

## Divisibility theory for ideals

Let  $R$  to be a commutative unitary ring.

A non-zero non-unit element is said to be **irreducible** if it is not a product of 2 non-units.

**Be careful!** Irreducible element should not be confused with prime element.

A non-zero non-unit element  $a$  in  $R$  is called **prime** if whenever  $a|bc$  for some  $b$  and  $c \in R$ , then  $a|b$  or  $a|c$ .

In integral domain, every prime element is irreducible but the converse is not true in general. The converse is true for GCD domain (where every non-zero elements have greatest common divisor). A UFD domain is a GCD domain which is noetherian.

Moreover while an ideal generated by a prime element is a prime ideal it is not true in general that an ideal generated by an irreducible ideal.

However, if  $R$  is a GCD domain and  $x$  is an irreducible element of  $R$  then the ideal generated by  $x$  is an irreducible ideal of  $R$ .

We want to understand the theory of divisibility in any ring of integer of some extension of  $\mathbb{Q}$  for instance, a good theory of divisibility we need to know what are the "minimal" generator and a unique decomposition through them on this ring in relation to the divisibility operation so we need a UFD domain, we need to understand the units. Note that the "prime property" is essential to the study of the divisibility theory on  $\mathbb{Z}$ . The problem is that already in a quadratic integer ring like  $K = \mathbb{Z}[\sqrt{-5}]$ , it can be shown using norm arguments that the number 3 is irreducible. However, it is not prime in this ring. Since, for example,  $3|(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$  but 3 does not divide either of the 2 factors. Also

$$21 = 3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

All this factor occurs to be irreducible in  $\mathbb{Z}[\sqrt{-5}]$ . Thues we have 2 prime decomposition different up to associated.

As a consequence, even if one could know the prime of  $\mathcal{O}_K$  thanks to the ones of  $\mathbb{Z}$ , this would not be enough to understand the arithmetic of  $\mathcal{O}_K$ .

The ideal was to consider the ideal instead of the element and the prime ideal could take the place of the prime number even if this theory is well-understood for Dedekind Domains. It turn out to bring very interesting aspect in general.

Let  $\mathfrak{a}, \mathfrak{b}$  be two ideals of  $B$ , one can define the product as:

$$\mathfrak{a}\mathfrak{b} = \{ \sum a_i b_i \mid a_i \in \mathfrak{a} \text{ and } b_i \in \mathfrak{b} \}$$

Note that  $(1) = R$ , and  $(1)\mathfrak{b} = \mathfrak{b}$ .

When  $\mathfrak{a} = \{0\}$ ,  $\mathfrak{a}\mathfrak{b} = \{0\}$ .

Note that in  $\mathbb{Z}$ , ideal are principal and if  $\mathfrak{a} = (a)$ ,  $\mathfrak{b} = (b)$  for some  $a, b \in \mathbb{Z}$ ,  $\mathfrak{a}\mathfrak{b} = (ab)$ .

We say that  $\mathfrak{a}$  divide  $\mathfrak{b}$  if  $\mathfrak{b} \subseteq \mathfrak{a}$ , we write  $\mathfrak{a} \mid \mathfrak{b}$ .

In  $\mathbb{Z}$ , then for any  $a, b \in \mathbb{Z}$

$$a \mid b \Leftrightarrow (a) \mid (b)$$

An ideal  $\mathfrak{p}$  in  $R$  is **prime** if

1.  $\mathfrak{p} \neq R$ ;
2. if  $a, b \in R$  and  $ab \in \mathfrak{p}$  then  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ .

In  $\mathbb{Z}$ , to be a prime  $p$  is characterize by  $p \neq 1$  (i.e  $(p) \neq R$ ) and for any  $a, b \in R$ ,

$$(p \mid a \Rightarrow p \mid a \text{ or } p \mid b) \Leftrightarrow (\mathfrak{p} \mid (ab) \Rightarrow \mathfrak{p} \mid (a) \text{ or } \mathfrak{p} \mid (b) \Rightarrow (p) \text{ is a prime ideal})$$

*Remember that  $\mathfrak{p}$  is a prime ideal if and only if  $\frac{R}{\mathfrak{p}}$  is an integral domain. In particular, a commutative ring is an integral domain if and only if  $\{0\}$  is a prime ideal.*

Prime ideals have also the following essential property satisfied by the prime number: Let  $\mathfrak{p}_i$  and  $\mathfrak{p}$  be prime ideals, where  $i = 1, \dots, n$ , if  $\mathfrak{p} \mid \mathfrak{p}_1 \dots \mathfrak{p}_n$  then  $\mathfrak{p} \mid \mathfrak{p}_i$  for some  $i$ . (Indeed, otherwise, for all  $i$ , there is  $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$  and  $a_1 \dots a_n \in \mathfrak{p}$ , which is a contradiction with the fact that  $\mathfrak{p}$  is a prime ideal).

A **maximal ideal** of  $R$  is a proper ideal  $\mathfrak{m}$  such that for any ideal  $\mathfrak{a}$  with  $\mathfrak{m} \mid \mathfrak{a}$  then either  $\mathfrak{a} = \mathfrak{m}$  or  $\mathfrak{a} = R$ .

In  $\mathbb{Z}$ , to be an irreducible element  $p$  is characterize by  $p \neq 1$  (i.e  $(p) \neq R$ ) and for any  $a, b \in R$ ,

$$(a \mid p \Rightarrow a = 1 \text{ or } a = p) \Leftrightarrow ((a) \mid \mathfrak{p} \Rightarrow \mathfrak{p} = (a) \text{ or } (a) = R \Rightarrow (p) \text{ is a maximal ideal})$$

*Remember that an ideal  $\mathfrak{m}$  is maximal if and only if  $R/\mathfrak{m}$  is a field.*

In particular, maximal ideals are also prime.

**Krull's theorem:** Each proper ideal of a commutative ring is contained in at least one maximal ideal.

In  $\mathbb{Z}$ , prime ideals corresponds exactly to ideals generated by prime elements. This is only true because  $\mathbb{Z}$  is a PID.

**GCD** We define the sum of two ideal to be

$$\mathfrak{a} + \mathfrak{b} = \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

This corresponds to the notion of GCD for any  $a, b \in \mathbb{Z}$ ,  $(a) + (b) = (gcd(a, b))$ .

We say that  $\mathfrak{a}$  and  $\mathfrak{b}$  are two ideals are **relatively coprime** if  $(1) = \mathfrak{a} + \mathfrak{b}$ .

**LCM** We now consider the intersection of two ideal  $\mathfrak{a}, \mathfrak{b}$ ,

$$\mathfrak{a} \cap \mathfrak{b} = \{a | a \in \mathfrak{b} \text{ and } a \in \mathfrak{a}\}$$

In  $\mathbb{Z}$ , note that  $\forall a, b \in \mathbb{Z}$ ,  $(a) \cap (b) = (lcm(a, b))$ .

**Operations on ideals** Let  $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$  ideals of  $R$ . Then

1.  $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$
2.  $\mathfrak{a} \subseteq \mathfrak{b}$  or  $\mathfrak{c} \subseteq \mathfrak{b}$ , then  $\mathfrak{b} \cap (\mathfrak{a} + \mathfrak{c}) = \mathfrak{b} \cap \mathfrak{a} + \mathfrak{b} \cap \mathfrak{c}$ .
3. If  $\mathfrak{a} + \mathfrak{b} = R$ , then  $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ .

**Theoreme:** Let  $\mathfrak{a}_1, \dots, \mathfrak{a}_n$  be ideal in  $R$  such that  $\mathfrak{a}_i + \mathfrak{a}_j = R$ , if  $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_n$ , we define a map

$$\begin{aligned} \phi : \frac{R}{\mathfrak{a}} &\rightarrow \frac{R}{\mathfrak{a}_1} \oplus \dots \oplus \frac{R}{\mathfrak{a}_n} \\ a &\mapsto (a + \mathfrak{a}_1, \dots, a + \mathfrak{a}_n) \end{aligned}$$

When  $R$  is noetherian, for every ideal  $\mathfrak{a} \neq 0$  of  $R$ , there exist nonzero prime ideal  $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$  such that  $\mathfrak{p}_1 \dots \mathfrak{p}_r | \mathfrak{a}$ .

## In Dedekind domain

For an integral domain  $R$  which is not a field, all of the following conditions are equivalent:

1. Every nonzero proper ideal factors into primes.
2.  $R$  is Noetherian, and the localization at each maximal ideal is a Discrete Valuation Ring.
3. Every fractional ideal of  $R$  is invertible.
4.  $R$  is an integrally closed, Noetherian domain with Krull dimension one (i.e., every nonzero prime ideal is maximal).

Suppose now on that  $R$  is a Dedekind domain. Denote by  $K$  its fraction field.

1. The fractional ideals (i.e. finitely generated submodule of  $K$ ) form an abelian group, the ideal group  $J_K$  of  $K$ . The identity element (1) and the inverse of  $\mathfrak{a}$  is

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq R\}$$

(i.e.  $\mathfrak{a}\mathfrak{a}^{-1} = (1)$ )

2.  $\mathfrak{a} | \mathfrak{b}$  if and only if there is an ideal  $\mathfrak{c}$  such that  $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ .
3. Every fractional ideals  $\mathfrak{a}$  of  $K$  different from (0) or (1) admits a unique factorization

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}$$

into nonzero prime ideal  $\mathfrak{p}_i$  of  $R$  which is unique up to the order of the factors.

4. For any ideals  $\mathfrak{a}, \mathfrak{b}$  of  $R$ ,

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$$

5. The class group  $Cl_K = J_K/P_K$  fits inside the exact sequence:

$$1 \rightarrow R^* \rightarrow K^* \rightarrow J_K \rightarrow Cl_K \rightarrow 1$$

(When  $K$  is a number theory, the class group  $Cl_K$  is finite and the group of units  $\mathcal{O}_K^*$  is the direct product of the finite cyclic group  $\mu(K)$  and a free abelian group of rank  $r + s - 1$  where  $r$  is the number of real embedding and  $s$  the number of complex embedding.)

6. Given  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  prime ideals. Taking  $\pi_i \in \mathfrak{p}_i^{r_i} \setminus \mathfrak{p}_i^{r_i+1}$ , by CRT there is  $x \in A$  such that

$$x \equiv \pi_i \pmod{\mathfrak{p}_i^{r_i}}, \text{ for any } i$$

That is  $(x) = \prod_{i=1}^n \mathfrak{p}_i^{r_i} \mathfrak{a}$  with  $\mathfrak{a}$  coprime with  $\mathfrak{p}_i$  for any  $\mathfrak{p}_i$ . In other words,  $v_{\mathfrak{p}_i}$  is exactly  $r_i$  in  $(x)$

7. if  $\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$  and  $\mathfrak{b} = \prod_i \mathfrak{p}_i^{f_i}$  where the  $\mathfrak{p}'$ s are maximal ideal, then

$$\mathfrak{a} + \mathfrak{b} = \prod_i \mathfrak{p}_i^{\min(e_i, f_i)} \text{ and } \mathfrak{a} \cap \mathfrak{b} = \prod_i \mathfrak{p}_i^{\max(e_i, f_i)}.$$

Note that  $\mathfrak{a} + \mathfrak{b}$  is the smallest ideal containing  $\mathfrak{a}$  and  $\mathfrak{b}$  and  $\mathfrak{a} \cap \mathfrak{b}$  is the smallest ideal contained in  $\mathfrak{a}$  and  $\mathfrak{b}$ . The results follows then from the fact, that  $\prod_i \mathfrak{p}_i^{e_i} \subseteq \prod_i \mathfrak{p}_i^{f_i}$  if and only if  $e_i \geq f_i$ , for all  $i$ .

8. For any prime ideal  $\mathfrak{p}$  of  $R$ , and  $R \subseteq B$  Dedekind domain, one always has

$$\mathfrak{p}B \neq B$$

(Indeed, let  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  ( $\mathfrak{p} \neq 0$ ), so that  $\pi R = \mathfrak{p}\mathfrak{a}$  with  $\mathfrak{p} \nmid \mathfrak{a}$ , hence  $\mathfrak{p} + \mathfrak{a} = R$ . Writing  $1 = b + s$ , with  $b \in \mathfrak{p}$  and  $s \notin \mathfrak{p}$  and  $s\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{a} = \pi R$ . If one had  $\mathfrak{p}B = B$ , then it would follow that  $sB = s\mathfrak{p}B \subseteq \pi B$ , so that  $s = \pi x$ , for some  $x \in B \cap K = R$ , i.e.  $s \in \mathfrak{p}$ , a contradiction)

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

where  $\mathfrak{P}_i$  are the prime ideal over  $\mathfrak{p}$  (i.e.  $\mathfrak{p} = \mathfrak{P}_i \cap R$ ).

Now, if  $K$  is the fraction field of  $R$  and  $B$  is the integral closure of  $K$  in some finite extension  $L$ , we denote by  $f_i = [B/\mathfrak{P}_i : R/\mathfrak{p}]$  the inertia degree. If  $L/K$  separable, we have the fundamental identity

$$\sum_{i=1}^r e_i f_i = n$$

## Ramification

Let  $K$  the fraction field of a Dedekind ring  $A$ ,  $L/K$  a finite extension and  $B$  the algebraic closure of  $A$  on  $L$ .

Suppose that  $L/K$  is separable given by a primitive element  $\theta \in B$  with minimal polynomial

$$p(X) \in A[X]$$

So that  $L = K(\theta)$ . Denote by  $\mathcal{F}$  the conductor of  $A[\theta]$  the biggest ideal  $\mathcal{F}$  of  $B$  which is contained in  $A[\theta]$ .

$$\mathcal{F} = \{\alpha \in B | \alpha B \subseteq A[\theta]\}$$

Let  $\mathfrak{p}$  be a prime ideal of  $A$  which is relatively prime to the conductor  $\mathcal{F}$  of  $A[\theta]$  and let  $\bar{p}(X) = \bar{p}_1(X)^{e_1} \dots \bar{p}_r(X)^{e_r}$  be the factorization of  $p(x) \bmod \mathfrak{p}$  into irreducible  $\bar{p}_i(X) \equiv p_i(X) \bmod \mathfrak{p}$ , with all  $p_i(x) \in A[x]$  monic. Then

$$\mathfrak{P}_i = \mathfrak{p}B + p_i(\theta)B, \quad i = 1, \dots, r$$

are the different prime ideals of  $B$  above  $\mathfrak{p}$ . The inertia degree  $f_i$  of  $\mathfrak{P}_i$  is the degree of  $\bar{p}_i(X)$  and one has  $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ .

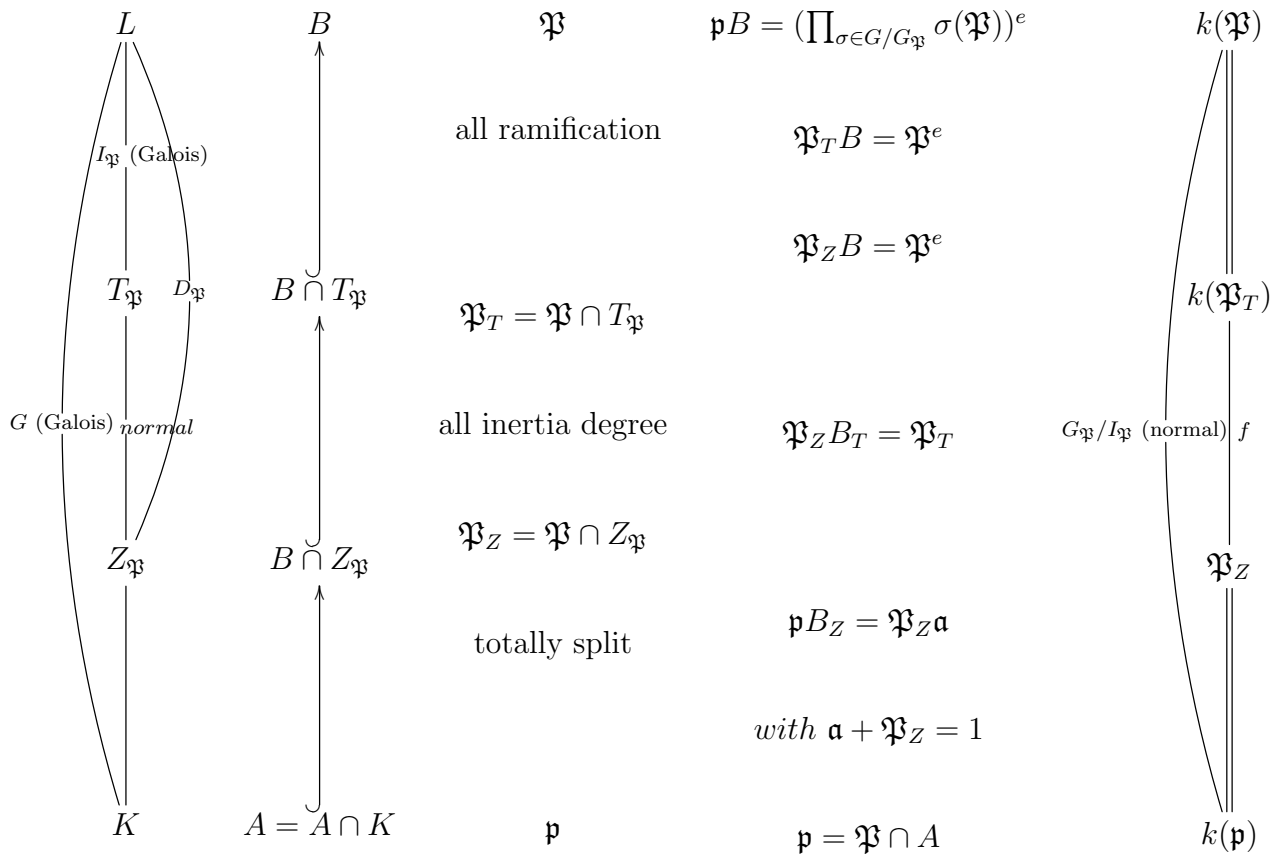
Let  $\mathfrak{p}$  be a prime of  $A$ , such that  $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$  is the prime decomposition of  $\mathfrak{p}B$ . The prime  $\mathfrak{p}$  is said to:

1. **split completely** (or **totally split**) in  $L$  if  $r = n = [L = K]$  (so that  $e_i = f_i = 1$ , for any  $i$ )
2. **non split** (or **in decomposed**) if  $r = 1$  (i.e. there is one single prime ideal of  $L$  over  $\mathfrak{p}$ ).
3. **unramified** if all  $\mathfrak{P}_i$  are unramified, that is  $e_i = 1$  and  $k(\mathfrak{P}_i)/k(\mathfrak{p})$  is separable, otherwise it is said ramified.

There are only finitely of prime ideal which are ramified in  $L$ .

# Hilbert ramification theory

Let  $\mathfrak{p}$  be a prime ideal of  $A$  and  $\mathfrak{P}$  be a prime of  $B$  above  $\mathfrak{p}$ . We suppose that  $L/K$  is Galois of Galois group  $G$  and  $|G| = [L : K] = n$ . Let  $S$  be a set of representative of the coset in  $G/G_{\mathfrak{P}}$ . Let  $e$  be the index of ramification of  $\mathfrak{p}$  and  $f$  its inertia degree.



## Cyclotomic field

Let  $K = \mathbb{Q}(\zeta)$  with  $\zeta$  a primitive  $n^{th}$  root of unity,  $K$  is called a Cyclotomic field.  $\mathcal{O}_K = \mathbb{Z}[\zeta]$  is the ring of the integer of  $K$  and  $1, \zeta, \dots, \zeta^{\phi(n)}$  where  $\phi(n)$  is the Euler function evaluated at  $n$ .

Let  $n = \prod_p p^{v_p}$  be the prime factorization of  $n$  and, for even prime number  $p$ , let  $f_p$  be the smallest positive integer such that

$$p^{f_p} \equiv 1 \pmod{n/p^{v_p}}$$

Then one has the factorization

$$p\mathbb{Z}[\zeta] = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^{\phi(p^{v_p})}$$

where  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  are distinct prime ideals, all of degree  $f_p$ .

A prime  $p$  is ramified if and only if  $n \equiv 0 \pmod p$  except in the case where  $p = 2 = (4, n)$ .

A prime number  $p \neq 2$  is totally split in  $\mathbb{Q}(\zeta)$  if and only if  $p \equiv 1 \pmod n$ .

Let  $\xi$  a primitive  $q$ -root of unity, let  $q^* = (-1)^{\frac{q-1}{2}} q$  then  $q^* = \tau^2$  where

$$\tau = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left(\frac{a}{q}\right) \xi^a$$

so that

$$\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta)$$