Math 525: Algebraic Number Theory

Last edited January 29, 2023

February 23

These are the course notes for Math 525: Algebraic Number Theory course given in Boğaziçi University in Spring '22 by Alp Bassa.

0 Introduction

The textbook for the course is P. M. Cohn, Algebraic Numbers and Algebraic Functions. This book is the elementary version of E. Artin, Algebraic Numbers and Algebraic Functions. A further aim might be to read the harder version after (or during) this course.

Algebraic Numbers (Number Fields)

Number fields are the finite extensions of the rational field $\mathbb{Q}$. Questions about the arithmetic of the integers are answered by considering the number fields and their ring of integers.

Question. *Which primes can be written as a sum of two squares?*

We see that

$$2 = 1^2 + 1^2,\ 5 = 2^2 + 1^2,\ 13 = 2^2 + 3^2,$$

and that 3, 7, and 11 cannot be written as a sum of two squares. So we guess that a prime number p is a sum of two squares if and only if $p = 2$ or $p \equiv 1 \mod 4$.

It is easy to see that if $p \neq 2$ and $p \not\equiv 1 \mod 4$, then p cannot be written as a sum of two squares because only other option for p modulo 4 is $p \equiv 3 \mod 4$, yet only squares modulo 4 are 0 and 1, so 3 is not a sum of two squares modulo 4.

On the other hand, if $p = x^2 + y^2$ for two integers x and y, in the field of complex numbers this factors as $p = (x+iy)(x-iy)$, or more precisely, in the field $\mathbb{Q}(i)$, or even more precisely, in its ring of integers $\mathbb{Z}[i]$ which is called the *ring of Gaussian integers*.

There is an interesting relation between the prime ideals of $\mathbb{Z}$ and the prime ideals of $\mathbb{Z}[i]$. As $\mathbb{Z}$ is a principal ideal domain, we can associate its prime ideals with its prime elements. Under this view, an integer prime either stays a prime in $\mathbb{Z}[i]$ or it "splits" into two Gaussian primes as given in the following figure.

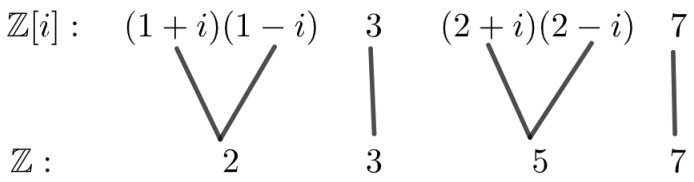


Figure 1: Primes of $\mathbb{Z}$ split as primes of $\mathbb{Z}[i]$.

Notice that 2 splits into two primes that are associates, so they generate the same ideal in $\mathbb{Z}[i]$. This is called a *ramification*.

But all these assume $\mathbb{Z}[i]$ is *nice*. That it has these so-called primes and factorization but what does factorization in $\mathbb{Z}[i]$ even mean? Does it make sense to talk about primes of $\mathbb{Z}[i]$? Is every element of $\mathbb{Z}[i]$ a product of primes? Is such a factorization unique?

Proposition 0.1. *The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain.*

Proof. A Euclidean norm $N\colon \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ on $\mathbb{Z}[i]$ is defined as the restriction of the complex norm to $\mathbb{Z}[i]$. □

Proposition 0.2. *Every Euclidean domain is a unique factorization domain (UFD).*

We notice that the units of $\mathbb{Z}[i]$ can be classified as those elements $z = z_1 + z_2 i \in \mathbb{Z}[i]$ with norm $N(z) = 1$. Indeed, if z is a Gaussian unit, $N(z)$ is a positive integer unit, i.e. 1 because in such a case $N(z)N(z^{-1}) = 1$ since the norm is multiplicative. On the other hand, if $N(z) = 1$, then $z_1^2 + z_2^2 = (z_1 + z_2 i)(z_1 - z_2 i) = 1$, yielding an inverse to z.

The norm of an integer p is $N(p) = p^2$. So if $p \in \mathbb{Z}[i]$ is reducible, say $p = \alpha\beta$ with α and β non-unit Gaussian integers, as the norm is multiplicative, both $N(\alpha)$ and $N(\beta)$ must be p.

It remains to prove the following proposition.

Proposition 0.3. *If $p \equiv 1 \mod 4$ is a prime in $\mathbb{Z}$, then $p = \alpha\beta$ for α and β non-unit Gaussian integers.*

Proof. When $p \equiv 1 \mod 4$ the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/(p-1)\mathbb{Z}$ of the field $\mathbb{Z}/p\mathbb{Z}$ of p elements is a cyclic group of order divisible by 4. Let a be a generator of $\mathbb{Z}/(p-1)\mathbb{Z}$. Then $x = a^{\frac{p-1}{4}}$ satisfies $x^2 + 1 \equiv 0 \mod p$.[1] Now p must divide $x^2 + 1$. If p were to stay a prime in $\mathbb{Z}[i]$, then it would divide at least one of $x + i$ or $x - i$, implying but neither $\frac{x}{p} + \frac{i}{p}$ nor $\frac{x}{p} - \frac{i}{p}$ is a Gaussian integer. Hence $p \in \mathbb{Z}[i]$ is not a prime anymore. Since $\mathbb{Z}[i]$ is a UFD, failing to be prime means failing to be irreducible. □

Algebraic Functions

Take $p(x, y) \in \mathbb{R}[x, y]$ to be $p(x, y) = y^2 - (x^3 - x)$. The zero locus of p above the real line gives the following picture:

[1] Alternatively, one can use Wilson's theorem that says $(p-1)! \equiv -1 \mod p$ for a prime $p \in \mathbb{Z}$ and take $x = ((p-1)/2)!$.

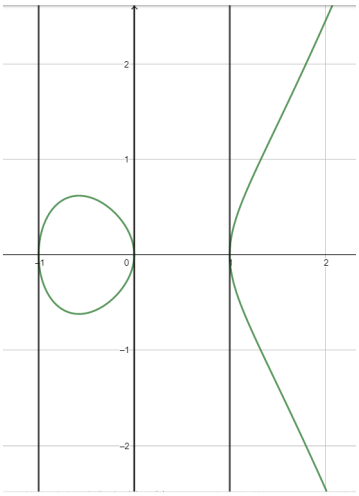


Figure 2: Real points of the elliptic curve $E : y^2 = x^3 - x$.

February 28

1 Fields with Valuations

1.1 Absolute Values

Given a nontrivial (commutative) ring R (with unity), an absolute value on R is a function $|\cdot| : R \to \mathbb{R}$ with

A1: $|x|$ is nonnegative for all $x \in R$ and zero if and only if $x = 0$.

A2: **Triangle inequality.** $|x + y| \leq |x| + |y|$ for all $x, y \in R$.

A3: $|xy| = |x||y|$ for all $x, y \in R$.

Some immediate consequences of the definition are as follows:

Proposition 1.1.

- $|1| = 1$.
- $|-1| = 1$.

- $|-x| = |x|$.
- $|\cdot|x| - |y|\cdot| \leq |x-y|$
- $|x_1 + \cdots + x_n| \leq |x_1| + \cdots + |x_n|$.

Proof.
- $|1| = |1 \cdot 1| = |1| \cdot |1|$, hence $|1| = 1$
- Let $|-1| = a > 0$. Then $|-1| \cdot |-1| = a^2 = |1| = 1$, hence $a = 1$.
- $|-x| = |-1| \cdot |x| = |x|$ by above.
- Note that

$$|x - y + y| \leq |x - y| + |y| \implies |x| - |y| \leq |x - y|$$
$$|y - x + x| \leq |x - y| + |x| \implies -|x - y| \leq |x| - |y|$$

  The result follows from these two.

- Proof is by induction. Base case $n = 1$ is trivial, suppose the result holds for $n = k$. Then $|x_1 + \ldots x_k| \leq |x_1| + \ldots + |x_k|$. So we have that $|x_1 + \ldots x_k| + |x_{k+1}| \leq |x_1| + \ldots + |x_k| + |x_{k+1}|$.

□

Proposition 1.2. *If there is an absolute value on a commutative ring R with unity, it is necessarily an integral domain.*

Proof. Let $a, b \in R$ such that $|a|, |b| \neq 0$. Then $|ab| = |a| \cdot |b| \neq 0$ by A3, thus $ab \neq 0$ by A1. □

Example 1.1. For any integral domain R, the trivial absolute value $|\cdot|: R \to R$ is defined as $|x| = 0$ if $x = 0$ and $|x| = 1$ if $x \neq 0$ for any element $x \in R$.

Example 1.2. The usual absolute value on $\mathbb{R}$ or $\mathbb{C}$.

Example 1.3. Let $p \in \mathbb{Z}$ be a prime number. Every rational number $r \in \mathbb{Q}$ can be written as $r = p^k \frac{a_0}{b_0}$ where $p \nmid a_0, b_0$. The p-adic absolute value $|\cdot|_p: \mathbb{Q} \to \mathbb{Q}$ on such an r is defined as $|r|_p = p^{-k}$.

The intuition here is that the rationals whose nominator has lots of p factor in it are "small". This explains the intiution behind defining $|0|_p = 0$.

Example 1.4. Let K be a field and

$$K(x) = \{\frac{f(x)}{g(x)} \colon f(x) \in K[x], g(x) \in K[x]^\times$$

be its ring of rational functions. Given an irreducible element $p(x) \in R$, elements of $K(x)$ can be written as

$$\frac{f(x)}{g(x)} = p(x)^k \frac{f_0(x)}{g_0(x)}$$

where $p(x) \nmid f_0(x), g_0(x)$. We define the absolute value $|\cdot|_{p(x)} \colon R \to R$ on such a rational function as $|\frac{f(x)}{g(x)}|_{p(x)} = 2^{-k}$[2], and we set $|0|_{p(x)} := 0$.

The next proposition is part an example, part a proposition.

Proposition 1.3. *The only absolute value on $\mathbb{F}_q$ is the trivial absolute value.*

Proof. Let x be a non-zero element in $\mathbb{F}_q$. Then $|x^{q-1}| = |1| = 1 = |x|^{q-1}$ by A3. Then by A1, $|x| = 1$. □

A2': **Ultrametric inequality.** $|x + y| \leq max\{|x|, |y|\}$

An absolute value satisfying A2' is called a non-archimedean absolute value.

Proposition 1.4 (Strict triangle inequality)**.** *For a non-archimedean absolute value, if $|x| \neq |y|$ then $|x + y| = max\{|x|, |y|\}$.*

Proof. Without loss of generality say $|x| > |y|$. Assume $|x+y| \neq \max\{|x|, |y|\}$ so $|x+y| < \max\{|x|, |y|\} = |x|$. But $|x| = |x+y-y| \leq \max\{|x+y|, |y|\} < |x|$, contradiction. □

Using the strict triangle inequality, we can infer that every triangle in nonarchimedean geometry is isosceles. Indeed, if the three corners of the triangle

[2]Actually, any real number greater than 1 works. (Does it?)

are x, y, z, then $|x-z| = |x-y+y-z| = \max\{|x-y|, |y-z|\}$ and either $|x-y| = |y-z|$ or $|x-y|$ equals of $|x-y|$ or $|y-z|$.

A good example is the ring $K((x))$ of formal Laurent series over a field K. An absolute value on $K((x))$ maps $\sum_{n=N}^{\infty} a_n x^n$ to 2^{-N}. For $N \neq M$, two elements $f(x) = \sum_{n=N}^{\infty} a_n x^n$ and $g(x) = \sum_{n=M}^{\infty} b_n x^n$ with absolute values 2^{-N} and 2^{-M}, respectively, have the absolute value $2^{\min\{-N,-M\}}$ when added. A similar account holds for the ring of integers when they are viewed as base p numbers. For example $11 = 23^0 + 03^1 + 13^2$ and $6 = 23^1$ have absolute values 2^0 and 2^1, respectively, and their sum $17 = 23^0 + 23^1 + 13^2$ has the absolute value $2^0 = \min\{2^0, 2^1\}$.

Proposition 1.5. *Let R be a commutative ring with an absolute value $|\cdot|_R$. Then the absolute value can be extended uniquely to an absolute value on the field of fractions F of R.*

Proof. By Proposition 1.2, R must be an integral domain. Let F be its field of fractions; any $r \in F$ has the form $r = \frac{a}{b}$, where $a, b \in R$ with $b \neq 0$. If there is such an extension of $|.|_R$ in R to $|.|_F$ in F since $rb = a$ by A3 we must have $|a|_F = |b|_F |r|_F$ as $a, b \in R$ these absolute values must coincide which means $|a|_F = |a|_R$ and $|b|_F = |b|_R$. Therefore if such an extension exists it must be this way $|r|_F = \frac{|a|_R}{|b|_R}$. This shows that there is at most one extension. To show that it really exists we must prove that it is well defined and it satisfies the axioms of being an absolute value. Now let $r = \frac{a}{b} = \frac{a'}{b'}$, hence $ab' = ba'$ using the multiplicativity of $|.|_R$ we get $|a| \cdot |b'| = |b| \cdot |a'|$ so $\frac{|a|_R}{|b|_R} = \frac{|a'|_R}{|b'|_R}$. This shows that $|.|_F$ is well defined on F. The verification of A1-A3 is straightforward. □

Proposition 1.6. *For a commutative ring R, an absolute value $|\cdot| \colon R \to \mathbb{R}$ on R is non-archimedean if and only if $|m \cdot 1_R| \leq 1$ for all $m \in \mathbb{Z}$, i.e. the set $\{|m \cdot 1_R| \colon m \in \mathbb{Z}\} \in [0, 1]$ is bounded.*

Proof. If R is non-archimedean, then the result is trivial if we use complete (or strong) induction. For the reverse direction we have

$$|x+y|^n = \Big|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\Big| \leq \sum_{i=0}^{n} \Big|\binom{n}{i} \cdot 1_R\Big| |x|^i |y|^{n-i} \leq (n+1) \max\{|x|, |y|\}^n.$$

Taking the n'th root of the above equation and letting n to infinity gives the result. □

Corollary 1.7. *Any absolute value on a field of positive characteristic is non-archimedean.*

Proof. When the field is finite,It is immediate from Proposition 1.3.

Assume that F is an infinite field of positive characteristic p.In particular,we have $p.1_F = 0_F$.Let $k \in \mathbb{N}$,then using divison Algorithm,there exists $q, r \in \mathbb{N}$ such that $k = pq + r$.Thus,we have that $|r.1_F| = |k.1_F|$. and $|k.1_F| \leq |1_F| + ... + |1_F|$,so the image of F restricted to $\mathbb{Z}$ is bounded which shows that $|.|_F$ is non-Archimedean. □

1.1.1 Topology defined by an absolute value

Once we have an absolute value on a field K, we can define a metric $d\colon K \times K \to \mathbb{R}$ with

M1: $d(x, y) \geq 0$ for all $x, y \in K$ and $d(x, y) = 0$ if and only if $x = y$.

M2: $d(x, y) = d(y, x)$ for all $x, y \in K$.

M3: $d(x, z) \leq d(x, y) + d(y, z) \forall x, y, z \in K$.

M4: **Translational invariance.** $d(x + a, y + a) = d(x, y)$ for all $a \in K$.

M5: $d(a \cdot x, a \cdot y) = |a| d(x, y)$ for all $a \in K$.

Note that we can always recover the original absolute value as $|x| = d(x, 0)$.

Endowed with this metric, we can talk about open (resp. closed) sets or balls on K and continuity.

Proposition 1.8. *Field operations are continuous.*

Proof. We need to show that changing $x \in K$ to some $a \in K$ while changing $y \in K$ to $b \in K$, we get results comparable to the size of the change. For example, in the case of addition, we see that

$$\begin{aligned} d(x+y, a+b) &= |(x+y) - (a+b)| \\ &= |(x-a) + (y-b)| \\ &\leq |x-a| + |y-b| \\ &= d(x,a) + d(y,b). \end{aligned}$$

Similarly, for multiplication we get

$$\begin{aligned} d(xy, ab) &= |xy - ab| \\ &= |(y-b)a + (x-a)b + (x-a)(y-b)| \\ &\leq d(y,b)|a| + d(x,a)|b| + d(x,a)d(y,b). \end{aligned}$$

Also, for inversion one has

$$\begin{aligned} d(x^{-1}, a^{-1}) &= |x^{-1} - a^{-1}| \\ &= \left| \frac{1}{x} - \frac{1}{a} \right| \\ &= \left| \frac{a-x}{xa} \right| \\ &= \left| \frac{a-x}{|x| \cdot |a|} \right| \\ &= \frac{d(a,x)}{|x||a|} \end{aligned}$$

□

This shows that there is a correspondence between the absolute values on K and the topologies on K. For example, in the case of the trivial absolute value, every singleton is open because the ball of radius $1/2$ centered at a point contains only that point; hence, the trivial absolute value corresponds to the discrete topology.

In light of this observation, we say that two absolute values on K are *equivalent* if they define the same topology on K. The next proposition gives us more ways to realize such a relation.

Proposition 1.9. *The following are equivalent for two non-trivial absolute values $|\cdot|_1$ and $|\cdot|_2$ on K*

(i) $|\cdot|_1$ *and* $|\cdot|_2$ *are equivalent.*

(ii) $B(0,1,|\cdot|_1) \subset B(0,1,|\cdot|_2)$.

(iii) For each $x \in K$, *if* $|x|_1 < 1$ *then* $|x|_2 < 1$.

(iv) For each $x \in K$, *if* $|x|_1 > 1$ *then* $|x|_2 > 1$.

(v) There is some nonnegative real number $\gamma \in \mathbb{R}$ *such that* $|x|_1 = |x|_2^\gamma$ *for every* $x \in K$.

Proof. □

March 2

Lemma 1.10. *For an absolute value* $||: K \to \mathbb{R}$ *on a field* K,

$$\lim_{n\to\infty} \left|\frac{a^n}{1+a^n}\right| = \begin{cases} 0 & \text{if } |a| < 1 \\ 1 & \text{if } |a| > 1. \end{cases}$$

Proof. For $|a| < 1$ we have $\left|\dfrac{a^n}{1+a^n}\right| = \dfrac{|a^n|}{|1+a^n|} \leq \dfrac{|a|^n}{||1|-|a|^n|}$ using reverse-triangle inequality. For sufficiently large n, $||1|-|a|^n| > c$ for some positive constant c. Letting $n \to \infty$ shows the assertion. For the case $|a| > 1$, note that $\dfrac{|a^n|}{|1+a^n|} \leq \dfrac{|a|^n}{||1|-|a|^n|}$ and $\dfrac{|a^n|}{|1+a^n|} \geq \dfrac{|a|^n}{1+|a|^n}$. It follows that $1 \leq \lim\limits_{n\to\infty} \dfrac{|a^n|}{|1+a^n|} \leq 1$. □

The next theorem says that two inequivalent absolute values are seriously independent.

Theorem 1.11 (Approximation theorem)**.** *Given a field K, nontrivial pairwise inequivalent absolute values $||_1, \dots, ||_r$ on K, elements $\alpha_1, \dots, \alpha_r \in K$, and $\epsilon \in \mathbb{R}^+$, there is always some $\alpha \in K$ such that*

$$|\alpha - \alpha_1|_1 < \epsilon, \dots, |\alpha - \alpha_r| < \epsilon.$$

Proof. For each $j = 1, 2, \dots, r$ we will find some $u_j \in K$ such that u_j is close to 1 with respect to the absolute value $||_j$ and close to 0 with respect to $||_i$ for all $i \neq j$. Then $\alpha = \alpha_1 u_1 + \cdots + \alpha_r u_r$ will satisfiy

$$|\alpha - \alpha_j| \leq |\alpha_j||u_j - 1| + \sum_{i \neq j} |\alpha_i||u_i|,$$

and we will be able to make it as small as possible.

As the absolute values are pairwise inequivalent, when $r = 2$ we can find some $a, b \in K$ such that $|a|_1 > 1 \geq |a|_2$ and $|b|_2 > 1 \geq |b|_1$ by Proposition 1.9. Then ab^{-1} satisfies $|ab^{-1}|_1 > 1 \geq |ab^{-1}|_2$. For the inductive step we assume there is some $a \in K$ with $|a|_1 > 1 > |a|_2, \dots, |a|_r$ and find some $c \in K$ that keeps these relations and also satisfies $|c|_{r+1} < 1$.

If $|a|_{r+1} < 1$ we are done. On the other hand, when $|a|_{r+1} = 1$, using the argument in the base case we find some $b \in K$ such that $|b|_1 > 1 > |b|_{r+1}$. If ab satisfies all the relations, we are done. Otherwise, for some big enough $n \in \mathbb{N}$, we can take $c = a^n b$. Finally, if $|a|_{r+1} > 1$, again for some $b \in K$ with $|b|_1 > 1 > |b|_{r+1}$, we take $c = \frac{a^n}{1+a^n} b$ making use of Lemma 1.10. □

Corollary 1.12. *Given a field K, nontrivial pairwise inequivalent absolute values $||_1, \dots, ||_r$ on K, elements $\alpha_1, \dots, \alpha_r \in K$, and $\epsilon_1, \dots, \epsilon_r \in \mathbb{R}^+$, there is always some $\alpha \in K$ such that*

$$|\alpha - \alpha_1|_1 < \epsilon_1, \dots, |\alpha - \alpha_r| < \epsilon_r.$$

Proof. Take $\epsilon = \min\{\epsilon_1, \dots, \epsilon_r\}$ and use the approximation theorem. □

1.2 Completions

Given a ring R with an absolute value $||\colon R \to \mathbb{R}$ on it, a sequence $(c_n)_{n\in\mathbb{N}}$ of elements $c_n \in \mathbb{R}$ is said to converge to $c \in \mathbb{R}$ if

$$\lim_{n\to\infty} |c_n - c| = 0,$$

or equivalently, given $\epsilon > 0$ there is some index $N \in \mathbb{N}$ such that $|c_n - c| < \epsilon$ for all $n > N$.

A sequence $(c_n)_{n\in\mathbb{N}}$ is called a Cauchy sequence if for every $\epsilon > 0$ there is some index $N \in \mathbb{N}$ such that $|c_i - c_j| < \epsilon$ for all $i, j > N$.

Looking at the inequality $|c_i - c_j| \leq |c_i - L| + |c_j - L|$ for a sequence $(c_n)_{n\in\mathbb{N}}$ converging to some $L \in \mathbb{R}$, we see that every convergent sequence is Cauchy; but, it is certainly not the case that every Cauchy sequence is convergent in an arbitrary ring R.

For example, when $R = \mathbb{Q}$ the sequence

$$(c_n)_{n\in\mathbb{N}} = (3, 3.1, 3.14, 3.141, 3.1415, \dots)$$

of the prefixes of the irrational number $\pi \in \mathbb{R}$ of increasing length converges to π in the reals, but it merely keeps getting closer and closer to the actual value of π when viewed in the rationals with the limit $\lim_{n\to\infty} c_n$ undefined.

A ring R is said to be complete with respect to some absolute value $||\colon R \to \mathbb{R}$ if every Cauchy sequence in R is convergent with respect to $||$.

Theorem 1.13. *For every ring R with some absolute value $|\cdot|$ on it, there exists a complete absolute valued ring $\widehat{R}$ and an analytic (isometric) embedding $\iota\colon R \hookrightarrow \widehat{R}$ such that*

1. *R is dense in $\widehat{R}$,*
2. *$\widehat{R}$ is complete,*
3. *$\widehat{R}$ is universal, that is, if $f\colon R \hookrightarrow \widehat{S}$ is any analytic embedding of R into a complete ring $\widehat{S}$, then there is a unique embedding $\widehat{f}\colon R \hookrightarrow \widehat{S}$ such that the following diagram commutes:*

4. $\widehat{R}$ is a field if R is a field.

Proof. The set $R^{\mathbb{N}} = \{(c_n)_{n\in\mathbb{N}} \colon c_n \in R \forall n \in \mathbb{N}\}$ of sequences in R forms a ring under componentwise addition and multiplication.

The set C of Cauchy sequences in R forms a subring of $R^{\mathbb{N}}$. Indeed, if $(c_n)_{n\in\mathbb{N}}$ and $(d_n)_{n\in\mathbb{N}}$ are two Cauchy sequences in R, then $(c_n + d_n)_{n\in\mathbb{N}}$ and $(c_n \cdot d_n)_{n\in\mathbb{N}}$ are Cauchy sequences because the addition and the multiplication are continuous with respect to the absolute value $|\cdot|$.

The set I of Cauchy sequences that converge to 0 is an ideal of C, or more generally, of the set of bounded sequences. Let $\widehat{R} = C/I$.[3] We can view an element $r \in R$ as the constant sequence $(r, r, \dots) \in C$. For $s \in R$, if $s \neq r$ then $(r, r, \dots)$ and $(s, s, \dots)$ are in different classes in C/I because $(rs, rs, \dots) \notin I$. Therefore,

$$\begin{aligned} \iota \colon R &\hookrightarrow C/I \\ r &\mapsto \overline{r} + I := (r, r, \dots) + I \end{aligned}$$

is an embedding.

We can extend the absolute value $|\cdot| \colon R \to \mathbb{R}$ to $\widehat{R}$ as

$$\begin{aligned} \iota \colon R &\hookrightarrow C/I \\ (c_n) + I &\mapsto \lim_{n\to\infty} |c_n|. \end{aligned}$$

The limit exists because $(|c_n|)$ is a Cauchy sequence (since $||c_i| - |c_j|| \leq |c_i - c_j|$) in the complete field $\mathbb{R}$. Also, the mapping of classes to reals is well-defined because if $(c_n)_{n\in\mathbb{N}} - (d_n)_{n\in\mathbb{N}} \in I$, then $\lim_{n\to\infty} |c_n| \lim_{n\to\infty} |d_n|$. Now, ι becomes an embedding.

We see that R is dense in $\widehat{R}$ as for $(\alpha_n)_{n\in\mathbb{N}} + I \in \widehat{R}$, $(\alpha - \overline{\alpha_k}) + I$ goes to $\overline{0} + I$ with respect to the extended absolute value on $\widehat{R}$. It follows that for every $\alpha \in \widehat{R}$ there is always some $\alpha' \in C$ such that $\alpha' + I$ is arbitrarily close to $\alpha + I$ with respect to $|\cdot|$, hence $\iota(R) \cong R$ is dense in $\widehat{R}$.

[3]Put another way, we add a point in the limit of each non-convergent $(c_n)_{n\in\mathbb{N}} \in C$; but we do not want to put two different elements in the same spot, so we set $(c_n)_{n\in\mathbb{N}} \sim (d_n)_{n\in\mathbb{N}}$ for $(c_n)_{n\in\mathbb{N}}, (d_n)_{n\in\mathbb{N}} \in C$ if $\lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n$, and mod out by this relation.

Let $(\alpha^{(n)})_{n\in\mathbb{N}}$ be a Cauchy sequence in $\widehat{R}$. Since R is dense in $\widehat{R}$, for each $n \in \mathbb{N}$ there is some $\beta_n \in R$ such that

$$|\alpha^{(n)} - \overline{\beta_n}| < \frac{1}{n}.$$

Let us call $\beta = (\beta_n)_{n\in\mathbb{N}}$. It follows that $(\alpha^{(n)} - \beta)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\widehat{R}$, hence so is $(\alpha^{(n)} - (\alpha^{(n)} - \beta)) = \beta$. Because

$$|\alpha^{(n)} - \beta| \leq |\alpha^{(n)} - \overline{\beta_n}| + |\overline{\beta_n} - \beta|,$$

we see that $\lim_{n\to\infty} |\alpha^{(n)} - \beta| = 0$.

Given an analytic embedding $f\colon R \to \widehat{S}$ of R into a complete ring $\widehat{S}$, define

$$\begin{aligned} \widehat{f}\colon \widehat{R} &\to \widehat{S} \\ (\alpha_n)_{n\in\mathbb{N}} &\mapsto \lim_{n\to\infty} (f(\alpha)n)_{n\in\mathbb{N}}. \end{aligned}$$

For two representatives $(\alpha'_n)_{n\in\mathbb{N}} + I = (\alpha_n)_{n\in\mathbb{N}} + I$ of the same class,

$$\begin{aligned} \lim_{n\to\infty} |f(\alpha_n) - f(\alpha'_n)| &= \lim_{n\to\infty} |f(\alpha_n - \alpha'_n)| \\ &= \lim_{n\to\infty} |\alpha_n - \alpha'_n| \\ &= 0. \end{aligned}$$

So $\widehat{f}$ is well-defined, and

$$\widehat{f}(\iota(r)) = \widehat{f}(\overline{r} + I) = \lim_{n\to\infty} f(r) = f(r).$$

As $|(\alpha_n)_{n\in\mathbb{N}}| = \lim_{n\to\infty} |f(\alpha_n)| = \widehat{f}((\alpha_n)_{n\in\mathbb{N}})$, we see that $\widehat{f}$ is analytic. Furthermore, $\widehat{f}$ is an embedding because if $\widehat{f}((a_n)_{n\in\mathbb{N}}) = 0$, then

$$\lim_{n\to\infty} |f(a_n)| = \lim_{n\to\infty} |a_n| = 0,$$

so $(a_n)_{n\in\mathbb{N}} + I = \overline{0} + I \in \widehat{R}$. Because R is dense in $\widehat{R}$, the map $\widehat{f}\colon \widehat{R} \hookrightarrow \widehat{S}$ is unique.

If $\widehat{R}'$ is another complete ring with R dense in it, there exist embeddings $\widehat{f}\colon \widehat{R} \hookrightarrow \widehat{R}'$ and $\widehat{g}\colon \widehat{R}' \hookrightarrow \widehat{R}$, so $\widehat{R} \cong \widehat{R}'$.

When R is a field, the inverse of a nonzero class of sequences $(c_n)_{n\in\mathbb{N}} \in \widehat{R}$ where $c = (c_n)_{n\in\mathbb{N}}$ is a representative with no zero coordinates is $c^{-1} := (c_n^{-1})_{n\in\mathbb{N}} \in R^{\mathbb{N}}$. We see that $c^{-1} \in C \setminus I$ because

$$|c_i^{-1} - c_j^{-1}| = |\frac{c_j - c_i}{c_i c_j}$$

where the numerator goes to 0 and the denominator is bounded. □

Question. *Does $\widehat{R}$ being a field imply that R is a field?*

Example 1.5. With respect to the usual absolute value, the completion of $\mathbb{R} = \widehat{\mathbb{Q}}$ and $\mathbb{C} = \widehat{\mathbb{Q}(i)}$.

March 7

Answer. No, consider $K[x, x^{-1}] \subset K((x))$ which is a subring of the field of formal Laurent series. It is not a field as $x^2 + 1 \in K[x, x^{-1}]$ but its inverse $\frac{1}{x^2+1}$ is not in this subring as it is not a Laurent polynomial. Consider its completion with respect to the absolute value defined as $|\frac{a}{b}|_x = 2^{-r}$ for $\frac{a}{b} = x^r \frac{a_0}{b_0}$ where $x \nmid a_0, b_0$. For bigger r, $\frac{a}{b}$ becomes highly divisible by x so we get smaller absolute value, meaning that with completion we are allowed to have higher degrees of x, but for x^{-1} converse happens so principal part stops at some $-N$. Hence its completion gives the *field* of Laurent series.

1.2.1 Archimedean Absolute Values

We will not concern ourselves with archimedean absolute values as they are not particularly interesting from a number theoretical point of view, so we confine ourselves to just stating the following theorems.

Theorem 1.14. *(Ostrowski's Theorem)*

1. *Any archimedean absolute value on $\mathbb{Q}$ is equivalent to the usual absolute value.*
2. *Let K be a field with an archimedean absolute value for which it is complete, then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.*

1.3 Valuations

Let K be a field with a non-archimedean absolute value $|\cdot|$. We had defined the p-adic absolute value as $|x| = p^{-v}$, so we can think of v as $v(x) = -log(|x|)$. With this idea in mind, we add an element ∞ to the real field such that $x < \infty$ for all $x \in \mathbb{R}$ and define a *valuation* as a mapping $v : K \to \mathbb{R} \cup \{\infty\}$ which satisfies the following axioms:

V1: $v(x) \in \mathbb{R}$ for all $0 \neq x \in K$ and $v(0) = \infty$.

V2: $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

V3: $v(xy) = v(x) + v(y)$ for all $x, y \in K$.

Some basic facts about valuations are given in the following proposition.

Proposition 1.15. *Let $v\colon K \to \mathbb{R} \cup \{\infty\}$ be a valuation on the field K. Then*

1. $v(1) = v(-1) = 0$.
2. $v(-x) = v(x)$ *for every* $0 \neq x \in K$.

Proof. By V3, $v(-1) = v(1) + v(-1) \implies v(1) = 0$. Then $v(1) = v(-1) + v(-1) = 0 \implies v(-1) = 0$. Again by V3, $v(-x) = v(-1) + v(x) = v(x)$. □

For two absolute values we said they are equivalent if one is a positive power of the other. Translating it to valuations via $v(x) = -\log|x|$ we get that two valuations v_1 and v_2 are equivalent if for some $\gamma > 0$ we have $v_1(x) = \gamma v_2(x)$ for all $x \in K$.

Example 1.6. Trivial absolute value gives the trivial valuation

$$v(x) = \begin{cases} \infty, & x = 0 \\ 0, & x \neq 0. \end{cases}$$

Example 1.7. For a prime number p, we can define the p-adic valuation

$$v : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$$

as $v_p(a/b) = r$ for

$$\frac{a}{b} = p^r \frac{a_0}{b_0}$$

where $p \nmid a_0, b_0$.

Proposition 1.16. *$\Gamma = v(K^*) \subset \mathbb{R}$ is a subgroup of $(\mathbb{R}, +)$. Here Γ is called the value set.*

The real part of the image $v(K^\times)$ of the valuation is called the *value set* of the valuation v.

Proposition 1.17. *The value set $\Gamma = v(K^\times)$ associated to the valuation $v \colon K \to \mathbb{R} \cup \{\infty\}$ is a subgroup of $(\mathbb{R}, +)$. Furthermore, either $\Gamma = 0$ and v is trivial, or*

1. *Γ has a least positive element and $\Gamma = \lambda\mathbb{Z}$ for some $\lambda > 0$.*
2. *Γ does not have a least positive element and Γ is dense in $\mathbb{R}$.*

Proof. For two elements $v(k_1), v(k_2) \in \Gamma$, we have

1. $-v(k_1) = v(k_1^{-1}) \in \Gamma$.
2. $v(k_1) - v(k_2) = v(k_1/k_2) \in \Gamma$.

For the case (i), say $\lambda \in \Gamma$ is the least positive element. As Γ is a subgroup, every multiple $n\lambda \in \Gamma$ for all $n \in \mathbb{Z}$. Say $a \in \Gamma$ which is not of the type $n\lambda$. Choose $n\lambda$ such that it is the closest element of $\lambda\mathbb{Z}$, but then $0 < a - n\lambda < \lambda$ meaning that λ is not the least positive element, contradiction. Therefore, $\Gamma = \lambda\mathbb{Z}$.

Now suppose that Γ does not contain a least positive element. Since v is not a trivial valuation, it has an element $k \neq 0$ such that $v(k) > 0$. Since Γ does not contain a least positive element there exist a sequence of elements k_n such

that $a_n = v(k_n) \to 0$ as $n \to \infty$. Since this sequence has an accumulation point at 0, and Γ is an additive group, we are done.

□

Valuations in the first case are called *discrete valuations*.

As valuations are equivalent up to multiplication with a constant, multiplying with $\frac{1}{\lambda}$ we get $\Gamma = \mathbb{Z}$. This valuation is called the *normalized discrete valuation*.

Proposition 1.18. *If $v(x) \neq v(y)$ then $v(x+y) = min\{v(x), v(y)\}$.*

Corollary 1.19. *If $x_1 + ... + x_n = 0$ for some $x_1, \ldots, x_n \in K^\times$, then at least two summands have the same valuation.*

Proof. Otherwise

$$\infty = v(0) = \min\{v(x_1), \ldots, v(x_n)\} < \infty.$$

□

A subring V of K with the property that for all $x \in K^\times$ either $x \in V$ or $x^{-1} \in V$ is called a *valuation ring*. Elements of V are called V-integers.

Proposition 1.20. *The set $\mathcal{O}_v = V = \{x \in K \colon v(x) \geq 0\} \cup \{0\} \subset K$ analogous to the closed unit ball in the topology induced by the related absolute value is a valuation ring.*

Proof. By definition, $0 \in \mathcal{O}_v$.Let $x_1, x_2 \in V$,hence we have $v(x_1 + x_2) = \min(v(x_1), v(x_2))$ since both $v(x_1)$ and $v(x_2)$ are greater than zero,their minimum will be greater than 0,showing $x_1 + x_2 \in V$.Similarly, $v(x_1 x_2) = v(x_1) + v(x_2)$,so from this one can easily deduce that $x_1 x_2 \in V$.So it is a subring of K.Let $x \in K^x$,then if $v(x) \leq 0$,then $v(x^{-1}) \geq 0$ showing that $x^{-1} \in V$. Hence V is a valuation ring.

□

We will call $\mathcal{O}_v$ the valuation ring associated to the valuation v.

Example 1.8. If v is the trivial valuation, then the valuation ring associated to v is K itself.

Example 1.9. If v is the p-adic valuation on the rationals, then

$$V = \{\frac{a}{b} \colon (a,b) = 1 \text{ and } p \nmid b\}.$$

Given a valuation ring V of a field K, we can ask whether it comes from some valuation v on K. Notice that divisibility in V is reflected on v because if $ab = c$ with $a, b, c \in K$, then $v(a) + v(b) = v(c)$ where $v(a), v(b), v(c) \geq 0$, so $v(a) \leq v(c)$. It follows that $a \mid c$ if and only if $ca^{-1} \in V$. Using that V is a valuation ring, given $a, c \in V \setminus \{0\}$, either $ca^{-1} \in V$ or $ac^{-1} \in V$, so either $a \mid c$ or $c \mid a$.

March 14

Proposition 1.21. *Every valuation ring V is a local ring.*

Proof. Suppose $\mathfrak{m}_1, \mathfrak{m}_2 \triangleleft V$ are two maximal ideals of V. Take $a \in \mathfrak{m}_1 \setminus \mathfrak{m}_2$ and $c \in \mathfrak{m}_2 \setminus \mathfrak{m}_1$. In particular a and c are in V, so either $a \mid c$ and $c \in \mathfrak{m}_1$ or $c \mid a$ and $a \in \mathfrak{m}_2$.

□

The field $V/\mathfrak{m}$ is called the residue field of V.

If V is associated to a valuation v on K, then the unique maximal ideal $V \setminus V^\times$ of V is given by

$$\mathfrak{m} = V \setminus V^\times = \{x \in K \colon v(x) > 0\}.$$

In this case, the field $V/\mathfrak{m}$ is also called the residue field of v.

A *generalized valuation* $v \colon K \to \mathcal{T} \cup \{\infty\}$ has the image any totally ordered group $\mathcal{T}$. Now, given any valuation ring $V \subset K$, we can define a generalized

valuation

$$\begin{aligned} v\colon K &\to \mathcal{T} \cup \{\infty\} \\ x &\mapsto xV^\times \\ 0 &\mapsto \infty \end{aligned}$$

where $\mathcal{T} = K^\times / V^\times$.

Instead, we will work on the case where the valuation ring is a principal ideal domain. These are called *principal valuation rings*. They correspond in a one-to-one manner to normalized discrete valuations. In this case, the unique maximal ideal of the valuation ring will be generated by each and every element $p \in K$ with $v(p) = 1$.

Proposition 1.22. *If $\mathfrak{m} = p \cdot V$ then p is irreducible in V.*

Proof. If $d \mid p$ for some $d \in V$, then $(d) \supseteq (p)$, but (p) is a maximal ideal. □

Proposition 1.23. *Every $c \in K^\times$ can be written uniquely in the form*

$$c = p^r \cdot u$$

with $r \in \mathbb{Z}$ and $u \in V^\times$.

Proof. As V is a PID, it is in particular a UFD. It is moreover local, so it has a unique irreducible element, i.e. a unique prime. □

Associated to a principal valuation ring V we recover the valuation

$$\begin{aligned} v\colon K &\to \mathbb{R} \cup \{\infty\} \\ p^r u &\mapsto r \\ 0 &\mapsto \infty. \end{aligned}$$

Any generator of the maximal ideal of a principal valuation ring is called a *uniformizer*.

March 14

From the discussion above follows the following theorem.

Theorem 1.24. *There is a 1-1 correspondence between normalized principal valuations and principal valuation rings.*

Example 1.10. The p-adic valuation on $\mathbb{Q}$ has the value set $\mathbb{Z}$ and the valuation ring

$$V_p = \left\{ \frac{a}{b} \in \mathbb{Q} \colon p \nmid b \right\}$$

with the maximal ideal

$$\mathfrak{m}_p = \left\{ \frac{a}{b} \in \mathbb{Q} \colon p \nmid b \text{ and } p \mid a \right\}.$$

The residue field in this case is $V_p/\mathfrak{m}_p \cong \mathbb{F}_p$.

Theorem 1.25. *Any nontrivial valuation V on $\mathbb{Q}$ is a p-adic valuation for some prime p.*

Proof. By Theroem 1.24, it is enough to find all valuation rings V of $\mathbb{Q}$.

Now, let V be a valuation ring of $\mathbb{Q}$. Since $1 \in V$ we have $\mathbb{Z} \subset V$. Let $\mathfrak{m}$ be the maximal ideal of V. Consider $\mathfrak{m} \cap \mathbb{Z}$.Since $\mathbb{Z} \hookrightarrow$ V so for any prime ideal $\mathfrak{p}$ of V,$p \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$,therefore $\mathfrak{m} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Then $\mathfrak{m} \cap \mathbb{Z}$ is either generated by 0 implying $V = \mathbb{Q}$ corresponding to the trivial valuation, or some prime number $p \in \mathbb{Z}$ which corresponds to the p-adic valuation because divisibility in V is reflected on the magnitude of the valuation, so $n \in p\mathbb{Z}$ if and only if $v_p(n) \geq v_p(p)$. □

The idea in the proof can be generalized as follows:

Let $f : A \to B$ be any ring homomorphism.Let $\mathfrak{p}$ be any prime ideal of B and let's define $\mathfrak{p}^c = \{x \in A : f(x) \in \mathfrak{p}\}$ .Then $\mathfrak{p}^c$ is a prime ideal of A.In our case,since we embed $\mathbb{Z}$ into V,so any pre-image of prime ideal has the form $\mathbb{Z} \cap p$.

1.4 Function Fields

Let K be a field. Consider the field $K(x)$ of rational functions on K. Analogous to $\mathbb{Z}$ sitting inside $\mathbb{Q}$ with the p-adic valuation on it for every prime

integer p, we have $K[x] \subset K(x)$ with the $p(x)$-adic valuation on it. In Example 1.4, we have seen the $p(x)$-adic absolute value and the valuation is defined similarly as

$$v_{p(x)}\left(\frac{a}{b}\right) = r \text{ for } 0 \neq \frac{a}{b} = p(x)^r \frac{a_0(x)}{b_0(x)} \text{ where } p(x) \nmid a_0(x), b_0(x)$$

and $v_{p(x)}(0) = \infty$.

A valuation of $K(x)$ *over* K is one that is trivial on K. Note that the $p(x)$-adic valutaion on $K(x)$ is over K. This is a concept that does not appear in the rationals. Its goal is to focus on the contribution of $K(x) \setminus K$ and not the coefficients'.

Theorem 1.26. *If $(V_{p(x)}, \mathfrak{m}_{p(x)})$ is a valaution ring associated to $p(x) \in K[x]$, there is the chain*

$$K \hookrightarrow V_{p(x)} \overset{\phi}{\twoheadrightarrow} V_{p(x)}/\mathfrak{m}_{p(x)}$$

with $\ker \phi \cap K = \{0\}$. Therefore $V_{p(x)}/\mathfrak{m}_{p(x)}$ is a field extension of K. More explicitly,

$$V_{p(x)} = \left\{ \frac{a(x)}{b(x)} \colon p(x) \nmid b(x) \right\}$$
$$\mathfrak{m}_{p(x)} = \left\{ \frac{a(x)}{b(x)} \in \colon p(x) \nmid b(x) \text{ and } p(x) \mid a(x) \right\},$$

and $V_{p(x)}/\mathfrak{m}_{p(x)} = K(\overline{x})$ where $\overline{x} = x + \mathfrak{m} \in V_{p(x)}/\mathfrak{m}_{p(x)}$ is the class of $x \in K[x]$.

Proof. □

Theorem 1.27. *Any nontrivial valuation on $K(x)$ is either a $p(x)$-adic valuation for some irreducible polynomial $p(x) \in K[x]$ or it is the valuation associated to x^{-1} given by*

$$v_{x^{-1}}\left(\frac{f(x)}{g(x)}\right) = \deg g(x) - \deg f(x)$$

where we set $\deg 0 = -\infty$.

Proof. Similar to Theorem 1.24, it is enough to find all the valuation rings $V \subset K[x]$ of $K(x)$. Let $\mathfrak{m}$ be the maximal ideal of V.

Case 1 $K[x] \subset V$ **or, equivalently,** $x \in V$**:** The ideal $\mathfrak{m} \cap K[x]$ of $K[x]$ is generated either by 0 implying $V = K(x)$ and the valuation is trivial, or by some irreducible polynomial $p(x) \in K[x]$, hence $V = V_{p(x)}$.

Case 2 $x \notin V$, **so** $x^{-1} \in \mathfrak{m}$**:** We have $K[x] \subset K(x)$, but there is no canonical way of choosing a generator for transcendental extensions like $K(x)$. Any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PGL_2(K)$ gives another generator $\frac{ax+b}{cx+d}$ for $K(x)$. In particular, $K[x^{-1}] \subset K(x^{-1}) = K(x)$ and by assumption $x^{-1} \in V$. So $x^{-1}K[x^{-1}] = \mathfrak{m} \triangleleft V$ because x^{-1} is irreducible in $K[x^{-1}]$.

Given $a(x^{-1})/b(x^{-1}) \in K(x^{-1})$, we can write

$$\frac{a(x^{-1})}{b(x^{-1})} = (x^{-1})^r \frac{a_0(x^{-1})}{b_0(x^{-1})}$$

where $x^{-1} \nmid a_0(x^{-1}), b_0(x^{-1})$. For a polynomial $f = a_0x^n + \cdots + a_n \in K[x]$, we have

$$f = (x^{-1})^n(a_0 + \cdots + a_n(x^{-1})^n)$$

and define $v_{x^{-1}}(f) = -n = -\deg f$. Now if $\frac{f(x)}{g(x)} \in K(x)$ we can set

$$\begin{aligned} v_{x^{-1}}\left(\frac{f(x)}{g(x)}\right) &= v(f(x)) - v(g(x)) \\ &= -\deg f - (-\deg g) \\ &= \deg g - \deg f. \end{aligned}$$

□

Example 1.11. If K is an algebraically closed field, say $K = \mathbb{C}$, then there is a valuation for each irreducible polynomial $x - \alpha \in \mathbb{C}[x]$ and one corresponding to x^{-1}. From the geometric object $\mathbb{C}$, one gets the field $\mathbb{C}(x)$ of rational functions on $\mathbb{C}$. By looking at valuations, one returns to the initial object plus ∞. This is in fact $\mathbb{P}_1(\mathbb{C})$ with the affine chart $\mathbb{A}^1(\mathbb{C}) \cong \mathbb{C}$, but the point $\mathbb{P}_1(\mathbb{C}) \setminus \mathbb{A}^1(\mathbb{C})$ depends on the choice. For example, if one prefers 0 to be the point at infinity, x^{-1} is replaced by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} x^{-1} = x.$$

Example 1.12. Instead of looking at the affine space, we can specialize the above construction to the case of an irreducible variety $E \subset \mathbb{A}^2(\mathbb{C})$ for example defined by $f(x,y) = y^2 - x^2(x+1) \in K[x,y]$. For each point $P \neq \mathcal{O}$ on the elliptic curve E we get a valuation on $K(x,y)$ with the relation $f(x,y) = 0$ corresponding to the inclusion $K(x) \subset K(x,y)$, and one at ∞ corresponding to the point $\mathcal{O}$ on E.

For most points, the correspondence between the points of the elliptic curve and the valuations is 2-to-1, except for the points with $y = 0$ which are called the ramification points.

Example 1.13. Associated to each $\alpha \in \mathbb{C}$, we have a valuation on $\mathbb{C}(x)$ and also the evaluation map $\frac{f(x)}{g(x)} \overset{ev_\alpha}{\mapsto} \frac{f(\alpha)}{g(\alpha)}$, but the denominator might not always be defined. This corresponds to $(x-\alpha) \nmid g(x)$, i.e. the evaluation is defined only on $V_{x-\alpha}$. The map

$$\begin{aligned} \pi \colon V_{x-\alpha} &\to V_{x-\alpha}/\mathfrak{m}_{x-\alpha} \\ \frac{f(x)}{g(x)} &\mapsto \frac{f(x)}{g(x)} + \mathfrak{m}_{x-\alpha} \end{aligned}$$

now has the image the field of definition of α.

Example 1.14. For a field that is not algebraically closed such as $K = \mathbb{R}$, there are three types of valuations: one per each $x - \alpha, \alpha \in \mathbb{R}$, one per each $x^2 + ax + b$ with $a, b \in \mathbb{R}, a^2 - 4b < 0$, and one for x^{-1}.

In the first case, the valuation ring and its unique maximal ideals are

$$\begin{aligned} V_{x-\alpha} &= \left\{ \frac{f}{g} \colon x - \alpha \nmid g \right\}, \\ \mathfrak{m}_{x-\alpha} &= \left\{ \frac{f}{g} \colon x - \alpha \nmid g \text{ and } x - \alpha \mid f \right\}, \end{aligned}$$

respectively, with the quotient map given by

$$\begin{aligned} V_{x-\alpha} \overset{\phi}{\to} V_{x-\alpha}/\mathfrak{m}_{x-\alpha} &\overset{ev_\alpha}{\cong} \mathbb{R} \\ \frac{f}{g} \mapsto \frac{f}{g} + \mathfrak{m}_{x-\alpha} &\mapsto \frac{f(\alpha)}{g(\alpha)}. \end{aligned}$$

In the second case, for example x^2+1 gives has the imaginary solutions $\{i,-i\}$ where neither one of them is defined over $\mathbb{R}$ independently, but the Galois orbit is defined as a whole and leads to a unique valuation over $\mathbb{R}(x)$ because for $f,g\in\mathbb{R}[x]$,

$$\frac{f}{g}(i)=0 \iff \overline{\frac{f}{g}(i)}=\frac{f}{g}(-i)=0.$$

Similarly, in general, for any $x^2+ax+b\in\mathbb{R}[x]$ with $a^2-4b<0$ there is one single valuation on $\mathbb{R}(x)$ with the valuation ring V_{x^2+ax+b} given by

$$V_{x^2+ax+b}=\left\{\frac{f}{g}\colon x^2+ax+b\nmid g\right\},$$

the maximal ideal $\mathfrak{m}_{x^2+ax+b}$ given by

$$\mathfrak{m}_{x^2+ax+b}=\left\{\frac{f}{g}\colon x^2+ax+b\nmid g \text{ and } x^2+ax+b\mid f\right\}.$$

The residue field is

$$\begin{aligned} V_{x^2+ax+b}/\mathfrak{m}_{x^2+ax+b} &= \mathbb{R}[x]/(x^2+ax+b)\\ &= \mathbb{R}(\overline{x}) \ \cong \mathbb{C}\\ \frac{f}{g} &\ \mapsto \frac{f}{g}(i). \end{aligned}$$

It is interesting to note that on $\mathbb{Q}$ each distinct pair of primes p and q leads to residue fields $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ that lives in disjoint worlds.

March 16

If $(V,\mathfrak{p})$ is the (local) valuation ring associated to some (discrete) valuation $v\colon K\to\mathbb{R}\cup\{\infty\}$, the completion $\widehat{K}$ with respect to the absolute value $|x|=\gamma^{-v(x)}$ for some $\gamma>1$ induced on K has the valuation ring

$$W=\{x\in\widehat{K}\colon v(x)\geq 0\}$$

with the maximal ideal $\mathcal{P}$. Note that $V=W\cap K$.

Proposition 1.28. *With the notation above, $V/\mathfrak{p}=W/\mathcal{P}$.*

Proof. Let $a \in W$. As $v(a) = \lim_{n\to\infty} v(a_n) \geq 0$, we can see a as a Cauchy sequence in V. This means there is some $N \geq 0$ such that $|c - c_k| < 1$ for all $k \geq N$ which translates to $v(c - c_k) > 0$, hence $c - c_k \in P$.

By the second isomorphism theorem,

$$V/\mathfrak{p} = V/(V \cap \mathcal{P}) \cong (V + \mathcal{P})/\mathcal{P} = W/\mathcal{P}.$$

□

By the definition of valuation of a Cauchy sequence, the value group Δ of v on $\widehat{K}$ is the completion of the value group Γ of v on K. In particular, if $\Gamma = \mathbb{Z}$ then $\Delta = \mathbb{Z}$, too.

We have seen that when v is a principal valuation the valuation ring V is a principal ideal domain. In particular, the unique maximal ideal $\mathfrak{p} = (p)$ for some prime $p \in V$. An element $x \in K$ is in $\mathfrak{p}^n V$ if and only if $p^n \mid x$ in V, i.e. $v(x) > n-1$. So the balls of the form $\mathfrak{p}^n V$ form a basis for the neighborhoods of 0. Mimicking this construction around nay $a \in V/\mathfrak{p}^n \setminus \{0\}$ we see that

$$a + \mathfrak{p}^n V = \{x \in V \colon v(a) > n - 1\}$$

is an open neighborhood of a. So

$$V/\mathfrak{p}^n V = \bigcup_{a \in V/\mathfrak{p}^n \setminus \{0\}} a + \mathfrak{p}^n V$$

is open. But now, both $\mathfrak{p}^n V$ and $V \setminus \mathfrak{p}^n V$ are open, hence the topological space V is disconnected. Moreover, we can separate any two points by taking n sufficiently large. So the only connected subsets of V are singletons, i.e. V is totally disconnected.

Every $x \in K^\times$ can be written in a unique way as

$$x = p^n u$$

for some unit $u \in V^\times =: U$, so we have

$$K^\times = \langle p \rangle \times U.$$

Define

$$U_n := 1 + \mathfrak{p}^n V = \{x \in K \colon v(x-1) \geq n\}.$$

For example, if U is the units of the completion $K[\![x]\!]$ of $K[x]$ under the valuation associated to x, then

$$U_n = \{1 + a_n x^n + a_{n+1} x^{n+1} + \dots\}.$$

We have the filtration

$$K^\times \supseteq U_0 \supseteq U_1 \supseteq \dots$$

where $U_0 = V$. The intersection of all U_n is given by

$$\bigcap_{n=1}^{\infty} U_n = \{1\}.$$

The surjective group homomorphism $\phi_{|U} \colon U \twoheadrightarrow F^\times$ which is the restriction of the ring homomorphism $\phi \colon V \to F = V/\mathfrak{p}$ has the kernel $\ker \phi_{|U} = U_1$. Similarly $U_n/U_{n+1} \cong F$ for each $n \geq 0$.

1.5 Completion and Power Series

Let K be a field, v a principal valuation v on it with a uniformizer π. So we know that $v(\pi) = 1$ and the maximal ideal $\mathfrak{p}$ of the valuation ring V is generated by π.

Let $A \subset V$ be a set of representatives of each coset under $\phi \colon V \to V/\mathfrak{p}$.

Example 1.15. For the p-adic valuation on $\mathbb{Q}$ we can take $A = \{0, \dots, p-1\}$.

Example 1.16. For the x-adic valuation on $K(x)$ we can take $A = K$.

Now, assume $0 \in A$ represents $\mathfrak{p}$. Every $c \in K^\times$ can be written uniquely as $c = \pi^r u$ for some integer $r \in \mathbb{Z}$ and a unit $u \in V^\times$ in the valuation ring. There is a unique nonzero element of A such that

$$\phi(u) = \phi(c\pi^{-r} = \phi(a)$$

which means $a - c\pi^{-r} \in \langle \pi \rangle$, i.e. $v(c - \pi^{-r}a) \geq 1$ implying $v(c - \pi^r a) \geq r+1$. So for any $n \geq r$ there is a unique sum $a_r\pi^r + a_{r+1}\pi^r + \cdots + a_n\pi^n$ such that $v(c - (a_r\pi^r + a_{r+1}\pi^r + \cdots + a_n\pi^n)) \geq n+1$ where each $a_i \in A$ and $a_r \neq 0$.

Every element in $K^\times$ has a unique representative as a power series, but not every power series corresponds to an element of K. This holds only if K is complete.

Define addition and multiplication on A as follows: Given elements $a_1, a_2 \in A$ their sum $a_1 + a_2 = a$ where $a \in A$ is by construction the unique element satisfying $\phi(a) = \phi(a_1 + a_2)$; similarly, their product $a_1 a_2 = b$ for $\phi(b) = \phi(a_1 a_2)$.

Now, given two power series

$$c = \sum a_i \pi^i \text{ and } c' = \sum a_i' \pi^i,$$

define their sum $c + c'$ as

$$c + c' = \sum s_i \pi^i$$

where

$$\begin{aligned} s_0 &= a_0 + a_0' \mod \langle \pi \rangle \\ s_1 &= (a_0 + a_0' - s_0)\pi^{-1} + a_1 + a_1' \mod \langle \pi \rangle \\ &\vdots \end{aligned}$$

and their product cc' as

$$cc' = \sum t_i \pi^i$$

where

$$\begin{aligned} t_0 &= a_0 a_0' \mod \langle \pi \rangle \\ t_1 &= (a_0 a_0' - t_0)\pi^{-1} + a_0 a_1' + a_1 a_0' \mod \langle \pi \rangle \\ &\vdots \end{aligned}$$

For example, one may write

$$17 = 23^0 + 23^1 + 13^2$$

where $A = \{0, 1, 2\}$ or

$$17 = 23^0 + 23^1 + 43^2 + 23^3 + 23^4 + \ldots.$$

2 Extensions

Let w be a valuation on a field L extending another field K, let $W \subset L$ be the associated valuation ring with the maximal ideal $Q \subset W$, and let Δ be the value group of w. The residue class field of w is denoted $L_w = W/Q$.

The restriction $v = w_{\restriction K}$ is a valuation on K. We say w *lies over* v. Let V be the valuation ring of v with the maximal ideal $P \subset V$. The value group Γ of v is not only a subset but also a subgroup of Δ. In particular, if Δ is trivial, then so is Γ. Let $K_v = V/P$ be the residue class field of v.

If Δ and Γ are both nontrivial so that $\Delta = r\mathbb{Z}$ and $\Gamma = s\mathbb{Z}$ for some $r, s \in \mathbb{R}$, then $s = kr$ for some $k \in \mathbb{Z}$ and $\Delta/\Gamma \cong \mathbb{Z}/k\mathbb{Z}$ is finite. The ratio $e = (\Delta : \Gamma)$ is called the *ramification index* of L/K or of Q/P. The extension is said to be *ramified* if $e > 1$ and *unramified* otherwise.

Since v is a restriction of w, the valuation ring V of v can also be expressed as

$$V = \{x \in K \colon w(x) = 0\} = W \cap K.$$

Conversely, if $W \subset L$ is a valuation ring, then $W \cap K$ will always be a valuation ring of K. Indeed, if $x \in K$ then either $x \in W$ or $x^{-1} \in W$ because W is a valuation ring of $L \supset K$, but both x and x^{-1} are always in K, so either $x \in W \cap K$ or $x^{-1} \in W \cap K$, proving that $W \cap K$ is a valuation ring of K.

Similarly,

$$P = \{x \in K \colon w(x) > 0\} = Q \cap K.$$

It is also true that $P = Q \cap V$.

Comparing the residue class fields, we see that

$$K_v = V/P = V/(Q \cap V) \cong (V + Q)/Q \subset W/Q = L_w.$$

When L_w is a finite extension of K_v, the extension degree $f = [L_w : K_v]$ is called the *residue degree* or the *inertia degree* of L/K or of Q/P or of W/V.[4]

[4]Sometimes there will be multiple pairs of residue class field extensions attached to the same pair of fields with varying residue degrees.

The following example carries the geometric intuition:

Example 2.1. Let $L = \mathbb{R}(x)$ be the field of rational functions with real coefficients. We have seen in Example 1.14 that L has one valuation at ∞ corresponding to x^{-1} and one valuation for each irreducible polynomial $p(x) \in \mathbb{R}[x]$. Number fields do not have isomorphic subfields, but in the function field case we have

$$K = \mathbb{R}(t) = \mathbb{R}(x^2) \cong L.$$

The indeterminate x above has the irreducible polynomial $irr(x, K) = T^2 - t$, so the extension degree $[L : K] = 2$. In this particular setup, it is true that

$$L = K(x) = \mathbb{R}(t)(x) = \mathbb{R}(x).$$

So L can be written as $L = \mathbb{R}(t, x)$ with $x^2 = t$.

Geometrically, the situation is reflected in the following figure.

The picture tells us that there will be a valuation on K for each valuation $x - x_0$ (or point x_0) on L by forgetting the x-coordinate. It also tells us that there are three possibilities going up:

1. Above any valuation $t - t_0$ (or point t_0) of K there will be two valuations.
2. At 0 the two points collide.
3. For the negative points $-t_0$ there will be complex points $(-t_0, \sqrt{t_0}i)$ above. Together these complex points $(-t_0, \pm\sqrt{t_0}i)$ form a Galois orbit and a single valuation corresponding to $x^2 + t_0^2$ with residue class field $\mathbb{C}$ whereas the residue class field below is $\mathbb{R}$. $\Diamond$

March 23

If $K \subseteq L \subseteq M$ is a tower of field extensions with a valuation u of M restricted to w on L and v on K, then the residue degrees satisfy

$$f_{u/v} = f_{u/w} f_{w/v}.$$

If the value groups of u, v and w are A, Δ and Γ, respectively, then the ramification indices satisfy

$$e_{M/K} = (A : \Gamma) = (A : \Delta)(\Delta : \Gamma) = e_{M/L} e_{L/K}.$$

Theorem 2.1. *If a valuation w on L lies over some valuation v on K with ramification index e and residue degree f, then*

$$ef \leq [L : K].$$

Proof. If $[L : K] = \infty$, then there is nothing to prove.

Suppose $[L : K] = \dim_K L < \infty$. Then it is enough to find ef many K-linearly independent elements in L.

By the definition of $f = [L_w : K_v]$, there are $u_1, \ldots, u_f \in W$ such that $\overline{u_1}, \ldots, \overline{u_r} \in L_w$ are linearly independent over K_v where W is the valuation ring of w. We claim that $u_1, \ldots, u_r$ are linearly independent over K. Indeed, being linearly independent, the images $\overline{u_1}, \ldots, \overline{u_r}$ are never $\overline{0} = Q$ in L_w, so $u_1, \ldots, u_f \notin Q$ which means $w(u_i) = 0$ for all $i = 1, \ldots, f$ where Q is the maximal ideal of W. If there were $a_1, \ldots, a_f \in K$ such that

$$a_1u_1 + \cdots + a_fu_f = 0, \text{ i.e. } w(a_1u_1 + \cdots + a_fu_f) = \infty,$$

then assuming that –without loss of generality– $w(a_1) \leq w(a_i)$ for all i and $w(a_1) = w(a_j)$ for all $j = 1, \ldots, k$ for some $k < f$, set $c_i = a_it^{-l}$ where t is a uniformizer of w and $l = w(a_1)$. Then we get

$$c_1u_1 + \cdots + c_ku_k = ct^{l+1}t^{-l}$$

for some $c \in L$. Reducing modulo Q, we get that $c_j = 0$ and $a_j = 0$ for all $j = 1, \ldots, k$ because

$$\overline{c}_1\overline{u}_1 + \cdots + \overline{c}_k\overline{u}_k = \overline{0}$$

where $\overline{u}_1, \ldots, \overline{u}_k$ are linearly independent over K_v. Repeating with

$$a_{k+1}u_1 + \cdots + a_fu_f = 0,$$

we see that $f \leq [L : K]$. In particular, if L/K is finite, then f is finite, i.e. the extension L_w/K_v is finite.

To complete the proof, choose some $\pi_1, \ldots, \pi_e \in L$ such that

$$\{w(\pi_1), \ldots, w(\pi_e)\}$$

is a complete set of representatives of cosets Δ/Γ. The claim is that

$$\{u_i\pi_j\}_{i=1,\dots,f,\, j=1,\dots,e}$$

consists of K-linearly independent elements of L.

Indeed, if

$$\sum_{i,j} a_{ij}u_i\pi_j = 0$$

for some $a_{ij} \in K$, then for $A_j = \sum_i a_{ij}u_i$ we get that $\sum_j A_j\pi_j = 0$. By Proposition 1.18, $w(A_h\pi_h) = w(A_k\pi_k)$ for some $h \neq k$ which implies

$$w\left(\frac{\pi_k}{\pi_h}\right) = \min\{v(a_{1h}), \dots, v(a_{fh})\} - \min\{v(a_{1k}), \dots, v(a_{fk})\} \in \Gamma.$$

Contradiction. □

Corollary 2.2. *If a valuation w on L lies over a valuation v on K, then v is trivial (resp. principal) if and only if w is.*

Proof. As v is the restriction of w, the properties of w obviously emanate on to v. On the other hand, if v is trivial, as $\Delta \leq \mathbb{Z}$ having $|\Delta| = e \cdot |\Gamma| = e$ is not possible. Similarly, if v is principal, then we have

$$\Delta \subseteq \frac{1}{e}\Gamma,$$

so w is principal, too. □

Corollary 2.3. *If L/K is an algebraic field extension, then L_w/K_v is also algebraic and Δ/Γ is torsion.*

2.1 Complete Fields

Fix a field K, complete with respect to an absolute value $|\cdot|$.

A function $\|\cdot\| : V \to \mathbb{R}$ on a K-vector space V satisfying

N1: $\|x\| \in \mathbb{R}$ for all $0 \neq x \in K$ and $\|x\| = \infty$.

N2: $\|x+y\| \geq \min\{\|x\|, \|y\|\}$ for all $x, y \in K$.

N3: $\|cy\| = |c|\|y\|$ for all $x, y \in K$.

is called a *norm*.

A norm defines a metric $d(x,y) = \|x-y\|$ satisfying $d(cx,cy) = |c|d(x,y)$ for all $c \in K$.

March 28

Let V be a finite dimensional K-vector space. Fix a basis $w_1, \ldots, w_n$ (hence an isomorphism $V \cong K$) for V over K. For any $x = \sum_{i=1}^{n} c_i w_i$ define the cubical norm on V as $\|x\| = \max\{|c_i|\}$. Note that the value depends on the basis, but the topologies induced by different bases are equal.[5]

Lemma 2.4. *If $(K, |\cdot|)$ is complete, then $(V, \|\cdot\|)$ is also complete. Moreover, any other norm on V gives the same topology as the cubical norm.*

Proof. Let $(a_j)_{j\in\mathbb{N}}$ be a Cauchy sequence in V. Let each a_i be given as

$$a_j = \sum_{i=1}^{n} c_{ij} w_i,$$

where $\{w_1, \ldots, w_n\}$ is a basis of V over K and each $c_{ij} \in K$.

Being a Cauchy sequence in this setup of cubical norm means

$$\lim_{j,k\to\infty} \max_i |c_{ij} - c_{ik}| = 0.$$

In particular,

$$\lim_{j,k\to\infty} \max |c_{ij} - c_{ik}| = 0$$

for each $i = 1, \ldots, n$. Using that K is complete, let b_i be the limit of $(c_{ij})_{j\in\mathbb{N}}$. It easily follows that

$$a = \lim_{j\to\infty} (a_j) = \sum_{i=1}^{n} b_i w_i.$$

[5]This goes to say that the linear transformations and in particular the base changes are continuous.

This concludes the first part of the lemma.

Now, let $N(\cdot)$ be any other norm on V. To show that $N(\cdot)$ and $\|\cdot\|$ induces the same topology on V it suffices to prove that $\lim_{j\to\infty} N(a_j) = 0$ if and only if $\lim_{j\to\infty} \|a_j\| = 0$ which amounts to telling that

$\Longrightarrow$: Opens of the topology induced by $N(\cdot)$ are contained in those of $\|\cdot\|$.

$\Longleftarrow$: Opens of the topology induced by $\|\cdot\|$ are contained in those of $N(\cdot)$.

Hence that they induce the same topology.

Let $(a_j)_{j\in\mathbb{N}}$ be a sequence in V such that $\|a_j\| \to 0$. Then, with the notation above,

$$\begin{aligned} N(\sum_{i=1}^{n} b_i w_i) &\leq \sum_{i=1}^{n} N(b_i w_i) \\ &= \sum_{i=1}^{n} |b_i| N(w_i) \\ &\leq \sum_{i=1}^{n} \max_i |b_i| N(w_i) \\ &= \|a\| \sum_{i=1}^{n} N(w_i), \end{aligned}$$

and the last sum is a constant depending on the basis, so $N(a_j) \to 0$.

Conversely, if $N(a_j) \to 0$ and $\|a_j\| \nrightarrow 0$, then at least one limit b_{i_0} does not converge to 0. Without loss of generality, assume $i_0 = 1$. Let (a'_j) be given as

$$a'_j = \frac{a_j}{|b_{1j}|},$$

where j runs over a subsequence of (b_{1j}) satisfying

$$|b_{1j} > \epsilon_0$$

for some $\epsilon_0 > 0$.

We are back to to the initial setting of this implication, but now we have $c_{1j} = 1$ for all j's in this restricted subsequence. As $c_{1j} = 1$ always, the cubical norm $\|a'_j\|] \geq 1$ always. But now

$$\begin{aligned} 0 &= \lim_{j\to\infty} N(w_1 + c_{2j}w_2 + \cdots + c_{nj}w_n) \\ &= N(w_1) + \lim_{j\to\infty} N(c_{2j}w_2 + \cdots + c_{nj}w_n), \end{aligned}$$

so

$$\lim_{j\to\infty} N(w_1 + c_{2j}w_2 + \cdots + c_{nj}w_n) = -N(w_1). \tag{1}$$

Note that the lemma holds for $V = K$. By induction, we can assume that it also holds for $W = \langle w_2, \ldots, w_n\rangle \subset V$. In particular, it says that W is complete, but the contradiction is given by (1) which says $w_1 \in W$. □

We saw that topology induced by a norm is unique on a complete field which means that norms are all equivalent. Let $||_1$ and $||_2$ be two norms on L which is an extension of a complete field K. Equivalence implies that $||_1 = ||_2^\gamma$ but as they agree on K we must have $\gamma = 1$, meaning that $||_1 = ||_2$. Hence we have the following theorem.

Theorem 2.5. *Let K be a complete absolute valued field. Then any algebraic extension E of K has at most one extension of the absolute value and it is complete for the induced topology*

March 30

In order to consider the extensions of valuations v on K, we can equivalently deal with valuation rings $W \supseteq V$ of L for a valuation ring V of K.

Let R be a subring of K. An element $c \in K$ is said to be integral over R if it satisfies a monic equation

$$c^n + a_1c^{n-1} + \cdots + a_{n-1}c + a_n = 0$$

for some $a_i \in R$.

Homework 2.1. When $R = \mathbb{Z}$ and $K = \mathbb{Q}(i)$, elements $c \in K$ that are integral over R are precisely the elements of $\mathbb{Z}[i]$.

The set of elements $c \in K$ such that c is integral over R is called the integral closure of R in K. If the integral closure of R in K is R itself, then we say R is integrally closed in K.

Homework 2.2. Principal ideal domains are integrally closed in their field of fractions.

Proposition 2.6. *Unique factorization domains are integrally closed in their field of fractions.*

Proof. Let K be the field of fractions of a UFD R. Let $\frac{a}{b} \in K$ where a and b are relatively prime. If

$$\left(\frac{a}{b}\right)^n + a_1\left(\frac{a}{b}\right)^{n-1} + \cdots + a_n = 0$$

for some $a_i \in R$, then multiplying by a common denominator b we get

$$b(a_1 a^{n-1} b^{n-2} + \cdots + a_n b^{n-1}) = -a^n.$$

Since R is a UFD, it follows that $b \mid a^n$, but the assumption was that b and a are relatively prime, so b must be a unit. □

For a nonexample look at $R = k[x, y]/(y^2 - x^3)$. As $y^2 - x^3 \in k[x, y]$ is prime, the quotient ring R is an integral domain. Let K be its field of fractions. Take $c = \frac{y}{x} \in K$. Because of the relation asserted by $y^2 - x^3 = 0$, in $R[T]$ we have

$$c^2 - x = 0.$$

This is an anomaly due to the zero set

of $y^2 - x^3$ being singular.

Theorem 2.7. *The integral closure of an integral domain R in its field of fractions K is a subring of K.*

To prove this theorem, we look for an easier description of integrality over R.

Lemma 2.8. *Integrality of $c \in K$ over R is the same as there being a finitely generated nonzero R-submodule M of K such that*

$$cM \subseteq M.$$

Proof. ($\Longrightarrow$) if $c \in K$ satisfies

$$c^n + a_1 c^{n-1} + \cdots + a_n = 0$$

for some $a_i \in R$, then we can replace c^n by

$$c^n = -(a_1 c^{n-1} + \cdots + a_n),$$

and use this relation to rewrite c^{n+i} for all $i > 0$ in terms of $1, c, \ldots, c^{n-1}$. This says that the R-algebra $R[c]$ is a finitely generated R-module.

($\Longleftarrow$) Let $\{u_1, \ldots, u_n\}$ be a set of genereators for M. By assumption, we can write

$$\begin{aligned} cu_1 &= c_{11}u_1 + \cdots + c_{1n}u_n \\ &\vdots \\ cu_n &= c_{n1}u_1 + \cdots + c_{nn}u_n. \end{aligned}$$

In terms of matrices, this is

$$A \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = 0$$

for

$$A = \begin{bmatrix} c_{11} - c & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} - c & \ldots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} - c \end{bmatrix}.$$

The determinant $\det A$ is 0 and it gives a monic relation for c over R. □

Proof. (Theorem 2.7.) Given c_1, c_2 with M_1, M_2 satisfying the assertion of Lemma 2.8, take $M = M_1 M_2$ for $c_1 + c_2$ or $c_1 c_2$ to prove closure under addition and multiplication. □

Lemma 2.9. *Valuation rings are integrally closed in their field of fractions.*

Proof. Let W be a valuation ring of L with the field of fractions K. Every $c \in L$ satisfies either $c \in W$ so $c \in K$, or $c \notin W$ so $c^{-1} \in W$ yielding $c \in K$. It follows that $L \subseteq K$. As L is a field and $W \subseteq L \subseteq K$, we get that the field of fractions $K = L$.

Let $c \in L$ be integral over W. Assume $c \notin W$. It follows that $c^{-1} \in m \lhd W$ where m is the unique maximal ideal of W. If c satisfies

$$c^n + a_1 c^{n-1} + \cdots + a_n = 0$$

for some $a_i \in W$, then

$$1 = -a_1 c^{-1} - \cdots - a_n (c^{-1})^n \in m.$$

This contradiction proves that W is integrally closed in its field of fractions K. □

It is a fact that the integral closure of some subring R of a field K is the intersection of all valuation rings of L containing K. If our aim is to find valuation rings extending some $V \subseteq K$, then we can look for valuation rings W containing the integral closure of V in L.

Theorem 2.10. *If L is a finite and algebraic extension of K, and V is a valuation ring of K, then there is a valuation ring W of L containing V.*

Proof. Let I be the integral closure of V in L.

Claim. The field of fractions of I is L.

Proof of claim. Every $\gamma \in L$ satisfies some polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x].$$

By Theorem 2.7, K is the field of fractions of V; therefore, expressing each a_i as $a_i = \frac{b_i}{b_i'}$ we can write $f(x) = g(x)/c$ for

$$g(x) = cx^n + b_1 x^{n-1} + \cdots + b_n \in V[x]$$

and $c = b_1' \cdots b_n'$. Note that

$$g(\gamma) = c\gamma^n + b_1\gamma^{n-1} + \cdots + b_n = 0.$$

Multiplying by c^{n-1} we get

$$\eta^n + b_1\eta^{n-1} + b_2 c\eta^{n-2} \cdots + b_n c^{n-1} = 0$$

where $\eta = c\gamma$ which, as shown, satisfies a monic equation over V; therefore, $\eta \in I$. It follows that $\gamma = \frac{\eta}{c}$ is in the field of fractions F of I. As γ is arbitrary, $L \subseteq F$, so $L = F$. □

Consider the family $\mathcal{F}$ of subrings S of L containing I and having the intersection $S \cap K = V$. Note that $\mathcal{F} \neq$ because $I \in F$ as V is integrally closed. By Zorn's lemma, $\mathcal{F}$ has a maximal element W.

If R is a subring of L containing W, then for $c \in R \backslash W$ we have $K \cap W[c] = K$ by maximality of W. ... [missing]

Every $r \in W[c]$ induces a map $\alpha \overset{m_r}{\mapsto} r\alpha$ on $W[c]$ between K and finite-dimensional K-vector space L, hence itself a K-vector space with $\ker m_r = \{0\}$. As $W[c]$ is finite dimensional, m_r is an isomorphism; in particular, $rs = 1$ for some $s \in W[c]$, i.e. $W[c]$ is a field. Since the field of fractions of I is L, it follows that $W[c] = L$, and W is a maximal subring of L which is not a field because $W \subsetneq L$ because $W \cap K = V$.

Take $c \in W$ with $c^{-1} \notin W$. By the above claim, $W[c^{-1}] = L$. If L were finitely generated as a W-module, for a fixed m which is the maximum such that c^{-m} appears in the generators of L, every element of L would be in the form ac^{-m} for some $a \in W$, but $c^{-(m+1)} \in L$ is a counterexample, showing that L is not finitely generated as a W-module.

To see that W is a valuation ring of L, assume there is some $u \in L$ such that neither u nor u^{-1} is in L. Then $W[u] = W[u^{-1}] = L$ by the maximality of W as a subring of L. It follows that

$$\begin{aligned} u &= a_0 + a_1 u^{-1} + \cdots + a_r u^{-r} \\ u^2 &= a_0 u + a_1 + \cdots + a_r u_{-r+1} \\ &\vdots \end{aligned}$$

So u^n can be written as a W-linear combination of $1, \ldots, u^{-r}$, contradicting the previous paragraph. $\square$

This proof uses Zorn's Lemma, so it is not very constructive. To construct valuations in field extensions L/K where K is complete, we define a valuation $w : E \to \mathbb{R} \cup \{\infty\}$ on E, the normal closure of L, and restrict it to L to get a valuation $u : L \to \mathbb{R} \cup \{\infty\}$ on L. By the theorem (2.5), there is a unique extension w of v to E. If $\sigma : E \to E$ is an automorphism of E, then $w \circ \sigma : E \to \mathbb{R} \cup \infty$ is once again a valuation on E, by the uniqueness then $w = w \circ \sigma$. Now we define the norm $N_{E/K}(\alpha)$ of $\alpha \in E$ over K as

$$N_{E/K}(\alpha) = \sigma_1(\alpha) \ldots \sigma_r(\alpha) \ ,$$

where $\{\sigma_1, \ldots, \sigma_r\}$ is the set of automorphisms of E over K. Then

$$w(N_{E/K}(\alpha)) = w\left(\prod_{i=1}^{r} \sigma_i(\alpha)\right) = \sum_{i=1}^{r} w(\sigma_i(\alpha)) = r \cdot w(\alpha) \ . \tag{2}$$

The set of automorphisms of E is a group so $\sigma\{\sigma_1, \ldots, \sigma_r\} = \{\sigma_1, \ldots, \sigma_r\}$ for any $\sigma \in Aut(E)$, it follows that $N_{E/K} \in K$, so

$$w(N_{E/K}(\alpha)) = v(N_{E/K}(\alpha)) \ .$$

Combining this with (2) we get $w(\alpha) = \frac{v(N_{E/K}(\alpha))}{r}$. By the normality of E, we have the following

$$w(\alpha) = \frac{1}{[E : K]} v(N_{E/K}(\alpha))$$

Now consider the case that α is transcendental over K which is not necessarily complete, define a valuation w on $K[\alpha]$ by extending v as $w : K[\alpha] \to \mathbb{R} \cup \{\infty\}$ via

$$f = a_0 + \cdots + a_n \alpha^n \mapsto min\{v(a_0), \ldots, v(a_n)\} \ .$$

The function w on $K[\alpha]$ is a valuation. (Hint: the same idea as in Gauss' Lemma) Passing to the field of fractions $K(\alpha)$ of $K[\alpha]$ define $w(f/g) = w(f) - w(g)$.

This valuation w is called the Gaussian extension of v to $K(\alpha)$. Because w is defined by minimums, the value group Δ of $K(\alpha)$ and the value group Γ of

K are equal. Since $\alpha = 1 \cdot \alpha$, its valuation $w(\alpha) = 1$, so $\alpha \in W$ the valuation ring of $K(\alpha)$. If $Q \lhd W$ is the unique maximal ideal of W, then $\alpha + Q \in L_w$ is transcendental. Indeed if

$$\overline{a_0} + \overline{a_1}(\alpha + Q) + \ldots, \overline{a_n}(\alpha + Q)^n = \overline{0}$$

in K_v, where V is the valuation ring of v, each $\overline{a_i} = a_i + P$ for some $a_i \in K$ where $P \lhd V$ is the unique maximal ideal of V. The ring operations on K_v require $a_0 + a_1\alpha + \cdots + a_n\alpha_n \in Q$, in other words $w(a_0 + a_1\alpha + \cdots + a_n\alpha^n) > 0$ but $v(a_i) = 0$ for some a_i so that the polynomial is not constantly zero. This contradiction shows that there is no such f, meaning that α is transcendental over K_v. We can sum up our conclusion as follows:

Theorem 2.11. *Let K be any field with a general valuation v and $L = K(\alpha)$ a purely transcendental extension. Then the Gaussian extension of v to L is a valuation on L, with the same value group as v and with residue class field $K_v(\overline{\alpha})$, a purely transcendental extension of the residue class field K_v of K.*

2.1.1 Extensions of Incomplete Fields

Let L/K be a field extension. Let v be a valuation on K. Let $\hat{K}$ be the completion of K with respect to v. We can base extend L to the K-algebra via $L \otimes_K \hat{K}$. This $\hat{K}$-algebra will factor as $\prod K_i = L \otimes_K \hat{K}$ and v will be extended to w_i on each K_i.

2.1.2 Tensor Products

Let K be a ring. Let U, V be K-modules. A map $f : U \times V \to W$ from the direct product $U \times V$ of U and V to a K-module W is said to be K-bilinear if it is K-linear in both entries, in other words

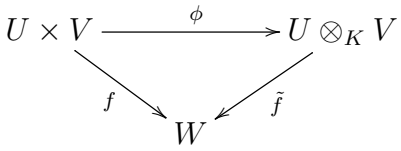
$$f(au_1 + bu_2, v) = af(u_1, v) + bf(u_2, v)$$
$$f(u, av_1 + bv_2) = af(u, v_1) + bf(u, v_2)$$

for all $a, b \in K$. In the case that K is a field and $U = V$ is a K-algebra, the map $(u_1, u_2) \mapsto u_1u_2$ is a K-bilinear map on the set $U \times U$. The tensor product is the tool to understand bilinear maps.

Theorem 2.12. *Given K-modules U and V, there exists a K-module $U \otimes_K V$, called the* tensor product *of U and V over K such that every bilinear map*

$$f \colon U \times V \to W$$

factors as in the following commutative diagram



for some $\phi \colon U \times V \to U \otimes_K V$ fixed for the U, V pair and a K-module homomorphism $\tilde{f}$.

Proof. Consider the free K-module A on $U \times V$. Imposing the bilinearity conditions, consider the submodule $B \subset A$ genearated by

$$(au_1 + bu_2, v) - a(u_1, v) - b(u_2, v)$$

and

$$(u, av_1 + bv_2) - a(u, v_1) - b(u, v_2)$$

for all $a, b \in V, u_i \in U, v_i \in V$. Define $U \otimes_K V$ to be

$$U \otimes_K V = A/B,$$

and the map ϕ as

$$\begin{aligned} \phi \colon U \times V &\to A/B \\ (u, v) &\mapsto u \otimes v. \end{aligned}$$

The elements of the form $u \otimes v$ are called the *pure tensors*, and

$$A/B = \{c_i((u, v) + B)\} = \{c_i u \otimes v\}$$

is the set of K-bilinear combinations of pure tensors.

Define $\tilde{f}$ as

$$\begin{aligned} \tilde{f} \colon U \otimes_K V &\to W \\ (u \otimes v) &\mapsto f(u, v). \end{aligned}$$

The well-definedness of $\tilde{f}$ is left as an exercise. □

Starting from K-modules U and V we have arrived at a K-module $U \otimes_K V$. If K was a field and U and V were K-algebras, then using $\mu_1 \colon U \otimes_K U \to U$ and $\mu_2 \colon V \otimes_K V \to V$ factoring the multiplication maps $U \times U \to U$ and $V \times V \to V$, we define the coordinatewise map μ on $U \otimes_K V$ as

$$\begin{aligned} \mu \colon (U \otimes_K V) \times (U \otimes_K V) &\to U \otimes_K V \\ (u_1 \otimes v_1, u_2 \otimes v_2) &\mapsto \mu_1(u_1 \otimes u_2) \otimes \mu_2(v_1 \otimes v_2) \end{aligned}$$

and see that $U \otimes_K V$ is a K-algebra, too.

In our case of interest, we will have $U = K(\alpha)$ and $V = \widehat{K}$. If $f(x) = irr(\alpha, K)$, then $U = K[x]/fK[x]$.

Theorem 2.13. *There are the isomorphisms*

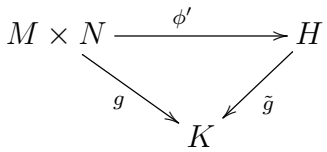
$$\begin{aligned} K(\alpha) \otimes_K \widehat{K} &\cong \widehat{K}[x]/f\widehat{K}[x] \\ &\cong \widehat{K}[x]/g_1\widehat{K}[x] \oplus \cdots \oplus \widehat{K}[x]/g_r\widehat{K}[x \end{aligned}$$

for some $g_1, \ldots, g_r \in \widehat{K}[x]$ *such that*

$$f = g_1 \ldots g_r.$$

April 6

To see that $M \otimes N$ is unique, take



such that g is a bilinear map that factors through H. Then taking $K = M \otimes N$ and the earlier module to be H, we see that $M \otimes N \cong H$.

Proposition 2.14. *Let* M *be an* R*-module. Then*

$$M \otimes_R R \cong M.$$

Proof. We will give two different proofs: one directly constructive, the other showcasing the universal property.

1. Write the isomorphism explicitly:

$$\begin{aligned} M \otimes_R R &\cong M. \\ rm \otimes 1 = m \otimes 1 &\mapsto rm \\ m \otimes 1 &\leftarrow\!\shortmid m \end{aligned}$$

□

2. Every bilinear map $f\colon M \times R \to L$ for some R-module L factors through M by a bilinear map

$$\begin{aligned} \tilde{f}\colon M &\to L \\ m &\mapsto f(m, 1). \end{aligned}$$

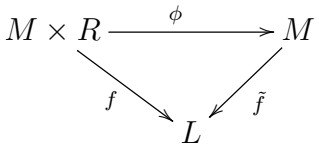
Note that $f = \tilde{f} \circ \phi$ where

$$\begin{aligned} \phi\colon M \times R &\to M \\ (m, r) &\mapsto rm, \end{aligned}$$

since

$$\begin{aligned} \tilde{f}(\phi(m, r)) &= \tilde{f}(rm) \\ &= r\tilde{f}(m) \\ &= rf(m, 1) \\ &= f(m, r). \end{aligned}$$

The R-module isomorphism $\tilde{f}$ thus defined is unique because of the restrictions of being bilinear.



□

Proposition 2.15. *Let $M_i, i \in I$ and N be R-modules. Then*

$$\left(\bigoplus_{i \in I} M_i \right) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N).$$

Proof. Exercise. □

In our case of interest, we will take all M_i in Proposition 2.15 to be R and denote $\bigoplus_{i\in I} R = R^I$ whence it says that every element of $R^I \otimes_R N$ can be written in a unique way as a finite sum

$$\sum e_i \otimes y_i$$

where $\{e_i\}_{i\in I}$ is the standard basis of the free R-module R and $y_i \in N$ is nonzero for only finitely many $i \in I$.

Corollary 2.16. *Let K be a field and let M and N be K-vector spaces. Then $\{e_i \otimes_K f_j\}$ is a basis for $M \otimes_K N$ if $\{e_i\}_{i\in I}$ is an K-basis for M and $\{f_j\}_{j\in J}$ is an K-basis for N.*

Proof. Apply Proposition 2.15 twice: with $M \cong K^I$ and with $N \cong K^J$. □

Say A is a K-algebra and F/K is a field extension. In particular, F is a free K-module. Let $\{e_i\}_{i\in I}$ be a basis of F over K. Then

$$\begin{aligned} F \otimes_K A &\cong (\bigoplus_{i\in I} K) \otimes_K A \\ &\cong \bigoplus_{i\in I} (K \otimes_K A) \\ &\cong \bigoplus_{i\in I} A. \end{aligned}$$

Let $\{b_j\}_{j\in J}$ be a K-basis for A. By Corollary 2.16, $\{e_i \otimes b_j\}$ is a K-basis for $F \otimes_K A$. Including F in the scalars, $\{1 \otimes b_j\}_{j\in J}$ is a basis of $F \otimes_K A$ as an F-module. In particular,

$$\dim_K A = \dim_F (F \otimes_K A).$$

April 11

Let E/K and F/K be two field extensions. Assume that E/K is a separable degree n extension. By the primitive element theorem $E = K(\beta)$ with $f(\beta) =$

0 for some irreducible $f \in K[x]$ of degree n. In particular, $E = K[x]/(f)$ is an n-dimensional E-vector space. The inclusion $K \hookrightarrow F$ induces an inclusion $K[x] \hookrightarrow F[x]$ between the polynomial rings which in turn induces an inclusion $K[x]/fK[x] \hookrightarrow F[x]/fF[x]$ between the quotient rings.

Lemma 2.17. *Let f, K, and F be as above. Then*

$$K[x]/fK[x] \otimes_K F \cong F[x]/fF[x].$$

Proof. We will give two proofs:

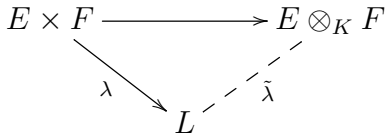
1. One way to prove this isomorphism is to show that the right hand side satisfies the universal property of the tensor product.

   The bilinear map $\lambda\colon E \times F \to F[x]/fF[x]$ is given as

   $$\lambda(h + fK[x], c) = hc + fF[x].$$

   To show the existence and uniqueness of the factoring map is left as an exercise.

2. The bilinear map λ in the first proof factors through $E \otimes_K F$ to some $la\tilde{m}bda$.

   If $c_m x^m + \cdots + c_0 \in F[x]/fF[x]$, then $\tilde{\lambda}(x^m \otimes c_m + \cdots + 1 \otimes c_0) = c_m x^m + \cdots + c_o$; therefore, $\tilde{\lambda}$ is surjective. Moreover, by the discussion after Corollary 2.16,

   $$\dim_F(F[x]/fF[x]) = \deg f = n;$$

   hence,

   $$E \otimes_K F \cong F[x]/fF[x].$$

□

The polynomial $f(x)$ seen in $F[x]$ might not be irreducible anymore. Let

$$f(x) = g_1(x) \dots g_r(x)$$

where $g_1, \dots, g_r \in F[x]$ be distinct irreducible polynomials. Then

$$E \otimes_K F = K_1 \oplus \dots \oplus K_r$$

where

$$K_j = F[x]/(g_j).$$

For each $j = 1, \dots, r$ there is an inclusion

$$\begin{aligned} \iota_j \colon E &\hookrightarrow K_j \\ \beta &\mapsto \beta_j, \end{aligned}$$

and F sits in K_j as the field of constants. Also, there are the projections

$$\pi_j \colon E \oplus_K F \twoheadrightarrow K_j.$$

Composing, we get

$$\lambda_j \colon E \to K_j.$$

The kernel $\ker \lambda_j$ is either 0 or the all of E. As $\lambda_{j|K}$ is the identity on K, we have $\ker \lambda_j = \{0\}$, i.e. λ_j injects into K_j.

Now, set $F = \widehat{K}$. For each $j = 1, \dots, r$ the valuation v on the complete field $\widehat{K}$ extends uniquely to some valuation w_j on K_j by some earlier theorem. The restrictions $v_j = w_{j|E}$ are valuations on E.

Lemma 2.18. *Each K_j is the completion of E at v_j.*

Proof. There exists the maps

$$L = K \otimes_K L \hookrightarrow \widehat{K} \otimes_K L \twoheadrightarrow K_j$$

where the injection has dense image because K is dense in $\widehat{K}$. □

Lemma 2.19. *Up to equivalence $v_1, \dots v_r$ are all the extensions of v to E.*

Proof. Let v' be a valuation on E extending v. As $E = K \otimes_K E$ sits densely in $\widehat{K} \otimes_K E$, by continuity, v' defines a valuation on

$$\widehat{K} \otimes_K E = K_1 \oplus \cdots \oplus K_r.$$

Defining $v'(k_j) = v'(0, \ldots, 0, k_j, 0, \ldots, 0)$ we see that v' defines a valuation on each K_j that extends v; but such an extension is unique as K_j is a finite separable extension of K, so $v'_{|K_j} = w_j$.

Without loss of generality, if $v'_{|K_1} \neq 0 \neq v'_{|K_2}$, then for $\alpha_1 \in K_1$ and $\alpha_2 \in K_2$ with $v'(\alpha_1) \neq 0 \neq v'(\alpha_2)$ the contradiction is given by

$$\begin{aligned} 0 &\neq v'(\alpha_1)v'(\alpha_2) \\ &= v'(\alpha_1, 0, 0, \ldots, 0)v'(0, \alpha_2, 0, \ldots, 0) \\ &= 0. \end{aligned}$$

It follows that v' on E is either the trivial valuation or one of the v_j. □

Lemma 2.20. *The valuations $w_1, \ldots, w_r$ are pairwise inequivalent.*

Proof. (I could not hear the proof.) □

Theorem 2.21. *(Collect all of them in our context here.)*

Theorem 2.22. *Let L/K be Galois of degree n, let v be a principal valuation on K, and let $w_1, \ldots, w_r$ be all the extensions of v to L. Then the ramification indices $e(w_i|v)$ are all equal*

$$e = e(w_i|v), \forall i,$$

and the inertia degrees $f(w_i|v)$ are all equal

$$f = f(w_i|v), \forall i.$$

Proof. Follows from the Galois group acting transitively on the valuations. For details, consult the textbook. □

2.2 Dedekind Domains

The ring $\mathcal{O}_K$ of integers of a number field K is given by the integral closure of $\mathbb{Z}$ in K, denoted $\mathrm{ic}_K(\mathbb{Z})$. The following proposition is another way of expressing $\mathcal{O}_K$:

Proposition 2.23. *The ring $\mathcal{O}_K$ is the set of elements of K satisfying a monic polynomial with integer coefficients.*

Proof. □

Up until now, we considered valuations on $\mathbb{Q}$ and their extensions to number fields. We have the following proposition to connect these approaches:

Proposition 2.24. *For each prime $p \in \mathbb{Z}$ one has the containment $\mathbb{Z} \subseteq \mathcal{O}_p$ and*

$$\mathbb{Z} = \bigcap_{p \text{ prime}} \mathcal{O}_p.$$

Proof. □

One can generalize this proposition to number fields.

Theorem 2.25. *For each valuation ring $\mathcal{O}$ of some number field K, one has the containment $\mathbb{Z} \subseteq \mathcal{O}$ and the integral closure $\mathrm{ic}_K(\mathbb{Z})$ of $\mathbb{Z}$ in K is given as*

$$\mathrm{ic}_K(\mathbb{Z}) = \bigcap_{\mathcal{O} \text{ valuation ring of } K} \mathcal{O}.$$

Proof. □

What is more general than looking at all valuations on a number field is to consider a family S of pairwise inequivalent principal valuations on an arbitrary field K and the associated ring

$$\mathcal{O}_S = \bigcap_{v \in S} O_v$$

of S-integers. The family S is called the *prime divisors* or *places*.

Example 2.2. Let $K = \mathbb{Q}$ and $S = \{v_2, v_3\}$. Then

$$\begin{aligned}\mathcal{O}_S &= \mathcal{O}_2 \cap \mathcal{O}_3 \\ &= \{\frac{a}{b} \in \mathbb{Q} | 2, 3 \nmid b\}.\end{aligned}$$

Let us denote by M_K all the valuations on some field K.

Example 2.3. Let $K = k(x)$ for some field k, and let $S = M_K$. Recall from Theorem 1.27 that the valuations on K are one for each irreducible polynomial $p(T) \in k[T]$ and one at infinity corresponding to $\frac{1}{T}$. It follows that if $\frac{f(T)}{g(T)}$ is an element of $\mathcal{O}_S$, then no irreducible polynomial can divide $g(T)$, implying $\deg g(T) = 0$. On the other hand, for

$$v_\infty(\frac{f}{g}) = -\deg f + \deg g$$

to be nonnegative, $\deg f$ must be 0; therefore,

$$\mathcal{O}_S = k.$$

We also saw that

$$\mathcal{O}_{M_K \setminus \{v_\infty\}} = k[x].$$

We say that S has the *strong approximation property* if

D1: Every valuation in S is principal.

D2: Every $x \in K$ is in $\mathcal{O}_p$ for all but finitely many $p \in S$.

D3: Given $p, p' \in S$ and for every $N > 0$, there exists some $x \in K$ satisfying

(i) $v_p(x - 1) > N$,
(ii) $v'_p(x) > N$,
(iii) $v_q(x) \geq 0$ for all $q \in S$.

Theorem 2.26 (Strong Approximation Theorem)**.** *Let S be a family of inequivalent valuations on some field K. Let $p_1, \ldots, p_n \in S$ and let $a_1, \ldots, a_n \in K$. If S has the strong approximation property, then for every $N > 0$ there exists some $x \in \mathcal{O}_S$ such that $v_{p_i}(x - a_i) > N$ for $i = 1, \ldots, n$.*

Proof. Read Cohn, Theorem 4.1. □

2.2.1 Fractional Ideals

We can define multiplication on ideals I and J of some ring R as

$$I \cdot J = \{\sum_{k=1}^{n} x_k y_k | x_k \in I, y_k \in J\}.$$

Basic properties of ideal multiplication are presented in the next proposition.

Proposition 2.27. *Multiplication of ideals is associative with the unit element being R.*

Proof. □

Two properties of a group is checked, the remaining one is the existence of inverses. Considering the case of $R = \mathbb{Z}$ and $I = 2\mathbb{Z}$, we realize the need for inverses in R:

$$2\mathbb{Z} \cdot \frac{1}{2}\mathbb{Z} = \mathbb{Z}.$$

To find generators like $\frac{1}{2}$, we need to pass to a field containing R. In particular, these inverse ideals are not ideals of R anymore.

Recall the properties of an ideal: We call I an ideal of R if

1. $I \subseteq R$,
2. $x + y \in I$ for every $x, y \in I$.
3. $cx \in I$ for every $c \in R, x \in I$.

Crossing out the first property we are left with closure under addition and multiplication by constants, in which case we call I an R-module. This calls for a definition: Let $\mathcal{O}$ be a ring contained in some field K. A *fractional ideal* I of $\mathcal{O}$ is an $\mathcal{O}$-module $I \subseteq K$ such that

$$u\mathcal{O} \subseteq I \subseteq v\mathcal{O}$$

for some $u, v \in K$.

If $I \subseteq \mathcal{O}$ is an ideal, then $u \in I$ arbitrary and $v = 1$ makes I a fractional ideal. In fact, the fractional ideals of $\mathcal{O}$ that are contained in $\mathcal{O}$ correspond to normal ideals in $\mathcal{O}$ and are called *integral ideals*.

Let I and J be fractional ideals of $\mathcal{O}$ with

$$u_1\mathcal{O} \subseteq I \subseteq v_1\mathcal{O}$$
$$u_2\mathcal{O} \subseteq J \subseteq v_2\mathcal{O}.$$

Then

$$I \cdot J = \{\sum_{k=1}^{n} x_k y_k | x_k \in I, y_k \in J\}$$

is a fractional ideal of $\mathcal{O}$ with

$$u_1u_2\mathcal{O} \subseteq IJ \subseteq v_1v_2\mathcal{O}.$$

Given a fractional ideal I of $\mathcal{O}$, does there exist some fractional ideal J such that $IJ = \mathcal{O}$? This is true *exactly when* $\mathcal{O}$ is a Dedekind domain. Going back, for a family S of inequivalent valuations, the ring $\mathcal{O}_S$ is a Dedekind domain exactly when S has the strong approximation property.

Let

$$I = \mathcal{O}f_1 + \cdots + \mathcal{O}f_r$$

for some

$$f_i = \frac{g_i}{h_i},\ g_i, h_i \in \mathcal{O}$$

be a finitely generated $\mathcal{O}$-submodule and let K be the field of fractions of $\mathcal{O}$. Define $h = h_1 \cdots h_r$. Multiplying by h kills the denominators, so we have $hI \subseteq \mathcal{O}$ and $I \subseteq h^{-1}\mathcal{O}$. It is easy to see that

$$\mathcal{O} \cdot I = I \text{ and } I \cdot \mathcal{O} = I,$$

so we have an identity element.[6] Given I, if there exists J such that $I \cdot J = \mathcal{O}$, we say that I is *invertible*.

[6]The $\subseteq$'s are by I being a sum with $\mathcal{O}$ coefficients and $\supseteq$'s are by $1 \in \mathcal{O}$.

In general, we define

$$(\mathcal{O} : I) = \{x \in \mathcal{O} \colon xI \subseteq \mathcal{O}\}$$

which is a fractional ideal and an $\mathcal{O}$-submodule because if $x_1, x_2 \in (\mathcal{O} : I)$ then $x_1 I \subseteq \mathcal{O}$ and $x_2 I \subseteq \mathcal{O}$ which gives $(a_1 x_1 + a_2 x_2)I \subseteq \mathcal{O}$ meaning that $a_1 x_1 + a_2 x_2 \in (\mathcal{O} : I)$ for every $a_1, a_2 \in \mathcal{O}$. Also, if $u\mathcal{O} \subseteq I \subseteq v\mathcal{O}$ then

$$v^{-1}\mathcal{O} \subseteq (\mathcal{O} : I) \subseteq u^{-1}\mathcal{O}$$

which means that $(\mathcal{O} : I)$ is a fractional ideal. Further, we always have $I \cdot (\mathcal{O} : I) \subseteq \mathcal{O}$; if equality holds, we say that I is *invertible* and its *inverse* I^{-1} is $(\mathcal{O} : I)$.

As an example, let $I \subseteq \mathbb{Q}$ be a $\mathbb{Z}$-module. For a common denominator $h \in \mathbb{Z}$, we have $hI \subseteq \mathbb{Z}$. The ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$, hence

$$hI = n\mathbb{Z} = \langle p_1 \rangle^{e_1} \dots \langle p_r \rangle^{e_r}$$

if n factors into primes as $n = p_1^{e_1} \dots p_r^{e_r}$. It follows that

$$\begin{aligned} I &= \langle p_1 \rangle^{e_1} \dots \langle p_r \rangle^{e_r} \langle q_1 \rangle^{-f_1} \dots \langle q_s \rangle^{-f_s} \\ &= \prod p_i^{a_i} \end{aligned}$$

where $h = q_1^{f_1} \dots q_s^{f_s}$ is the prime factorization of h.

This example hints at a correspondence between fractional ideals ideals and tuples $(a_p)_{p \in S}$ of integers. Observe that a_p is zero for infinitely many valuations. The second axiom of the strong approximation property says that $v_p(x) = 0$ for almost all $p \in S$ when x is fixed.

Define the multiplication of two formal products of valuations $\prod_{p \in S} p_i^{a_i}$ and $\prod_{p \in S} p_i^{b_i}$ as

$$\prod_{p \in S} p_i^{a_i} \prod_{p \in S} p_i^{b_i} = \prod_{p \in S} p_i^{a_i + b_i}.$$

Notice that this is a free abelian group generated by elements in S where instead of the additive notation $\sum a_i p_i$ we use the multiplicative notation as above.

We want to find an isomorphism between the set of fractional ideals and the tuples $(a_p)_{p\in S}$. We saw that (a_i) establishes a free abelian group so if we can construct such an isomorphism, then the fractional ideals, hence the number theory part will be tamed. We will see that such an isomorphism holds in the Dedekind domains, hence all fractional ideals will be invertible.

Let's first consider an example.

Example 2.4. Let $x \in \frac{7}{18}\mathbb{Z}$ so we have $v_2(x) \geq -1$, $v_3(x) \geq -2$, $v_7(x) \geq 1$ and $v_p(x) \geq 0$ for the others. We define $a_2 = -1$, $a_3 = -2$, $a_7 = 1$ and $a_p = 0$ so we get the product as $(2\mathbb{Z})^{-1} \cdot (3^2\mathbb{Z})^{-1} \cdot 7\mathbb{Z}$.

Let $\mathcal{F}$ be the set of $\mathcal{O}$-modules contained in K, and let $\mathcal{D}$ be the free abelian group generated by S :

$$\mathcal{D} = \left\{ \prod_{p\in S} p^{a_p} \colon a_p \in \mathbb{N} \right\}.$$

Define the maps

$$\begin{aligned} v_p \colon \mathcal{F} &\to \mathbb{Z} \\ I &\mapsto \min_{x\in I} v_p(x) \end{aligned}$$

and

$$\begin{aligned} \varphi \colon \mathcal{F} &\to \mathcal{D} \\ I &\mapsto \prod_{p\in S} p^{v_p(I)}. \end{aligned}$$

The map v_p is well defined: As $u\mathcal{O} \subseteq I \subseteq v\mathcal{O}$ we have $v_p(u) \geq v_p(I) \geq v_p(v)$, hence $v_p(x) \in \mathbb{Z}$.

Moreover, φ is a group homomorphism: Let I and J be two fractional ideals.

Then

$$\begin{aligned} v_p(I \cdot J) &= \min_{\sum_k a_k b_k \in I \cdot J} v_p\left(\sum a_k b_k\right) \\ &\geq \min_{\sum_k a_k b_k \in I \cdot J} \min_k v_p\left(a_k b_k\right) \\ &\geq \min_{a \in I,\, b \in J} v_p(ab) \\ &= \min_{a \in I} v_p(a) + \min_{b \in B} v_p(b) \\ &= v_p(I) + v_p(J). \end{aligned}$$

On the other hand, $v_p(I \cdot J) \leq v_p(I) + v_p(J)$ because $ab \in I \cdot J$ for $a \in I$ and $b \in J$ satisfying $v_p(a) = v_p(I)$ and $v_p(b) = v_p(J)$. We conclude that $v_p(I \cdot J) = v_p(I) + v_p(J)$ and that φ is a homomorphism.

April 20

On the other direction, define the map $\psi \colon \mathcal{D} \to \mathcal{F}$ as

$$\psi(\prod_{p \in S} p^{a_p}) = \{x \in K \colon v_p(x) \geq a_p\}.$$

Proposition 2.28. *The map ψ is a well-defined group homomorphism that satisfies $I \subseteq \psi(\varphi(I))$ for any $I \in \mathcal{F}$.*

Proof. The image $\psi(\prod_{p \in S} p^{a_p})$ is a $\mathcal{O}$-module contained in K:

The map ψ is a group homomorphism:

$I \subseteq \psi(\varphi(I))$: □

Lemma 2.29. *If S has the strong approximation property, then $\psi(\prod_{p \in S} p^{a_p})$ is a fractional ideal for every $\prod_{p \in S} p^{a_p}$.*

Proof. Let $\prod_{i=1}^n p_i^{a_i} \in \mathcal{D}$ with $a_i \neq 0$ for all $i = 1, \ldots, n$. Apply Theorem 2.26, the Strong Approximation Theorem, with $N = -\min a_1, \ldots, a_n, 0$ to get some $x \in \mathcal{O}_S$ such that $v_{p_i}(x - a_i) > N$ for $i = 1, \ldots, n$; consequently,

$$\psi(\prod_{p \in S} p^{a_p}) \subseteq x^{-1}\mathcal{O}_S.$$

To find a nonzero element $u \in \psi(\prod_{p\in S} p^{a_p})$, use the theorem again. Then $u\mathcal{O}_S \subseteq \psi(\prod_{p\in S} p^{a_p})$ and the image is a fractional ideal. □

Lemma 2.30. *Let A be a fractional ideal. If $x \in K$ such that $v_p(x) \geq v_p(A)$ for all $p \in S$, then $x \in A$, i.e. $\psi(\varphi(A)) \subseteq A$.*

Proof. Let $B = x^{-1}A$ and $C = B \cap \mathcal{O}_S$. For every $p \in S$ it must be the case that $v_p(B) \leq 0$ and $v_p(C) = 0$.

Take $c \in C$. If c is a unit in $C \subseteq B$, then $cc^{-1} = 1 \in B$, hence $x \in A$ and we are done; otherwise, choose $a_i \in C$ where $v_{p_i}(C)$, which is 0 because $C \subseteq \mathcal{O}_S$, is attained for those finitely many valuations $p_1, \ldots, p_n$ with $v_{p_i}(c) \neq 0$. By Theorem 2.26, for each $j = 1, \ldots, n$ there is some b_j such that

$$\begin{aligned} v_{p_j}(b_j - a_j^{-1}) &\geq v_{p_j}(c), \\ v_{p_i}(b_j) &\geq v_{p_i}(c),\ \forall i \in \{1, \cdot, \hat{j}, \cdot, n\}, \\ v_q(b_j) &\geq 0, q \neq p_1, \ldots, p_n. \end{aligned}$$

Since $v_p(c) \in \mathcal{O}_S$ and $v_{p_j}(a_j) = 0$ we have $b \in \mathcal{O}_S$.

Put $a = \sum a_j b_j$ and $d = c^{-1}(1 - a)$. If $d \in \mathcal{O}_S$, then $1 = dc + a \in c$ and we are done; otherwise, by the choice of each b's we have

$$\begin{aligned} v_{p_j}(1 - a) &= v_{p_j}((1 - (a_j b_j)) - \sum_{i\neq j} a_i b_i \\ &\geq v_{p_j}(-a_j(b_j - a_j^{-1})) && \geq 0 + v_{p_j}(c) \\ &= v_{p_j}(c), \end{aligned}$$

hence $c^{-1}(1 - a) \in \mathcal{O}_S$. □

Theorem 2.31. *When S has the strong approximation property, $\psi \circ \varphi$ is identity.*

Proof. Let $J = \prod_{p\in S} p^{a_p}$, $a_p \in \mathbb{Z}$. We need to find $x \in \psi(J)$ such that

$$v_p(x) = a_p \text{ and } v_q(x) \geq a_q,\ \forall q \neq p.$$

Since p's are normalized, v_p's are surjective. Take $\beta \in K$ such that $v_p(\beta) = a_p$ and use Theorem 2.26 to find x such that

$$v_p(x - \beta) = a_p + 1 \text{ and } v_q(x) \geq a_q, \forall q \neq p.$$

□

Theorem 2.32. *Let K be a field and let S be a set of places with the strong approximation property. Put $\mathcal{O}_S = \bigcap_{p \in S} \mathcal{O}_p$. Then the fractional ideals of $\mathcal{O}_S$ form an abelian group isomorphic to the divisor group on S. In particular, every fractional $\mathcal{O}$-ideal is invertible:*

$$I^{-1} = \psi(\varphi(I)^{-1}).$$

Theorem 2.33. *Let $\mathcal{O}$ be an integral domain with the field of fractions K. Then the following are equivalent:*

(i) $\mathcal{O}$ is the intersection of principal valuation rings $\mathcal{O}_p \subset K$ with the strong approximation property.

(ii) Fractional $\mathcal{O}$-ideals form a group with respect to the ideal multiplication.

(iii) $\mathcal{O}$ satisfies the following:

- *(a) $\mathcal{O}$ is Noetherian.*
- *(b) $\mathcal{O}$ is integrally closed in K.*
- *(c) Every nonzero prime ideal of $\mathcal{O}$ is maximal.*

An integral domain satisfying these properties is called a *Dedekind domain.*

Theorem 2.34. *Let A be a ring. Then the following are equivalent:*

(i) The set Σ of ideals of A satisfies the ascending chain condition: Every increasing chain $I_1 \subseteq I_2 \subseteq \ldots$ of ideals stabilizes, i.e. $I_k = I_{k+1} = \ldots$ for some k.

(ii) Every nonempty set of ideals $\mathcal{I} \subset \Sigma$ has a maximal element.

(iii) Every ideal of A is finitely generated.

Proof. The equivalence of (i) and (ii) is clear.

(i) $\implies$ (iii): Let I be an ideal of A, and let $f \in I$. If $I \setminus (f_1) = \emptyset$ we are done. Otherwise, choose $f_2 \in I \setminus (f_1)$ and so on. This constructs an ascending chain

$$(f_1) \subset (f_1, f_2) \subset \dots.$$

By (i), this chain stabilizes, i.e.

$$I \setminus (f_1, \dots, f_n) = \emptyset$$

for some n. As $(f_1, \dots, f_n) \subseteq I$, we get

$$I = (f_1, \dots, f_n).$$

(Note that, this proof uses the axiom of choice while choosing $f_1, f_2, \dots$. An alternative proof that do not use it is given next.)

(ii) $\implies$ (iii): Given an ideal I, consider the set S of the finitely generated ideals of A which are contained in I. This set is nonempty since $(0) \in S$. By (ii), S has a maximal element, say J. Let $f \in I$. By maximality, $(f, J) = J$ so $f \in J$.

(iii) $\implies$ (i). Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals of A. The set $I = \bigcup_{i=1}^{\infty} I_i$ satisfies $a + b \in I$ because some I_k contains both a and b, so $a + b \in I_k \subseteq I$. Also, if $r \in I$ and $a \in I$, then $ra \in I_k$ for some k, so $ra \in I$. It follows that I is an ideal. By (iii), it must be finitely generated. Let $I = (f_1, \dots, f_n)$. There is some I_k containing all f_i. Then

$$I = (f_1, \dots, f_r) \subseteq I_k \subseteq I_{k+1} \subseteq I,$$

so the chain stabilizes. □

A ring that satisfies these properties is called a Noetherian ring.

Lemma 2.35. *Let $\mathcal{O}$ be an integral domain with field of fractions K. If the set of $\mathcal{O}$-fractional ideals form a group, then $\mathcal{O}$ is Noetherian.*

Proof. Let I be an ideal of $\mathcal{O}$. We would like to show that I is finitely generated. If $I = (0)$ then it is already finitely generated. Otherwise, there is some fractional ideal I^{-1} of $\mathcal{O}$ such that $II^{-1} = \mathcal{O}$, which goes to say that, in particular,

$$\sum_{i=1}^{r} a_i b_i = 1$$

for some $a_i \in I$ and $b_i \in I^{-1}$.

Let $x \in I$. Write

$$x = x1 = x \sum_{i=1}^{r} a_i b_i = \sum_{i=1}^{r} a_i (x b_i).$$

As $II^{-1} = \mathcal{O}$ we have $xb_i \in \mathcal{O}$ for $i = 1, \ldots, r$; hence, I is generated by $a_1, \ldots, a_r$ over $\mathcal{O}$. □

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Consider the map

$$\begin{aligned} \Theta \colon K^\times &\to D_K \\ \alpha &\mapsto \prod p^{v_p(\alpha)} \end{aligned}$$

where D_K is the free abelian group on all (principal) valuations of K.

If $\alpha \in \ker \Theta$ then $\alpha \notin \mathfrak{m}_p$ for any maximal ideal $\mathfrak{m}_p$, hence $\alpha \in \mathcal{O}^\times$. Conversely, if $\alpha \in \mathcal{O}^\times$, then it is not contained in any proper ideal, so

$$\ker \Theta = \mathcal{O}^\times.$$

Denote $\mathcal{O}^\times = U$.

We have the short exact sequence

$$1 \longrightarrow U \longrightarrow K^\times \xrightarrow{\Theta} D_K \longrightarrow D_K/\Theta(K^\times) \longrightarrow 1,$$

which is a short (and fancy) way of saying that at each particular place in the sequence, the image and the kernel are the same. In this case, it says that U embeds into $K^\times$ and $U = \ker \Theta$ while the quotient map surjects.

Note that

$$v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$$

implies

$$\Theta(\alpha\beta) = \Theta(\alpha)\Theta(\beta),$$

so the image $Im\Theta$ of Θ is a subgroup of D_K.

The quotient $D_K/\Theta(K^\times)$ is called the *class group.* We will try to understand the map Θ by getting a hold on the units and on the class group.

April 25

Theorem 2.36. *Let $\mathcal{O}_K$ be the intersection $\mathcal{O}_K = \bigcap_{p\in S} \mathcal{O}_p$ of the valuation rings of all non-archimedean valuations of a number field K. The integral closure $ic_K(\mathbb{Z})$ of $\mathbb{Z}$ in K is $\mathcal{O}_K$.*

Proof. That $\mathcal{O}_K \subset ic_K(\mathbb{Z})$ follows from $ic_K(\mathcal{O}_p) = \bigcap_{p|q} \mathcal{O}_q$. For the other direction, let $\alpha \in ic_K(\mathbb{Z})$. Then there is some irreducible monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Having integer coefficients, $f \in \mathcal{O}_p[x]$ for all primes $p \in \mathbb{Z}$ hence $ic_K(\mathbb{Z}) \subseteq \mathcal{O}_K$. □

3 Algebraic Function Fields & Riemann-Roch

In what follows, we will deal with the rational function field $K(x)$ and its finite extensions F/K, which we call *function fields (over K).* Two good references for this part are [1] and [2].

We call K the constant field of F/K, but there may be more constants as in the case of $\mathbb{C}(x, \sqrt{x^3 + ax + b})/\mathbb{R}$. We call $\tilde{K} = F \cap \bar{K}$ *the full constant field of F/K.*

3.1 Valuations over the Constant Field

We have seen the valuations of $K(x)$ at Theorem 1.27. Valuations of a function field F/K are extensions of valuations of $K(x)$.

Proposition 3.1. *If v is a valuation of F over K, then v is also over $\tilde{K}$.*

Proof. Let $z \in \tilde{K}$. Assume $z \notin \mathcal{O}_v$. Then $z^{-1} \in P_v$. By definition z is algebraic, hence so is z^{-1}: There are $a_i \in K$ such that

$$(z^{-1})^r + \cdots + a_1 z^{-1} + a_0 = 0,$$

and

$$v(z) = v\left(-\frac{1}{a_0}((z^{-1})^{r-1} + \cdots + a_1)\right) \geq 0,$$

contradicting $z \notin \mathcal{O}_v$. We reach a similar contradiction when $z^{-1} \notin \mathcal{O}_v$, and conclude that $z \in \mathcal{O}_v \setminus P_v$, i.e. $v(z) = 0$. □

Maximal ideals P of valuations are called places and the set of all places of F/K is denoted $\mathbb{P}_F$. Furthermore, we use $\mathcal{O}_P$ and $\mathcal{O}_v$ interchangeably when $P = P_v$ and we denote by F_P the residue class field $\mathcal{O}_P/P$ of P.

One might see $\mathcal{O}_P$ as the functions defined at the place P, and by abuse of notation, P as functions which vanish there; whereas, the residue class field is the field of values of functions in F at P: Using the map

$$\begin{aligned} \mathcal{O}_P &\to F_P \\ z &\mapsto z + P, \end{aligned}$$

we will set $z(P) = z + P$ as the value of z at the place P. Also, we can extend this map to F as

$$\begin{aligned} F &\to F_P \cup \{\infty\} \\ z &\mapsto \begin{cases} z + P & \text{if } z \in \mathcal{O}_P \\ \infty & \text{if } z \notin \mathcal{O}_P. \end{cases} \end{aligned}$$

Homework 3.1. $\mathcal{O}_{p(x)}/P_{p(x)} \cong \mathbb{C}$ for $p(x) = x^2 + 1 \in \mathbb{R}[x]$.

Since we are dealing with valuations over K, for every P we have $K \cap P = \{0\}$. As a result, the composition of $K \subseteq \mathcal{O}_P$ and the map $\mathcal{O}_P \twoheadrightarrow F_P$ above, K injects into F_P. We define the degree of P as the degree of this field extension:

$$\deg P = [F_P : K].$$

If $\deg P = 1$ then P is called a *rational place.*

Lemma 3.2. *If $z \in P$ is nonzero, then $[F : K(z)]$ is finite.*

Proof. As $z \in P$ and nonzero, we know that $v(z) \neq 0$ and by Proposition 3.1, we have $z \notin \tilde{K}$. In particular, z is transcendental over K, so both F and $K(z)$ have transcendence degree 1 over K; hence, $[F : K(z)]$ is finite. □

Lemma 3.3. $[F_P : K] \leq [F : K(z)]$.

Proof. Suppose $z_1(P), \ldots, z_r(P) \in F_P$ are linearly independent where $z_1, \ldots, z_r \in \mathcal{O}_P$. If we can show that $z_1, \ldots, z_r$ are linearly independent over $K(z)$, then we are done.

Let

$$\varphi_1(z)z_1 + \cdots + \varphi_r(z)z_r = 0$$

for some $\varphi_1, \ldots, \varphi_r \in K(z)$. Multiplying by a common denominator and modding out the common z factors, we can take $\varphi_1, \ldots, \varphi_r \in K[z]$ not all divisible by z. Let $\varphi_i(z) = a_i + zg_i(z)$ with $a_i \in K$ and $g_i \in K[z]$. Evaluating the linear relation at P,

$$\varphi(P) + z_1(P) + \cdots + \varphi_r(P)z_r(P) = a_1z_1(P) + \ldots a_rz_r(P) = 0.$$

As $z_1(P), \ldots, z_r(P)$ are K-linearly independent, all $a_i = 0$. Contradiction. □

Proposition 3.4. $[F_P : K]$ *is always finite.*

Proof. Apply Lemmas 3.2 and 3.3. □

Corollary 3.5. $[\tilde{K} : K]$ *is finite.*

Proof. The degree $[F_P : K]$ is finite for any $P \in \mathbb{P}_F$ and $K \subseteq \tilde{K} \subseteq \mathbb{P}_F$. □

Corollary 3.6. *If there is one rational place on F, then $\tilde{K} = K$.*

For $z \in F$ and $P \in \mathbb{P}_F$ with $v_P(z) = n$, if $n > 0$ we say z has a zero of order n at P, and if $n < 0$ we say z has a pole of order n at P.

References

[1] Rosen, M. *Number theory in function fields*, vol. 210. Springer Science & Business Media, 2002.

[2] Stichtenoth, H. *Algebraic function fields and codes*, vol. 254. Springer Science & Business Media, 2009.