant n.\end{cases}$$

To prove this theorem, we need some lemmas

A.26 Lemma *The polynomial $P_{n,m}$ in A.4 satisfies*

$$P_{n,m}(s_1, \cdots, s_{m-1}, 0, \cdots, 0) = 0.$$

Therefore every nonzero term in $P_{n,m}(s_1, \cdots, s_{nm})$ contains a factor of s_i for some $i \geqslant m$.

Proof: Recall that $P_{n,m}$ is the polynomial with integer coefficients in nm indeterminates such that the coefficient of t^n in

$$g(t) = \prod_{1 \leqslant i_1 < \cdots < i_m \leqslant nm} (1 + x_{i_1} \cdots x_{i_m} t).$$

is $P_{n,m}(s_1, \cdots, s_{nm})$, where s_i is the i-th elementary symmetric polynomial of $x_1, \cdots, x_{nm}$. Setting $x_m = x_{m+1} = \cdots = x_{nm} = 0$ in $g(t)$, it follows that the coefficient of t^n is 0. This proves the statement. □

A.27 Lemma *Let x be an element of degree n in a λ-ring R. In the polynomial λ-ring $R[\xi]$ in which ξ has degree 1, the ideal I generated by the element*

$$z = \xi^n - \lambda^1(x)\xi^{n-1} + \cdots + (-1)^{n-1}\lambda^{n-1}(x)\xi + (-1)^n\lambda^n(x)$$

is a λ-ideal.

Proof: By (iv) of Proposition A.7, it suffices to show that $\lambda^m(z) \in I$ for $m \geqslant 1$. To do this, we first claim that I is also generated by $\lambda^n(x - \xi)$. Considering

$$\lambda_t(x - \xi) = (1 + \lambda^1(x)t + \cdots + \lambda^n(x)t^n)(1 + \xi t)^{-1},$$

we have for $r \geqslant 0$,

$$\lambda^{n+r}(x - \xi) = (-1)^{n+r}\xi^r(\xi^n - \lambda^1(x)\xi^{n-1} + \cdots + (-1)^n\lambda^n(x)),$$

in particular, $\lambda^n(x - \xi) = (-1)^n z$ and so I is also generated by $\lambda^n(x - \xi)$.

To prove the Lemma, it suffices to show that $\lambda^m(\lambda^n(x - \xi)) \in I$ for $m \geqslant 1$. But we have

$$\lambda^m(\lambda^n(x - \xi)) = P_{m,n}(\lambda^1(x - \xi), \cdots, \lambda^{mn}(x - \xi)).$$

By Lemma A.26, the right side of above is a sum of terms, each one containing a factor of $\lambda^{n+r}(x - \xi) = (-1)^{n+r}\xi^r z \in I$ for some $r \geqslant 0$, thus $\lambda^m(\lambda^n(x - \xi)) \in I$. □

A.28 Lemma *Let x be an element of degree n in a λ-ring R. Then there exists a λ-ring $R[x_1]$ containing R such that $\deg_\lambda(x_1) = 1$ and $\deg_\lambda(x - x_1) = n - 1$. Moreover, if R is augmented with $\varepsilon(x) = m$, then the augmentation can be extended to $R[x_1]$ in such a way that*

$$\varepsilon(x_1) = \begin{cases} 1 & \textit{if } m > 0, \\ 0 & \textit{if } m = 0. \end{cases}$$

and then

$$\varepsilon(x - x_1) = \begin{cases} m - 1 & \textit{if } m > 0, \\ 0 & \textit{if } m = 0. \end{cases}$$

Proof: Let ξ and I be as in Lemma A.27, and let $R[x_1] = R[\xi]/I$. Then x_1 is of degree 1 since so is ξ. Moreover, the element $x - x_1$ is of degree $n-1$ since $\lambda^{n+r}(x-\xi) \in I$ for some $r \geqslant 0$ and $\lambda^{n-1}(x-\xi) \notin I$.

Now, let R be augmented with $\varepsilon(x) = m$. Then, by Proposition A.8, $R[\xi]$ is augmented with $\varepsilon(\xi) = 0$ or 1. Note that if $\varepsilon(I) = 0$, then $R[x_1]$ is naturally augmented by $\varepsilon(\omega + I) = \varepsilon(\omega)$ for $\omega \in R[\xi]$. If $\varepsilon(x) = m$, then

$$\varepsilon(\lambda^r(x)) = \lambda^r(\varepsilon(x)) = \binom{m}{r}.$$

Now if $m > 0$, choose $\varepsilon(\xi) = 1$. Then

$$\begin{aligned}\varepsilon(z) &= \varepsilon(\xi^n - \lambda^1(x)\xi^{n-1} + \cdots + (-1)^{n-1}\lambda^{n-1}(x)\xi + (-1)^n\lambda^n(x)) \\ &= 1 - \binom{m}{1} + \cdots + (-1)^m\binom{m}{m} = (1-1)^m = 0,\end{aligned}$$

and thus $\varepsilon(I) = 0$. Then $R[x_1]$ can be augmented by $\varepsilon(x_1) = 1$.

If $m = 0$, choose $\varepsilon(\xi) = 0$. Then $\varepsilon(z) = 0$, thus $\varepsilon(I) = 0$. Then $R[x_1]$ can be augmented by $\varepsilon(x_1) = 0$. □

Proof (of Theorem A.25): By downward induction on $n = \deg_\lambda(x)$, we obtain a λ-ring $S = R[x_1, \cdots, x_n]$ in which each x_i is of degree 1 and $\deg_\lambda(x - x_1 - \cdots - x_n) = 0$, i.e., $x = x_1 + \cdots + x_n$ as desired. □

5 γ-filtration and Adams operations

A.29 (γ-ring) Let R be a λ-ring. We define the corresponding ***γ-structure*** γ^n and ***Grotbendieck power series*** γ_t as

$$\gamma^n(x) = \lambda^n(x + n - 1) \quad \text{and} \quad \gamma_t(x) = \sum_{n=0}^{\infty} \gamma^n(x)t^n.$$

One can see

$$\gamma_t(x) = \lambda_{t/(1-t)}(x) \quad \text{and} \quad \lambda_s(x) = \gamma_{s/(1+s)}(x).$$

The following statements are easy to check:

(i) $\gamma^n(x+y) = \sum \gamma^i(x)\gamma^{n-i}(y)$.

(ii) $\gamma_t(1) = \frac{1}{1-t}$. More generally, $\gamma_t(m) = (1-t)^{-m}$

(iii) The map $\gamma_t \colon R \to \Lambda(R)$ is also a group homomorphism.

(iv) $\gamma^n(x) = \sum_{i=0}^{\infty} \binom{n-1}{i}\lambda^{n-i}(x)$.

(v) $\lambda^n(x) = \sum_{i=0}^{\infty} (-1)^i\binom{n-1}{i}\gamma^{n-i}(x)$.

(vi) If $\deg_\lambda(x) = 1$, then $\gamma_t(x-1) = 1 + (x-1)t$ and thus $\deg_\gamma(x-1) \leqslant 1$. More generally, $\deg_\lambda(x) = n$ implies $\deg_\gamma(x-n) \leqslant n$.

(vii) Similar to Theorem A.24, there is a **verification principle** for γ-structures.

Now, suppose R is augmented with $\varepsilon\colon R \to \mathbb{Z}$ and $I = \ker\varepsilon$. We define a decreasing filtration $F_\gamma^\bullet$ on R as follows. First, let F_γ^n be the additive subgroup of R generated by monomials $\gamma^{n_1}(a_1)\cdots\gamma^{n_r}(a_r)$ with $a_i \in I$ and $\sum n_i \geqslant n$. We have

A.30 Proposition *$F_\gamma^\bullet$ is a decreasing filtration of the λ-ring R, which means*

(i) $F_\gamma^0 = R \supset F_\gamma^1 = I \supset F_\gamma^2 \supset \cdots$*;*

(ii) $F_\gamma^m F_\gamma^n \subset F_\gamma^{m+n}$*;*

(iii) each F_γ^n *is a* λ*-ideal of* R *for* $n \geqslant 1$*.*

Proof: (i), (ii) are obvious. By Proposition A.11, $R = \mathbb{Z} \oplus F_\gamma^1$ and so F_γ^n is an ideal for $n \geqslant 1$. To show F_γ^n is a λ-ideal, it suffices to show $\lambda^m(\gamma^n(x)) \in F_\gamma^n$ for all $x \in I$.

Indeed, we have

$$\begin{aligned}\lambda^m(\gamma^n(x)) &= \lambda^m(\lambda^n(x+n-1)) \\ &= P_{m,n}(\lambda^1(x+n-1), \cdots, \lambda^{mn}(x+n-1)).\end{aligned}$$

By Lemma A.26, $\lambda^m(\gamma^n(x))$ is a sum of monomials each a multiple of some $\lambda^i(x+n-1)$ for $i \geqslant n$. It remains to show them belong to F_γ^n.

Let $s = i - n$, then we have

$$\begin{aligned}\lambda^i(x+n-1) &= \gamma^{n+s}(x-s) \\ &= \sum_{r=0}^{n+s} \gamma^{n+s-r}(x)\gamma^r(-s).\end{aligned}$$

Since $\gamma^r(-s) = 0$ for $r > s \geqslant 0$, we have

$$\lambda^i(x+n-1) = \sum_{r=0}^{s} \gamma^{n+s-r}(x)\gamma^r(-s) \in F_\gamma^n.$$

Thus F_γ^n is a λ-ideal. □

This filtration is called the ***γ-filtration*** of R. We write $\mathrm{Gr}(R)$ for the graded ring associated to the γ-filtration, i.e.

$$\mathrm{Gr}_n(R) := F_\gamma^n / F_\gamma^{n+1}.$$

For any $x \in R$, one can see that $x - \varepsilon(x) \in I$, hence $\gamma^n(x - \varepsilon(x)) \in F_\gamma^n$. We define the n-th ***algebraic Chern class*** of x to be

$$c^n(x) := \gamma^n(x - \varepsilon(x)) \bmod F_\gamma^{n+1}.$$

6 Adams operations

A.31 (Adams operation) Let R be a λ-ring. The ***Adams operations*** ψ^n on R is defined by the generating function

$$\psi_t(x) = \sum_{n=1}^{\infty} \psi^n(x) t^n$$

satisfying

$$\psi_{-t}(x) = -t \frac{\mathrm{d}}{\mathrm{d}\,\mathrm{t}} \log\left(\lambda_t(x)\right) = -t \frac{\lambda_t'(x)}{\lambda_t(x)}.$$

One can verify from Remark A.21 that

$$\psi^n(x) = \nu_n(\lambda^1(x), \cdots, \lambda^n(x)),$$

where ν_n is the integral polynomial satisfying

$$\nu_n(s_1, \cdots, s_r) = x_1^n + \cdots + x_r^n.$$

A.32 Lemma *ψ^n is a λ-homomorphism. Moreover, $\psi^m\psi^n = \psi^{mn} = \psi^n\psi^m$. Let p be a prime number, then*

$$\psi^{p^r}(x) \equiv x^{p^r} \bmod p.$$

Proof: By Theorem A.25, we can write any $x, y \in R$ as sum $\sum x_i, \sum y_j$ of elements of degree 1 in a larger λ-ring. Then we have

$$\begin{aligned}
\psi^n(x+y) &= \sum x_i^n + \sum y_j^n = \psi^n(x) + \psi^n(y); \\
\psi^n(xy) &= \psi^n(\sum x_i y_j) = \sum (x_i y_j)^n = \sum x_i^n \sum y_j^n = \psi^n(x)\psi^n(y); \\
\psi^n(\lambda^m(x)) &= \psi^n(s_m(x_1, \cdots, x_r)) = s_m(x_1^n, \cdots, x_r^n) \\
&= \lambda^m(\sum x_i^n) = \lambda^m(\psi^n(x)).
\end{aligned}$$

Therefore, ψ^n is a λ-homomorphism.

As for the rest, by Theorem A.24, it suffices to check them for the case $x = s_1$, which is obvious. □

A.33 Lemma (Newton formula for Adams operations) *In any λ-ring R, the equality*

$$\psi^k(x) - \lambda^1(x)\psi^{k-1}(x) + \cdots + (-1)^{k-1}\lambda^{k-1}(x)\psi^1(x) = (-1)^{k+1}k\lambda^k(x)$$

holds for $x \in R$ and $k \geqslant 1$.

Proof: First, by the definition, we have

$$\psi_{-t}(x)\lambda_t(x) + t\lambda_t'(x) = 0.$$

Expanding it, we obtain

$$\left(\sum_{m=1}^{\infty} \psi^m(x)(-t)^m\right)\left(\sum_{n=0}^{\infty} \lambda^n(x)t^n\right) + \sum_{n=1}^{\infty} k\lambda^k(x)t^k.$$

Compare the coefficient of t^k, we obtain the required equality. □

By straightforward calculation, the Newton formula implies the following formulas.

$$\psi^n(x) = \det\begin{pmatrix} \lambda^1(x) & 1 & 0 & \dots & 0 \\ 2\lambda^2(x) & \lambda^1(x) & 1 & \ddots & \vdots \\ 3\lambda^3(x) & \lambda^2(x) & \ddots & \ddots & 0 \\ \vdots & \vdots & \ddots & \lambda^1(x) & 1 \\ n\lambda^n(x) & \lambda^{n-1}(x) & \dots & \lambda^2(x) & \lambda^1(x) \end{pmatrix},$$

$$n!\lambda^n(x) = \det\begin{pmatrix} \psi^1(x) & 1 & 0 & \dots & 0 \\ \psi^2(x) & \psi^1(x) & 2 & \ddots & \vdots \\ \psi^3(x) & \psi^2(x) & \ddots & \ddots & 0 \\ \vdots & \vdots & \ddots & \psi^1(x) & n-1 \\ \psi^n(x) & \psi^{n-1}(x) & \dots & \psi^2(x) & \psi^1(x) \end{pmatrix}.$$

One can see when R is ***$\mathbb{Z}$-torsion-free***, which means there exists no nonzero $x \in R$ such that $nx = 0$ for some $n \in \mathbb{Z}$, the above formulas allow us to write λ^n in terms of $\psi^1, \cdots, \psi^n$. Therefore

A.34 Theorem *In a $\mathbb{Z}$-torsion-free λ-ring, the λ-structure can be uniquely determined by its Adams operations.*

A.35 Corollary *Let $f\colon R \to S$ be a ring homomorphism between λ-rings in which S is $\mathbb{Z}$-torsion-free. If f commutes with Adams operators, then it is a λ-homomorphism.*

A.36 Lemma *Let R be an augmented λ-ring with augmentation $\varepsilon\colon R \to \mathbb{Z}$ with $I = \ker\varepsilon$ and γ-filtration $F_\gamma^\bullet$. If $x \in F_\gamma^n$, then $\psi^k(x) - k^n x \in F_\gamma^{n+1}$.*

Proof: First, it suffices to show $\psi^k\gamma^n x - k^n\gamma^n x \in F_\gamma^{n+1}$ for $x \in I$. Since $\psi^k\gamma^n - k^n\gamma^n$ is a natural operation on R, by verification principle for γ, we may assume $x = x_1 + \cdots + x_r$ with $\deg_\gamma(x_i) = 1$. Note that for those x_i, $\psi^k(x_i) = (1 + x_i)^k - 1$. Then

$$\begin{aligned}\psi^k\gamma^n x - k^n\gamma^n x &= \gamma^n\psi^k(x_1 + \cdots + x_r) - k^n s_n(x_1, \cdots, x_r)\\ &= s_n((x_1+1)^k - 1, \cdots, (x_r+1)^k - 1) - k^n s_n(x_1, \cdots, x_r),\end{aligned}$$

which is a symmetric polynomial of degree $\geqslant n + 1$. □

A.37 Corollary *The Adams operation ψ^k acts as k^n on* $\mathrm{Gr}_n(R)$.

7 The "heterodox" definition of λ-rings

Now, we give the "heterodox" definition of λ-rings.

A.38 Let A be an $\mathbb{F}_p$-algebra, then its ***Frobenius endomorphism*** is given by

$$\begin{aligned}F_p\colon A &\longrightarrow A\\ x &\longmapsto x^p.\end{aligned}$$

A ***p-typical ψ-ring*** is a commutative ring R equipped with a ***lift of Frobenius***, which means an endomorphism $F\colon R \to R$ satisfying

$$F \otimes \mathbb{F}_p = F_p.$$

A ***ψ-ring*** is a commutative ring equipped with a lift of Frobenius for each prime number p such that those lifts commute.

Lemma A.32 shows that any λ-ring R is a ψ-ring as ψ^p is a lift of Frobenius for prime number p.

Conversely, let R be a ψ-ring with lifts ψ^p and has characteristic 0. We define

$$\psi^{p^\nu} := \underbrace{\psi^p \circ \cdots \circ \psi^p}_{\nu},$$

and ψ^n for $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ by

$$\psi^n := \psi^{p_1^{\nu_1}} \circ \cdots \circ \psi^{p_r^{\nu_r}}.$$

Define

$$\psi_t(x) = \sum_{n=1}^{\infty} \psi^n(x) t^n,$$

and let

$$\lambda_t(x) = \exp\left(\oint \frac{\psi_{-t}(x)}{t}\,\mathrm{d}\,t\right).$$

Then, this gives a λ-structure on R whose Adams operations are ψ^n.

§ 5 Local Fields

I Review

A ***global field*** is a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_p(t)$. A ***local field*** is a complete valued field with respect to a discrete valuation and have a finite residue class field. For such a local field, the normalized exponential valuation is denoted by $v_{\mathfrak{p}}$, and $|\ |_{\mathfrak{p}}$ denotes the absolute value normalized by

$$|x|_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(x)},$$

where q is the cardinality of the residue class field.

(5.1) Proposition *A local field K is locally compact. Its valuation ring $\mathcal{O}$ is compact.*

(5.2) Proposition *The local fields are precisely the finite extensions of the fields $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.*

Remark: One can show that a field K which is locally compact with respect to a nondiscrete topology is isomorphic either to either $\mathbb{R}$ or $\mathbb{C}$, or to a local field (see [Weil, chap. I, §3]).

The local fields of characteristic $p \neq 0$ are the power series fields $\mathbb{F}_q((t))$, with $q = p^f$. The local fields of characteristic 0, i.e., the finite extensions of the fields of p-adic numbers $\mathbb{Q}_p$, are called ***p-adic number field***.

We next define the ***exponential function*** and ***logarithm function***. To do this, we use the following lemmas:

A.1 Lemma *Let K be a p-adic number field, a series $\sum a_n$ on K converges if and only if $|a_n|_{\mathfrak{p}}$ converges to 0.*

A.2 Lemma *Let K be a p-adic number field, then*

(i) $v_p(n!) = \sum_{i=1}^{r}[\frac{n}{p^i}]$. (this is (5.6).)

(ii) For $c \in \mathbb{R}$, one has:

$$nc - v_p(n!) \to \infty \iff c > \frac{1}{p-1},$$
$$nc - v_p(n) \to \infty \iff c > 0.$$

(iii) If $c > \frac{1}{p-1}$, then $nc - v_p(n!) > c$ for all n.

Here v_p is the extension of the normalized valuation v_p of $\mathbb{Q}_p$ on K. So, if $p\mathcal{O} = \mathfrak{p}^e$, then one has $v_{\mathfrak{p}} = ev_p$.

A.3 Lemma *The formal sum and product of convergence power series converge.*

A.4 Theorem *Let K be a p-adic number field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{p}$, and let $p\mathcal{O} = \mathfrak{p}^e$. Let $\exp(x), \log(1+x)$ be the following power sieres*

$$\exp(x) = \sum_{\nu=0}^{\infty} \frac{1}{\nu!} x^\nu \quad \textit{and} \quad \log(1+x) = \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} x^\nu .$$

(i) The following equalities for formal power series hold:

$$\begin{aligned} &\exp(x+y) = \exp(x)\exp(y), \\ &\log((1+x)(1+y)) = \log(1+x) + \log(1+y), \\ &\exp\log(1+x) = 1+x, \\ &\log\exp(x) = x. \end{aligned}$$

(ii) The convergence domain of exp *and* log *are*

$$\begin{aligned} D_{\exp} &= \left\{ v_p(x) > \frac{1}{p-1} \right\} = \left\{ v_{\mathfrak{p}}(x) > \frac{e}{p-1} \right\}, \\ D_{\log} &= \{ v_p(x) > 0 \} = \{ v_{\mathfrak{p}}(x) > 0 \}. \end{aligned}$$

(iii) When $n > \frac{e}{p-1}$, exp *and* log *yield two mutually inverse isomorphisms (and homeomorphisms)*

$$\begin{tikzcd} \mathfrak{p}^n \arrow[r, shift left, "\exp"] & U^{(n)} \arrow[l, shift left, "\log"] \end{tikzcd}.$$

(This is (5.5)*.)*

In ANT, those results are organized as follows. First, a lemma

(5.3) Proposition *The multiplicative group of a local field K admits the decomposition*

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)}.$$

Here π is a prime element, $(\pi) = \{\pi^k | k \in \mathbb{Z}\}$, $q = \#\kappa$ is the number of elements in the residue class field $\kappa = \mathcal{O}/\mathfrak{p}$, and $U^{(1)} = 1 + \mathfrak{p}$ is the group of principal units.

Then, the logarithm function can be continued to whole K^*.

(5.4) Proposition *For a p-adic number field K there is a uniquely determined continuous homomorphism*

$$\log \colon K^* \to K$$

such that $\log p = 0$ which on principal units $(1+x) \in U^{(1)}$ is given by the series

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots .$$

The following proposition is the main theorem.

(5.5) Proposition *Let K be a p-adic number field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{p}$, and let $p\mathcal{O} = \mathfrak{p}^e$. Then the power series*

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \quad \textit{and} \quad \log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots ,$$

yield, for $n > \frac{e}{p-1}$, two mutually inverse isomorphisms (and homeomorphisms)

$$\begin{tikzcd}\mathfrak{p}^n \arrow[r, shift left, "\exp"] & U^{(n)}. \arrow[l, shift left, "\log"]\end{tikzcd}$$

Finally, the following lemma is used in the proof of (5.5).

(5.6) Lemma *Let $\nu = \sum_{i=0}^{r} a_i p^i, 0 \geqslant a_i < p$, be the p-adic expansion of the natural number $\nu \in \mathbb{N}$. Then*

$$v_p(\nu!) = \frac{1}{p-1} \sum_{i=0}^{r} a_i(p^i - 1).$$

Next, we determine explicitly the structure of the locally compact multiplicative group K^* of a local field K.

First, the group of principal units $U^{(1)}$ is a $\mathbb{Z}_p$-module. This follows from the fact that $U^{(1)}/U^{(n+1)}$ is a $\mathbb{Z}/q^n\mathbb{Z}$-module, where $q = \#\kappa$ and the formulas

$$U^{(1)} = \varprojlim_n U^{(1)}/U^{(n+1)} \quad \text{and} \quad \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/q^n\mathbb{Z}.$$

Secondary, the The function $f(z) = (1+x)^z$ is continuous.

(5.7) Proposition *Let K be a local field and $q = p^f$ the number of elements in the residue class field. Then the following hold.*

(i) If K has characteristic 0, then one has (both algebraically and topologically)

$$K^* = \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

where $a \geqslant 0$ and $d = [K : \mathbb{Q}_p]$.

(ii) If K has characteristic p, then one has (both algebraically and topologically)

$$K^* = \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}.$$

(5.8) Corollary *If the natural number n is not divisible by the characteristic of K, then one finds the following indices for the subgroups of n-th powers K^{*n} and U^n in the multiplicative group K^* and in the unit group U:*

$$(K^* : K^{*n}) = n(U : U^n) = \frac{n}{|n|_{\mathfrak{p}}} \#\mu_n(K).$$

II Exercises

1 The logarithm function can be continued to a continuous homomorphism $\log\colon \overline{\mathbb{Q}_p}^* \to \mathbb{Q}$**, and the exponential function to a continuous homomorphism** $\exp\colon \overline{\mathfrak{p}}^{\frac{1}{1-p}} \to \overline{\mathbb{Q}_p}^*$**, where**

$$\overline{\mathfrak{p}}^{\frac{1}{1-p}} = \left\{ x \in \overline{\mathbb{Q}_p} \middle| v_p(x) > \frac{1}{1-p} \right\}$$

and v_p **is the unique extension of the normalized valuation on** $\mathbb{Q}_p$**.**

Why the codomain of log is $\mathbb{Q}$? There must be something wrong. If the correct notation is $\overline{\mathbb{Q}_p}$, then this follows from Lemma A.2.

2 Let K **be a** p**-adic number field. For** $1 + x \in U^{(1)}$ **and** $z \in \mathbb{Z}_p$ **one has**

$$(1+x)^z = \sum_{\nu=0}^{\infty} \binom{z}{\nu} x^\nu.$$

The series converges even for $x \in K$ **such that** $v_p(x) > \frac{e}{p-1}$**.**

Proof: Let $z = \lim z_i$ with $z_i \in \mathbb{Z}$, then we have

$$(1+x)^z = \lim_{i\to\infty} (1+x)^{z_i}.$$

But the binomial theorem,

$$(1+x)^z = \lim_{i\to\infty} \sum_{\nu=0}^{\infty} \binom{z_i}{\nu} x^\nu = \sum_{\nu=0}^{\infty} \binom{z}{\nu} x^\nu,$$

where $\binom{z_i}{\nu} = 0$ if $z_i \in \mathbb{Z}$ and $z_i < \nu$.

By Lemma A.1, the later series converges when $v_p(\binom{z}{\nu} x^\nu) \to \infty$ with $\nu \to \infty$. Since

$$\begin{aligned} v_p(\binom{z}{\nu} x^\nu) &= v_p(\frac{z! x^\nu}{\nu!(z-\nu)!}) \\ &= \nu v_p(x) + v_p(z!) - v_p(\nu!) - v_p((z-\nu)!) \\ &= \nu v_p(x) - v_p(\nu!). \end{aligned}$$

We see that the series converges when $v_p(x) > \frac{e}{p-1}$ by Lemma A.2. □

3 Under the above hypotheses one has

$$(1+x)^z = \exp(z \log(1+x)) \quad \textbf{and} \quad \log(1+x)^z = z \log(1+x).$$

4 For a p-adic number field K, every subgroup of finite index in K^* is both open and closed.

Proof: It suffices to prove this for $\mathbb{Z}_p$ since Proposition (5.7), while which is obvious. □

5 If K is a p-adic number field, then the groups K^{*n}, for $n \in \mathbb{N}$, form a basis of neighbourhoods of 1 in K^*.

Corollary (5.8)

6 Let K be a p-adic number field, $v_\mathfrak{p}$ the normalized exponential valuation of K, and dx the *Haar measure* on the locally compact additive group K, scaled so that $\int_\mathcal{O} dx = 1$. Then one has $v_\mathfrak{p}(a) = \int_{a\mathcal{O}} dx$. Furthermore,

$$I(f) = \int_{K^*} \frac{f(x)}{|x|_\mathfrak{p}} dx$$

is a Haar measure on the locally compact group K^*.

§ 6 Henselian Fields

I Review

Let (K, v) be a nonarchimedean valued field and $\widehat{K}$ its completion. Let $\mathcal{O}$, resp. $\widehat{\mathcal{O}}$, be the valuation rings of K, resp. $\widehat{K}$, with the maximal ideal $\mathfrak{p}$, resp. $\widehat{\mathfrak{p}}$. The ***henselization*** of the field K with respect to v is the valued field K_v, obtained by prolonging v to the separable closure K_v of K in $\widehat{K}$. Let $\mathcal{O}_v$ and $\mathfrak{p}_v$ denote the valuation ring and its maximal ideal of K_v.

In the case of K_v equals the algebraic closure of K in $\widehat{K}$, one can show that *Hensel's lemma* in the sense of (4.6) holds for $\mathcal{O}_v$. This follows from *Hensel's lemma* for $\widehat{\mathcal{O}}$, i.e. (4.6), and *Gauss's lemma* (cf. Lemma I.2.2.4)

(6.1) Definition A ***henselian field*** is a field with a nonarchimedean valuation v whose valuation ring $\mathcal{O}$ satisfies *Hensel's lemma* in the sense of (4.6). One also calls the valuation v or the valuation ring $\mathcal{O}$ henselian.

Remark: In general, a local ring is called Henselian if *Hensel's lemma* holds.

The results in this section can be summarized into the following theorem:

A.1 Theorem *Let (K, v) be a nonarchimedean valued field. The followings are equivalent:*

(i) (K, v) is Henselian;

(ii) v admits a unique extension to any given algebraic extension $L|K$;

(iii) Newton polygon of irreducible polynomials over K consists of a single segment;

(iv) The weak version of Hensel's Lemma *explained in* (6.7) *holds for $\mathcal{O}$.*

Proof: *(i)⇒(ii)* is (6.2), *(ii)⇒(iii)* is (6.4), *(iii)⇒(i)* is (6.6), *(i)⇒(iv)* is obvious and *(iv)⇒(iii)* is (6.7). □

(6.2) Theorem *Let K be a henselian field with respect to the valuation $|\ |$. Then $|\ |$ admits one and only one extension to any given algebraic extension $L|K$. It is given by*

$$|\alpha| = \sqrt[n]{N_{L|K}(\alpha)},$$

if $L|K$ has finite degree n. In any case, the valuation ring of the extended valuation is the integral closure of the valuation ring of K in L.

The main tool used in this section is Newton polygon of polynomials.

Let v be an arbitrary exponential valuation of the field K and let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$$

be a polynomial satisfying $a_0 a_n \neq 0$. To each nonzero term $a_i x^i$ we associate a point $(i, v(a_i)) \in \mathbb{R}^2$. We now take the lower convex envelope of the set of points

$$\{(0, v(a_0)), (i, v(a_i)), \cdots, (n, v(a_n))\}.$$

This produces a polygonal chain which is called the ***Newton polygon*** of $f(X)$.

(6.3) Proposition *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_0 a_n \neq 0$, be a polynomial over the held K, v an exponential valuation of K, and w an extension to the splitting field L of f.*

If $(r, v(a_r)) \leftrightarrow (s, v(a_s))$ is a line segment of slope $-m$ occurring in the Newton polygon of f, then $f(x)$ has precisely $s - r$ roots $\alpha_1, \cdots, \alpha_{s-r}$. of value

$$w(\alpha_1) = \cdots = w(\alpha_{s-r}) = m.$$

$f(x)$ factors into a product according to the slopes $-m_r < \cdots < -m_l$,

$$f(x) = a_n \prod_{j=1}^{r} f_j(x),$$

where

$$f_j(x) = \prod_{w(\alpha_i)=m_j} (x - \alpha_i).$$

Here the factor f_j corresponds to the $(r - j + 1)$-th segment of the Newton polygon, whose slope equals minus the value of the roots of f_j.

(6.4) Proposition *If the valuation v admits a unique extension w to the splitting field L of f, then the factorization*

$$f(x) = a_n \prod_{j=1}^{r} f_j(x),$$

is defined already over K, i.e., $f_j \in K[x]$.

If the polynomial f is irreducible, then, by the above factorization result, the Newton polygon consists of a single segment.

(6.5) Corollary *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ be an irreducible polynomial with $a_n \neq 0$. Then, if $|\ |$ is a nonarchimedean valuation of K with a unique extension to the splitting field, one has*

$$|f| = \max\{|a_0|, |a_n|\}.$$

(6.6) Theorem *A nonarchimedean valued field $(K, |\ |)$ is henselian if and only if the valuation $|\ |$ can be uniquely extended to any algebraic extension of K.*

(6.7) Proposition *A nonarchimedean field (K, v) is henselian if any monic polynomial $f(x) \in \mathcal{O}[x]$ which splits over the residue class field $\kappa = \mathcal{O}/\mathfrak{p}$ as*

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \bmod \mathfrak{p}$$

with relatively prime monic factors $\overline{g}(X), \overline{h}(x) \in \kappa[x]$, admits itself a splitting

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

into monic factors $g(x), h(x) \in \mathcal{O}[x]$ such that

$$g(x) \equiv \overline{g}(x) \bmod \mathfrak{p} \quad \textit{and} \quad h(x) \equiv \overline{h}(x) \bmod \mathfrak{p}.$$

Let K be a field which is henselian with respect to the exponential valuation v. If $L|K$ is a finite extension of degree n, then v extends uniquely to an exponential valuation w of L, namely

$$w(\alpha) = \frac{1}{n} v(N_{L|K}(\alpha)).$$

For the value groups and residue class fields of v and w, one gets the inclusions

$$v(K^*) \subset w(L^*) \quad \text{and} \quad \kappa \subset \lambda.$$

The index

$$e = e(w|v) := (w(L^*) : v(K^*))$$

is called the ***ramification index*** of the extension $(L, w)|(K, v)$ and the degree

$$f = f(w|v) := [\lambda : \kappa]$$

is called the ***inertia degree***.

(6.8) Proposition *One has $[L : K] > ef$ and the fundamental identity*

$$[L : K] = ef,$$

if v is discrete and $L|K$ is separable.

Remark: the separability condition can be dropped once K is complete with respect to the discrete valuation.

II Exercises

1 **In a henselian field the zeroes of a polynomial are continuous functions of its coefficients. More precisely, one has: let $f(x) \in K[x]$ be a monic polynomial of degree n and**

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

its decomposition into linear factors, with $m_i \geqslant 1$, $\alpha_i \neq \alpha_j$ for $i \neq j$. If the monic polynomial $g(x)$ of degree n has all coefficients sufficiently close to those of $f(x)$, then it has r roots $\beta_1, \cdots, \beta_r$, which approximate the $\alpha_1, \cdots, \alpha_r$ to any previously given precision.

2 **(Krasner's Lemma) Let $\alpha \in \overline{K}$ be separable over K and let $\alpha_1 = \alpha, \cdots, \alpha_n$ be its conjugates over K. If $\beta \in \overline{K}$ is such that**

$$|\alpha - \beta| < |\alpha - \alpha_i| \quad \textbf{for} \quad i = 2, \cdots, n,$$

then one has $K(\alpha) \subset K(\beta)$.

3 **(Theorem of F. K. Schmidt) A field which is henselian with respect to two inequivalent valuations is separably closed.**

4 **A separably closed field K is henselian with respect to any nonarchimedean valuation.**

More generally, every valuation of K admits a unique extension to any purely inseparable extension $L|K$.

5 **Let K be a nonarchimedean valued field, $\mathcal{O}$ the valuation ring, and $\mathfrak{p}$ the maximal ideal. K is henselian if and only if every polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}[x]$ such that $a_0 \in \mathfrak{p}$ and $a_1 \notin \mathfrak{p}$ has a zero $a \in \mathfrak{p}$.**

6 **A local ring $\mathcal{O}$ is henselian if and only if every finite commutative $\mathcal{O}$-algebra A splits into a direct product $A = \prod_{i=1}^{r} A_i$ of local rings A_i.**

This is a characterization of henselian rings which is important in algebraic geometry. Cf. [Milne, chap. I, §4, th. 4.2].

§ 7 Unramified and Tamely Ramified Extensions

In this section, we fix a base field K which is henselian with respect to a nonarchimedean valuation v.

I Review

(7.1) Definition A finite extension $L|K$ is called ***unramified*** if the extension $\lambda|\kappa$ of the residue class field is separable and one has

$$[L:K]=[\lambda:\kappa].$$

An arbitrary algebraic extension $L|K$ is called ***unramified*** if it is a union of finite unramified subextensions.

Remark: This definition does not require K to be henselian; it applies in all cases where v extends uniquely to L.

Many definitions and results can be simplified if one has introduced the notion of *supernatural numbers.*

A.1 A ***supernatural number*** is a formal product

$$n=\prod_p p^{v_p(n)},$$

where $v_p(n)$ is either a natural number or ∞, and p ranges over all primes.

Let m and n be supernatural numbers. We say that m *divides* n if $v_p(m)\leqslant v_p(n)$ for every prime p. Define the *product* of supernatural numbers n_i, for $i\in I$, by the formula

$$\prod_{i\in I} n_i := \prod_p p^{\sum_{i\in I} v_p(n_i)}.$$

The *greatest common divisor* and *least common multiple* of supernatural numbers n_i, for $i\in I$, are defined by

$$\gcd(\{n_i\}) := \prod_p p^{\inf(v_p(n_i))} \quad\text{and}\quad \operatorname{lcm}(\{n_i\}) := \prod_p p^{\sup(v_p(n_i))}.$$

The set $\widehat{\mathbb{N}}$ of supernatural numbers can be viewed as an extension of the monoid $\mathbb{N}$ by the *fundamental theorem of arithmetic* and setting

$$0=\prod_p p^{\infty}.$$

Supernatural numbers are used for profinite groups and field extensions.

Recall that a profinite group is an inverse limit of finite groups and hence its open subgroups are those of finite index.

Using supernatural numbers, one can define the ***index*** of a closed subgroup H in a *profinite* group G to be

$$(G : H) := \operatorname{lcm}\left((G : U) | U \text{ is an open subgroup of } G \text{ that contains } H\right).$$

Then define the ***order*** of G to be

$$|G| := (G : 1) = \operatorname{lcm}\left((G : U) | U \text{ is an open subgroup of } G\right).$$

Let $L|K$ be an algebraic extension. Its ***degree*** is defined to be

$$[L : K] := \operatorname{lcm}\left([E : K] | E|K \text{ is a finite subextension of } L|K\right).$$

A.2 Theorem *Unramified extensions form a* **distinguished class***, which means*

(i) Let $N|L|K$ be a tower of fields. The extension $N|K$ is unramified *if and only if both $N|L$ and $L|K$ are* unramified*.*

(ii) Let $L|K$ and $K'|K$ be two extensions inside an algebraic closure and let $L' = LK'$. If $L|K$ is unramified*, then so is $L'|K'$.*

(iii) The composite of two unramified *extensions of K is again* unramified*.*

Of course this theorem is stated as the following (7.2) and (7.3).

(7.2) Proposition *Let $L|K$ and $K'|K$ be two extensions inside an algebraic closure $\overline{K}|K$ and let $L' = LK'$. Then one has*

$$L|K \quad \textit{unramified} \quad \Longrightarrow \quad L'|K' \quad \textit{unramified.}$$

Each subextension of an unramified extension is unramified.

(7.3) Corollary *The composite of two unramified extensions of K is again unramified.*

(7.4) Definition Let $L|K$ be an algebraic extension. Then the composite $T|K$ of all unramified subextensions is called the ***maximal unramified subextension*** of $L|K$.

(7.5) Proposition *The residue class field of T is the separable closure λ_s of κ in the residue class field extension $\lambda|\kappa$ of $L|K$, whereas the value group of T equals that of K.*

The composite of all unramified extensions inside the algebraic closure $\overline{K}$ of K is simply called the ***maximal unramified extension*** $K_{nr}|K$ of K. Its residue class field is the separable closure $\overline{\kappa}_s|\kappa$. K_{nr} contains all roots of unity of order m not divisible by the characteristic of κ because the separable polynomial $x^m - 1$ splits over $\overline{\kappa}_s$ and hence also over K_{nr}, by *Hensel's lemma.* If κ is a finite field, then the extension $K_{nr}|K$ is even generated by these roots of unity because they generate $\overline{\kappa}_s|\kappa$.

(7.6) Definition An algebraic extension $L|K$ is called ***tamely ramified*** if the extension $\lambda|\kappa$ of the residue class fields is separable and one has $p \nmid [L:T]$. Here p is the characteristic of κ and is assumed to be positive. In the infinite case this latter condition is taken to mean that the degree of each finite subextension of $L|T$ is prime to p.

Remark: When the fundamental identity $ef = [L:K]$ holds and $\lambda|\kappa$ is separable, to say that the extension is unramified, resp. tamely ramified, simply amounts to saying that $e = 1$, resp. $(e, p) = 1$.

A.3 Theorem *Tamely ramified extensions form a* **distinguished class***, which means*

(i) Let $N|L|K$ be a tower of fields. The extension $N|K$ is tamely ramified *if and only if both $N|L$ and $L|K$ are* tamely ramified.

(ii) Let $L|K$ and $K'|K$ be two extensions inside an algebraic closure and let $L' = LK'$. If $L|K$ is tamely ramified, *then so is $L'|K'$.*

(iii) The composite of two tamely ramified *extensions of K is again* tamely ramified.

Proof: For the first statement, consider the equalities:

$$[N:K] = [N:L][L:K] \quad \text{and} \quad [\eta:\kappa] = [\eta:\lambda][\lambda:\kappa].$$

Here η denotes the residue class field of N. Let T_K^L denote the maximal unramified subextension of $L|K$ and T_K^N, T_L^N similarly, by the definitions, one has

$$[\eta:\kappa] = [T_K^N : K], \quad [\eta:\lambda] = [T_L^N : L] \quad \text{and} \quad [\lambda:\kappa] = [T_K^L : K].$$

Therefore

$$[N : T_K^N] = [N : T_L^N][L : T_K^L],$$

which implies the statement immediately. □

The following proposition provide a characterization of tamely ramified extensions, which implies the rest of the above theorem.

(7.7) Proposition *A finite extension $L|K$ is tamely ramified if and only if the extension $L|T$ is generated by radicals*

$$L = T(\sqrt[m_1]{a_1}, \cdots, \sqrt[m_r]{a_r}),$$

such that $(m_i, p) = 1$. In this case the fundamental identity always holds:

$$[L:K] = ef.$$

(7.8) Corollary *Let $L|K$ and $K'|K$ be two extensions inside an algebraic closure $\overline{K}|K$ and let $L' = LK'$. Then one has*

$$L|K \quad \textit{tamely ramified} \quad \Longrightarrow \quad L'|K' \quad \textit{tamely ramified.}$$

Each subextension of a tamely ramified extension is tamely ramified.

(7.9) Corollary *The composite of two tamely ramified extensions of K is again tamely ramified.*

(7.10) Definition Let $L|K$ be an algebraic extension. Then the composite $V|K$ of all tamely ramified subextensions is called the ***maximal tamely ramified subextension*** of $L|K$.

Let $w(L^*)^{(p)}$ denote the subgroup

$$w(L^*)^{(p)} := \{\omega \in w(L^*) | m\omega \in v(K^*) \text{ for some } m \text{ satisfying } (m,p) = 1\}\,.$$

(7.11) Proposition *The maximal tamely ramified subextension $V|K$ of $L|K$ has value group $w(V^*) = w(L^*)^{(p)}$ and residue class field equal to the separable closure λ_s of κ in $\lambda|\kappa$.*

The results obtained in this section may be summarized in the following picture:

$$\begin{array}{ccccccc}
K & \subset & T & \subset & V & \subset & L \\
\kappa & & \lambda_s & = & \lambda_s & & \lambda \\
v(K^*) & = & w(T^*) & & w(L^*)^{(p)} & & w(L^*)
\end{array}$$

If $L|K$ is finite and $e = e'p^a$ where $(e',p) = 1$, then $[V : T] = e'$. The extension $L|K$ is called ***totally (or purely) ramified*** if $T = K$, and ***wildly ramified*** if it is not tamely ramified, i.e., if $V \neq L$.

(7.12) Proposition *Let K be a local field with residue class field $\kappa = \mathbb{F}_q$, with $q = p^r$. Let $L = K(\zeta)$ and let $\mathcal{O}|\mathcal{o}$, resp. $\lambda|\kappa$, be the extension of valuation rings, resp. residue class fields, of $L|K$. Suppose that $(n,p) = 1$. Then one has:*

(i) The extension $L|K$ is unramified of degree f, where f is the smallest natural number such that of $q^f \equiv 1 \bmod n$.

(ii) The Galois group $G(L|K)$ is canonically isomorphic to $G(\lambda|\kappa)$ and is generated by the automorphism $\varphi\colon \zeta \mapsto \zeta^q$.

(iii) $\mathcal{O} = \mathcal{o}[\zeta]$.

(7.13) Proposition *Let ζ be a primitive p^m-th root of unity. Then one has:*

(i) $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ is totally ramified of degree $\varphi(p^m) = (p-1)p^{m-1}$.

(ii) $G(\mathbb{Q}_p(\zeta)|\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^*$.

(iii) $\mathbb{Z}_p[\zeta]$ *is the valuation ring of* $\mathbb{Q}_p$.

(iv) $1-\zeta$ *is a prime element of* $\mathbb{Z}_p[\zeta]$ *with norm* p.

If ζ_n is a primitive n-th root of unity and $n = n'p^m$, with $(n', p) = 1$, then Propositions 7.12 and 7.13 yield the following result for the maximal unramified and the maximal tamely ramified extension:

$$\mathbb{Q}_p \subset T = \mathbb{Q}_p(\zeta_{n'}) \subset V = T(\zeta_p) \subset \mathbb{Q}_p(\zeta_n).$$

II Exercises

1 The maximal unramified extension of $\mathbb{Q}_p$ is obtained by adjoining all roots of unity of order prime to p.

Proof: Since the field extension $K|\mathbb{Q}_p$ obtained by adjoining all roots of unity of order prime to p is unramified, it suffices to show that the residue class field κ is the separable closure of $\mathbb{F}_p$, which follows from the following Proposition 1.1. □

1.1 Proposition *The separable closure of finite field* $\mathbb{F}_q$ *with* $q = p^r$ *is obtained by adjoining all roots of unity of order prime to p.*

Proof: As every finite extension of a finite field $\mathbb{F}_q$ is separable, $\mathbb{F}_q$ is perfect. Thus, it suffices to show every finite extension of $\mathbb{F}_q$ is obtained by adjoining a root of unity of order prime to p. Indeed, let $\mathbb{F}_{q^s}|\mathbb{F}_q$ be a finite extension with primitive element ζ, then ζ is a (q^s-1)-th root of unity. □

2 Let K be henselian and $K_{nr}|K$ the maximal unramified extension. Show that the subextensions of $K_{nr}|K$ correspond 1-1 to the subextensions of the separable closure $\overline{\kappa}_s|\kappa$.

Proof: Since subextensions of $K_{nr}|K$ are unramified, they correspond 1-1 to their residue class field extensions, which are subextensions of the separable closure $\overline{\kappa}_s|\kappa$. □

3 Let $L|K$ be totally and tamely ramified, and let Δ, resp, Γ, be the value group of L, resp. K. Show that the intermediate fields of $L|K$ correspond 1-1 to the subgroups of Δ/Γ.

Proof: Since $L|K$ is totally ramified, its residue class field extension is trivial. Since $L|K$ is tamely ramified, so are the subextensions. Then the result follows from the fact that for totally and tamely ramified extension $L|K$, one has $[L:K] = (\Delta:\Gamma)$. □

§ 8 Extensions of Valuations

I Review

Let (K, v) be a valued field with completion K_v whose algebraic closure is $\overline{K_v}$. The canonical extension of v to $\overline{K}$ is again denoted by v and the unique extension of this latter valuation to $\overline{K_v}$ by $\bar{v}$.

Let $L|K$ be an algebraic extension. For any K-embedding $\tau\colon L \to \overline{K_v}$, we have an extension $w = \bar{v} \circ \tau$ of v to L.

A.1 (Localization) For finite extension $(L, w)|(K, v)$, its ***localization*** is merely the completion L_w respect to the valuation w. For infinite extension $L|K$, its ***localization*** L_w is not the completion, but the inverse limit

$$L_w := \varprojlim L_{iw}$$

of the completions of all finite subextensions $L_i|K$ of $L|K$.

The mapping $\tau\colon L \to \overline{K_v}$ is obviously continuous with respect to the valuations. It extends in a unique way to a continuous K-embedding

$$\tau\colon L_w \longrightarrow \overline{K_v}.$$

When $[L : K] < \infty$, it is given by the rule

$$x = \lim_{n\to\infty} x_n \mapsto \tau x := \lim_{n\to\infty} \tau x_n,$$

where $\{x_n\}_{n\in\mathbb{N}}$ is a w-Cauchy sequence in L, and hence $\{\tau x_n\}_{n\in\mathbb{N}}$ a v-Cauchy sequence in $\overline{K_v}$. Note here that the sequence τx_n converges in the finite complete extension $\tau L \cdot K_v$ of K_v.

We have

$$L_w = LK_v,$$

because if $L|K$ is finite, then the field $LK_v \subset L_w$ is complete by (4.8), contains the field L and therefore has to be its completion. If $L_w|K_v$ has degree $n < \infty$, then, by (4.8), the absolute values corresponding to v and w satisfy the relation

$$|x|_w = \sqrt[n]{|N_{L_w|K_v}(x)|_v}.$$

Remark (Local-to-global Principle): The field diagram

$$\begin{tikzcd} & L_w \arrow[dd, dash] \\ L \arrow[ur, dash] \arrow[dd, dash] & \\ & K_v \\ K \arrow[ur, dash] & \end{tikzcd}$$

is of central importance for algebraic number theory.

(8.1) Extension Theorem *Let $L|K$ be an algebraic field extension and v a valuation of K. Then one has:*

(i) Every extension w of the valuation v arises as the composite $w = \bar{v} \circ \tau$ for some K-embedding $\tau\colon L \to \overline{K_v}$.

(ii) Two extensions $v \circ \tau$ and $v \circ \tau'$ are equal if and only if τ and τ' are **conjugate** *over K_v, i.e., there exists a $\sigma \in \mathrm{Gal}(\overline{K_v}|K_v)$ such that $\tau' = \sigma \circ \tau$.*

Those who prefer to be given an extension $L|K$ by an algebraic equation $f(X) = 0$ will appreciate the following **concrete variant of the above extension theorem**.

Let $L = K(\alpha)$ be generated by the zero α of an irreducible polynomial $f(X) \in K[X]$ and let

$$f(X) = f_1(X)^{m_1} \cdots f_r(X)^{m_r}$$

be the decomposition of $f(X)$ over the completion K_v. The K-embeddings $\tau\colon L \to \overline{K_v}$ are then given by the zeroes β of $f(X)$ which lie in $\overline{K_v}$:

$$\tau\colon L \longrightarrow \overline{K_v}, \quad \tau(\alpha) = \beta.$$

Two embeddings τ and τ' are conjugate over K_v if and only if the zeroes $\tau(\alpha)$ and $\tau'(\alpha)$ are conjugate over K_v, i.e., if they are zeroes of the same irreducible factor f_i.

(8.2) Proposition *Suppose the extension $L|K$ is generated by the zero α of the irreducible polynomial $f(X) \in K[X]$. Then the valuations $w_1, \cdots, w_r$ extending v to L correspond 1-1 to the irreducible factors $f_l, \cdots, f_r$ in the decomposition*

$$f(X) = f_1(X)^{m_1} \cdots f_r(X)^{m_r}$$

of f over the completion K_v.

The extended valuation w_i is explicitly obtained from the factor f_i as follows: let $\alpha_i \in \overline{K_v}$ be a zero of f_i and let

$$\tau_i\colon L \longrightarrow \overline{K_v}, \quad \alpha \longmapsto \alpha_i,$$

be the corresponding K-embedding of L into $\overline{K_v}$. Then one has

$$w_i = \bar{v} \circ \tau_i.$$

τ_i extends to an isomorphism

$$\tau_i\colon L_w \xrightarrow{\sim} K_v(\alpha_i)$$

on the completion L_{w_i} of L with respect to w_i.

Let $L|K$ be again an arbitrary finite extension. We will write $w|v$ to indicate that w is an extension of the valuation v of K to L. The inclusions $L \hookrightarrow L_w$ induce homomorphisms $L \otimes_K K_v \to L_w$, via $a \otimes b \mapsto ab$, and hence a canonical homomorphism

$$\varphi \colon L \otimes_K K_v \longrightarrow \prod_{w|v} L_w .$$

(8.3) Proposition *If $L|K$ is separable, then $L \otimes_K K_v \cong \prod_{w|v} L_w$.*

(8.4) Corollary *If $L|K$ is separable, then one has*

$$[L:K] = \sum_{w|v} [L_w : K_v]$$

and

$$N_{L|K}(\alpha) = \prod_{w|v} N_{L_w|K_v}(\alpha), \quad \mathrm{Tr}_{L|K}(\alpha) = \sum_{w|v} \mathrm{Tr}_{L_w|K_v}(\alpha).$$

If v is a nonarchimedean valuation, then we define, as in the henselian case, the ***ramification index*** of an extension $w|v$ by

$$e_w = (w(L^*) : v(K^*))$$

and the ***inertia degree*** by

$$f_w = [\lambda_w : \kappa],$$

where λ_w, resp. κ, is the residue class field of w, resp. v.

(8.5) Fundamental identity of valuation theory *If v is discrete and $L|K$ separable, then*

$$\sum_{w|v} e_w f_w = [L:K].$$

If K is the field of fractions of a Dedekind domain $\mathcal{O}$, then to every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ is associated the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ of K. The valuation ring of $v_\mathfrak{p}$ is the localization $\mathcal{O}_\mathfrak{p}$. If $\mathcal{O}$ is the integral closure of $\mathcal{O}$ in L and if

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

is the prime decomposition of $\mathfrak{p}$ in L, then the valuation $w_i = \frac{1}{e_i} v_{\mathfrak{P}_i}, i = 1, \cdots, r$ are precisely the extensions of $v = v_\mathfrak{p}$ to L, e_i are the corresponding ramification indices and $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{O}/\mathfrak{p}]$ the inertia degrees.

Let us also emphasize once more that completions may always be replaced with henselizations.

II Exercises

1 **Up to equivalence, the valuations of the field $\mathbb{Q}(\sqrt{5})$ are given as follows.**

1) $|a{+}b\sqrt{5}|_1 = |a{+}b\sqrt{5}|$ **and** $|a{+}b\sqrt{5}|_2 = |a{-}b\sqrt{5}|$ **are the archimedean valuations.**

2) **If** $p = 2$ **or** 5 **or a prime number** $\neq 2, 5$ **such that** $\left(\frac{p}{5}\right) = -1$**, then there is exactly one extension of** $|\ |_p$ **to** $\mathbb{Q}(\sqrt{5})$**, namely**

$$|a + b\sqrt{5}|_{\mathfrak{p}} = |a^2 - 5b^2|_p^{1/2}.$$

3) **If** p **is a prime number** $\neq 2, 5$ **such that** $\left(\frac{p}{5}\right) = 1$**, then there are two extensions of** $|\ |_p$ **to** $\mathbb{Q}(\sqrt{5})$**, namely**

$$|a + b\sqrt{5}|_{\mathfrak{p}_1} = |a + b\gamma|_p, \quad |a + b\sqrt{5}|_{\mathfrak{p}_2} = |a - b\gamma|_p,$$

where γ **is a solution of** $x^2 - 5 = 0$ **in** $\mathbb{Q}_p$**.**

2 **Determine the valuations of the field** $\mathbb{Q}(i)$ **of the Gaussian numbers.**

Proof: $|a + bi|_1 = |a + bi|$, $|a + bi|_2 = |a - bi|$. □

3 **How many extensions to** $\mathbb{Q}(\sqrt[n]{2})$ **does the archimedean absolute value** $|\ |$ **of** $\mathbb{Q}$ **admit?**

4 **Let** $L|K$ **be a finite separable extension,** $\mathcal{O}$ **the valuation ring of a discrete valuation** v **and** $\mathcal{O}$ **its integral closure in** L**. If** $w|v$ **varies over the extensions of** v **to** L **and** $\widehat{\mathcal{O}}_v$**, resp.** $\widehat{\mathcal{O}}_w$**, are the valuation rings of the completions** K_v**, resp.** L_w**, then one has**

$$\mathcal{O} \otimes_{\mathcal{O}} \widehat{\mathcal{O}}_v = \prod_{w|v} \widehat{\mathcal{O}}_w.$$

5 **How does Proposition (8.2) relate to Dedekind's proposition, chap. I, (8.3)?**

6 Let $L|K$ be a finite field extension, v a nonarchimedean exponential valuation, and w an extension to L. If $\mathcal{O}$ is the integral closure of the valuation ring $\mathcal{o}$ of v in L, then the localization $\mathcal{O}_{\mathfrak{P}}$ of $\mathcal{O}$ at the prime ideal $\mathfrak{P} = \{\alpha \in \mathcal{O} | w(\alpha) > 0\}$ is the valuation ring of w.

Proof: First, it is obvious that $\mathcal{O}$ is contained in the valuation ring of w. Since $\mathcal{O}_{\mathfrak{P}} = \{\alpha \in L | \exists s \in \mathcal{O} \setminus \mathfrak{P} \text{ s.t. } s\alpha \in \mathcal{O}\}$. It suffices to show that $\exists s \in \mathcal{O} \setminus \mathfrak{P}$ s.t. $s\alpha \in \mathcal{O}$ if and only if $w(\alpha) \geqslant 0$. The "only if" is obvious. For any $\alpha \in L$ satisfying $w(\alpha) \geqslant 0$, there exists some $s \in \mathcal{O}$ such that $s\alpha \in \mathcal{O}$. If $w(s) = 0$, we are done. Otherwise, write s as $s = s'\pi^r$ with $w(s') = 0$ and π a prime element of w lying in $\mathcal{O}$. Note that s' must belong to $\mathcal{O}$. Since $w(s\alpha) > w(\alpha)$, we can write $s\alpha = \beta\pi^l$ with $s(\beta) = 0$ and $l > r$. Therefor, $s'\alpha = \beta\pi^{l-r} \in \mathcal{O}$ with $s' \in \mathcal{O} \setminus \mathfrak{P}$ as desired. □

§ 9 Galois Theory of Valuations

I Review

Let $L|K$ be a Galois extension with Galois group $G = \mathrm{Gal}(L|K)$. If v is an valuation of K and w an extension to L, then, for every $\sigma \in G$, $w \circ \sigma$ also extends v, so that the group G acts on the set of extensions $w|v$.

(9.1) Proposition *The group G acts transitively on the set of extensions $w|v$, i.e., every two extensions are conjugate.*

(9.2) Definition The ***decomposition group*** of an extension w of v to L is defined by

$$G_w = G_w(L|K) = \{\sigma \in \mathrm{Gal}(L|K) | w \circ \sigma = w\}\,.$$

If v is a nonarchimedean valuation, then the decomposition group contains two further canonical subgroups

$$G_w \supset I_w \supset R_w.$$

Let $\mathcal{o}$, resp. $\mathcal{O}$, be the valuation ring, $\mathfrak{p}$, resp. $\mathfrak{P}$, the maximal ideal, and let κ, resp. λ, be the residue class field of v, resp. w.

(9.3) Definition The ***inertia group*** of $w|v$ is defined by

$$I_w = I_w(L|K) = \{\sigma \in G_w | \sigma x \equiv x \bmod \mathfrak{P}, \quad \forall x \in \mathcal{O}\}\,,$$

and the ***ramification group*** by

$$R_w = R_w(L|K) = \left\{\sigma \in G_w \middle| \frac{\sigma x}{x} \equiv 1 \bmod \mathfrak{P}, \quad \forall x \in L^*\right\}.$$

Observe in this definition that, for $\sigma \in G_w$, the identity $w \circ \sigma = w$ implies that one always has $\sigma\mathcal{O} = \mathcal{O}$ and $\sigma x / x \in \mathcal{O}$, for all $x \in L^*$.

Functorial properties of the groups G_w, I_w, R_w. Consider two Galois extensions $L|K$ and $L'|K'$ and a commutative diagram

$$\begin{tikzcd} L \arrow[r, "\tau"] & L' \\ K \arrow[u] \arrow[r, "\tau"] & K' \arrow[u] \end{tikzcd}$$

with homomorphisms τ which will typically be inclusions. They induce a homomorphism

$$\tau^* \colon \mathrm{Gal}(L'|K') \longrightarrow \mathrm{Gal}(L|K), \quad \tau^*(\sigma') = \tau^{-1} \circ \sigma \circ \tau.$$

Observe here that, $L|K$ being normal, the same is true of $\tau L|\tau K$, and thus one has $\sigma'\tau L \subset \tau L$, so that composing with τ^{-1} makes sense.

Now let w' be a valuation of L', $v' = w'|_{K'}$ and $w = w' \circ \tau$, $v = w|_K$. Then we have the

(9.4) Proposition $\tau^*\colon \operatorname{Gal}(L'|K') \to \operatorname{Gal}(L|K)$ *induces homomorphisms*

$$\begin{aligned} G_{w'}(L'|K') &\longrightarrow G_w(L|K),\\ I_{w'}(L'|K') &\longrightarrow I_w(L|K),\\ R_{w'}(L'|K') &\longrightarrow R_w(L|K). \end{aligned}$$

In the latter two cases, v is assumed to be nonarchimedean.

Special case I: $K = K', L = L'$, one has

$$G_{w\circ\tau} = \tau^{-1}G_w\tau, \quad I_{w\circ\tau} = \tau^{-1}I_w\tau, \quad R_{w\circ\tau} = \tau^{-1}R_w\tau,$$

i.e., the decomposition, inertia, and ramification groups of conjugate valuations are conjugate.

Special case II: M is an intermediate field of $L|K$, then from the diagram

$$\begin{tikzcd} L \arrow[r, equal] & L \\ K \arrow[u] \arrow[r, hook] & M \arrow[u] \end{tikzcd}$$

τ^* becomes the inclusion $\operatorname{Gal}(L|M) \hookrightarrow \operatorname{Gal}(L|K)$, and we trivially get the

(9.5) Proposition *For the extensions $K \subset M \subset L$, one has*

$$\begin{aligned} G_w(L|M) &= G_w(L|K) \cap \operatorname{Gal}(L|M),\\ I_w(L|M) &= I_w(L|K) \cap \operatorname{Gal}(L|M),\\ R_w(L|M) &= R_w(L|K) \cap \operatorname{Gal}(L|M). \end{aligned}$$

Special case III: Let $w|v$ be an extension of valuations of $L|K$.

$$\begin{tikzcd} & L_w \\ L \arrow[ur, dash] \arrow[dd, dash] & \\ & K_v \arrow[uu, dash] \\ K \arrow[ur, dash] & \end{tikzcd}$$

Since in the local extension $L_w|K_v$ the extension of the valuation is unique, we denote the decomposition, inertia, and ramification groups simply by $G(L_W|K_v), I(L_w|K_v), R(L_w|K_v)$. In this case, the homomorphism τ^* is the restriction map

$$\operatorname{Gal}(L_w|K_v) \longrightarrow \operatorname{Gal}(L|K), \quad \sigma \mapsto \sigma|_L\,,$$

and we have the

(9.6) Proposition

$$\begin{aligned} G_w(L|K) &\cong G(L_w|K_v), \\ I_w(L|K) &\cong I(L_w|K_v), \\ R_w(L|K) &\cong R(L_w|K_v). \end{aligned}$$

The above proposition reduces the problems concerning a single valuation of K to the local situation. We identify the decomposition group $G_w(L|K)$ with the Galois group of $L_w|K_v$ and write

$$G_w(L|K) = G(L_w|K_v),$$

and similarly $I_w(L|K) = I(L_w|K_v)$ and $R_w(L|K) = R(L_w|K_v)$.

We now explain the concrete meaning of the subgroups G_w, I_w, R_w of $G = \mathrm{Gal}(L|K)$ for the field extension $L|K$.

The decomposition group G_w consists of all automorphisms $\sigma \in G$ that are continuous with respect to the valuation w. Denoting by $G_w \backslash G$ the set of all right cosets $G_w\sigma$, by W_v the set of extensions of v to L and choosing a fixed extension w, we obtain a bijection

$$G_w \backslash G \xrightarrow{\sim} W_v, \quad G_w\sigma \mapsto w\sigma.$$

(9.7) Definition The fixed field of G_w,

$$Z_w = Z_w(L|K) = \{x \in L | \sigma x = x, \quad \forall \sigma \in G_w\},$$

is called the ***decomposition field*** of w over K.

(9.8) Proposition *(i) The restriction w_Z of w to Z_w extends uniquely to L.*

(ii) If v is nonarchimedean, w_Z has the same residue class field and the same value group as v.

(iii) $Z_w = L \cap K_v$ (the intersection is taken inside L_w).

The inertia group I_w. Let $\mathcal{O}$ be the valuation ring of w and $\mathfrak{P}$ the maximal ideal, then, since $\sigma\mathcal{O} = \mathcal{O}$ and $\sigma\mathfrak{P} = \mathfrak{P}$, every $\sigma \in G_w$ induces a κ-automorphism

$$\bar{\sigma} \colon \mathcal{O}/\mathfrak{P} \longrightarrow \mathcal{O}/\mathfrak{P}, \quad x \bmod \mathfrak{P} \mapsto \sigma x \bmod \mathfrak{P},$$

of the residue class field and we obtain a homomorphism

$$G_w \longrightarrow \mathrm{Aut}_\kappa(\lambda)$$

with kernel I_w.

(9.9) Proposition *The residue class field extension $\lambda|\kappa$ is normal, and we have an exact sequence*

$$1 \longrightarrow I_w \longrightarrow G_w \longrightarrow \mathrm{Gal}(\lambda|\kappa) \longrightarrow 1.$$

(9.10) Definition The fixed field of I_w,

$$T_w = T_w(L|K) = \{x \in L | \sigma x = x, \quad \forall \sigma \in I_w\},$$

is called the ***inertia field*** of w over K.

For the inertia field, (9.9) gives us the isomorphism

$$\mathrm{Gal}(T_w|Z_w) \cong \mathrm{Gal}(\lambda|\kappa).$$

It has the following significance for the extension $L|K$.

(9.11) Proposition *$T_w|Z_w$ is the maximal unramified subextension of $L|Z_w$.*

If in particular K is a henselian field and $\overline{K}_s|K$ its separable closure, then the inertia field of this extension is the maximal unramified extension $T|K$ and has the separable closure $\overline{\kappa}_s|\kappa$ as its residue class field. The isomorphism

$$\mathrm{Gal}(T|K) \cong \mathrm{Gal}(\overline{\kappa}_s|\kappa)$$

shows that the unramified extensions of K correspond 1-1 to the separable extensions of κ.

The ramification group R_w is the kernel of the canonical homomorphism

$$I_w \longrightarrow \chi(L|K),$$

where

$$\chi(L|K) = \mathrm{Hom}(\Delta/\Gamma, \lambda^*),$$

where $\Delta = w(L^*)$, and $\Gamma = v(K^*)$. For $\sigma \in I_w$, then the associated homomorphism

$$\chi_\sigma \colon \Delta/\Gamma \longrightarrow \lambda^*$$

is given as follows: For any $\bar{\delta} \in \Delta/\Gamma$, choose a representation δ and an $x \in L^*$ such that $w(x) = \delta$. Put

$$\chi_\sigma(\bar{\delta}) = \frac{\sigma x}{x} \bmod \mathfrak{P}.$$

One sees immediately that mapping $\sigma \mapsto \chi_\sigma$ is a homomorphism $I_w \to \chi(L|K)$ with kernel R_w.

(9.12) Proposition *R_w is the unique p-Sylow subgroup of I_w.*

(9.13) Definition The fixed field of R_w,

$$V_w = V_w(L|K) = \{x \in L | \sigma x = x, \quad \forall \sigma \in R_w\},$$

is called the ***ramification field*** of w over K.

(9.14) Proposition *$V_w|Z_w$ is the maximal tamely ramified subextension of $L|Z_w$.*

(9.15) Corollary *We have the exact sequence*

$$1 \longrightarrow R_w \longrightarrow I_w \longrightarrow \chi(L|K) \longrightarrow 1.$$

II Exercises

1 Let K be a henselian field, $L|K$ a tamely ramified Galois extension, $G = G(L|K)$, $I = I(L|K)$ and $\Gamma = G/I = G(\lambda|\kappa)$. Then I is abelian and becomes a Γ-module by letting $\bar{\sigma} = \sigma I \in \Gamma$ operate on I via $\tau \mapsto \sigma\tau\sigma^{-1}$.

Show that there is a canonical isomorphism $I \cong \chi(L|K)$ of Γ-modules. Show furthermore that every tamely ramified extension can be embedded into a tamely ramified extension $L|K$, such that G is the semi-direct product of $\chi(L|K)$ with $G(\lambda|\kappa)$:

$$G \cong \chi(L|K) \rtimes G(\lambda|\kappa).$$

2 The maximal tamely ramified abelian extension V of $\mathbb{Q}_P$ is finite over the maximal unramified abelian extension T of $\mathbb{Q}_p$.

3 Show that the maximal unramified extension of the power series field $K = \mathbb{F}_p((t))$ is given by $T = \overline{\mathbb{F}_p}((t))$, where $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_p$, and the maximal tamely ramified extension by $T(\{t^{1/m} | m \in \mathbb{N}, (m,p) = 1\})$.

4 Let v be a nonarchimedean valuation of the field K and let $\bar{v}$ be an extension to the separable closure $\overline{K}_s$ of K. Then the decomposition field $Z_{\bar{v}}$ of $\bar{v}$ over K is isomorphic to the henselization of K with respect to v, in the sense of §6.

Index

Bibliography

Algebra

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[AM94] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Series in Mathematics, Westview Press, 1994.

Algebraic Geometry

[Milne] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

Analysis

[BGR84] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 261, Springer-Verlag, Berlin, 1984. A systematic approach to rigid analytic geometry. MR746961 (86b:32031)

Number Theory

[Weil] André Weil, *Basic number theory*, 3rd ed., Springer-Verlag, New York-Berlin, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Rob00] Alain M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000.