UFRJ

Notes in Algebraic Number Theory

Kevin Alves Vasconcellos

These notes were written during the course of Algebraic Number Theory in first semester of 2023 at Federal University of Rio de Janeiro. The course was based essentially on the J. Neukirch's book *Algebraic Number Theory*. I hope this material may be useful for you. If you find some error or some important misprint, please feel free to contact me.

Kevin Alves Vasconcellos[1]

[1] M.Sc in Mathematics // E-mail: kevin.vasconcellos@ufrj.br // Webpage: `www.im.ufrj.br/alunos/kevinvasconcellos`

Contents

Chapter 1

Preliminaries

1.1 The Fermat's Last Theorem

Theorem 1.1 (The Fermat's Last Theorem)**.** *Given $n \in \mathbb{N}$ an integer number greater than 2. There are no integers $x,\ y,\ z \in \mathbb{N}^+$ such that*

$$x^n + y^n = z^n.$$

The proof of this result is very sophisticated. The purpose of this section is to show we can suppose without lost generality some weaker conditions in order to prove this theorem.

Proposition 1.2. *In order to prove the Fermat's last theorem, it is enough to prove that it holds when* $\gcd(x, y, z) = 1$.

$$x^n + y^n = z^n.$$

Proof: In fact suppose that FLT is false. Thus there are $x,\ y,\ z \in \mathbb{N}^+$ such that $x^n + y^n = z^n$ for some $n \geq 3$. Considering $d = \gcd(x, y, z)$ and denoting $x = dx'$, $y = dy'$ and $z = dz'$, we obtain that

$$(dx')^n + (dy')^n = (dz')^n,$$

which implies that $x'^n + y'^n = z'^n$ and $\gcd(x', y', z') = 1$. This means that, if the FLT holds when $\gcd(x, y, z) = 1$, then certainly it holds on general case. $\square$

Proposition 1.3. *In order to prove the Fermat's last theorem, it is enough to prove that it holds for $n = 4$ and n odd prime integer.*

Proof: In fact suppose that FLT is false. Thus there are $x,\ y,\ z \in \mathbb{N}^+$ such that $x^n + y^n = z^n$ for some $n \geq 3$. If n is an odd number, then there exists an odd prime number p such that $n = mp$. Hence

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

If the FLT holds when n is an odd prime integer, then certainly it holds when n is odd. On the other hand, if n is even, then there are two cases: $n = 2m$, where m is an odd integer or $m = 4m$, where m is an integer. On the first case, we have $n = 2m'p$, where p is an odd prime number and the problem coincides with the previous case. If $n = 4m$, then

$$(x^m)^4 + (y^m)^4 = (z^m)^4.$$

If the FLT holds when $n = 4$, then certainly it holds when n is of form $n = 4m$. □

1.2 Localization

Definition 1.4. *Let R be a ring. A subset $S \subseteq R$ is said multiplicatively closed if*

- *S is closed under multiplication;*
- *$1 \in S$;*
- *$0 \notin S$.*

Let R be a ring, $S \subset R$ a multiplicatively closed subset. Define the following relation on $R \times S$: $(x, s) \sim (y, t)$ if and only if there is $z \in S$ such that $z(tx - sy) = 0$. It is easy to show that relation is an equivalence relation. Denote by x/s a representant element of equivalence class $[(x, s)]$ and denote by R_S the family of all equivalence classes. That is

$$R_S = \{x/s\ ;\ x \in R,\ s \in S\}.$$

Define the following binary operations

$$\begin{aligned} + : R_S \times R_S &\longrightarrow R_S & \qquad \cdot : R_S \times R_S &\longrightarrow R_S \\ (x/s, y/t) &\longmapsto (tx + sy)/(st) & (x/s, y/t) &\longmapsto (xy)/(st) \end{aligned}$$

It is easy to show these operations are well-defined and that $(R_S, +, \cdot)$ is a ring. Moreover there exists a natural ring homomorphism

$$\phi : R \longrightarrow R_S$$
$$x \longmapsto x/1.$$

Proposition 1.5. *Let R be a ring, $S \subset R$ a multiplicatively closed subset. If R is an integral domain, then so does R_S. Moreover, the natural ring homomorphism $\phi : R \longrightarrow R_S$ is one-to-one. In particular, R can be considered as a subring of R_S.*

Proof: Indeed let x/s and y/t be elements of R_S and suppose that $x/s \cdot y/t = (xy)/(st) = 0$. So there is $z \in S$ such that $zxy = 0$. As R is an integral domain and $z \neq 0$, one has $x = 0$ or $y = 0$, which implies that $x/s = 0$ or $y/t = 0$.

Now let $x \in R$ such that $\phi(x) = x/1 = 0$. So there is $s \in S$ such that $sx = 0$. As R is an integral domain and $s \neq 0$, one has $x = 0$, so the ring homomorphism is injective. □

Example 1.6. *Let R be a ring.*

(i): Given $\mathfrak{p} \in \operatorname{Spec}(R)$, the set $S = R \setminus \mathfrak{p}$ is multiplicatively closed and we denote by $R_\mathfrak{p}$ the localization of R in S. The ring $R_\mathfrak{p}$ is local, that is, it contains only one maximal ideal, namely $\mathfrak{p}R_\mathfrak{p}$;

(ii): If R is an integral domain, then the zero ideal is prime, thus $\operatorname{Quot}(R) = R_{(0)}$ is a field and is called total field of fractions of R.

Proposition 1.7 (Universal property of localization)**.** *Let R, B be rings, $S \subset R$ be a multiplicatively closed set and $f : R \longrightarrow B$ a ring homomorphism. If f takes each element of S in unity elements of B, then there is a unique $g : R_S \longrightarrow B$ such that the following diagram commutes*

$$\begin{tikzcd} & R_S \arrow[dr, "g"] & \\ R \arrow[ur, "\phi"] \arrow[rr, "f"] & & B \end{tikzcd}$$

Proof: Indeed define the map $g : R_S \longrightarrow B$ such that $g(x/s) = f(x)f(s)^{-1}$. It is easy to see that g is a well-defined ring homomorphism and clearly one has $g \circ \phi = f$. Now let $h : R_S \longrightarrow B$ be other ring homomophism which makes the diagram commute. Given $x/s \in R_S$, one has

$$x/s = (x/1)(1/s).$$

By commutativity of diagram, it holds that $h(x/1) = f(x)$. Moreover, since $1 = s/s = (s/1)(1/s)$, one has $1 = h(s/1)h(1/s)$, which implies that $h(1/s) = f(s)^{-1}$. Hence

$$h(x/s) = h((x/1)(1/s)) = h(x/1)h(1/s) = f(x)f(s)^{-1}.$$

Thus g exists and is unique. □

Corollary 1.8. *Let $S \subseteq T$ multiplicatively subsets of a ring R. Then there exists a unique ring homomorphism $\psi : R_S \longrightarrow R_T$ which makes the following diagram commute*

$$\begin{tikzcd}
& R_S \arrow[dr, "\psi"] & \\
R \arrow[ur, "\phi_S"] \arrow[rr, "\phi_T"] & & R_T
\end{tikzcd}$$

Moreover if R is an integral domain, then ψ is injective.

Proof: Indeed the ring homomorphism $\phi_T : R \longrightarrow R_T$ takes every element of S in unity elements of R_T. So it is enough to use the universal property. Moreover, it is easy to see that ψ is of form

$$\psi(x/s) = x/s.$$

Suppose that $\psi(x/s) = x/s = 0$, thus there exists $t \in T$ such that $tx = 0$, which implies that $x = 0$, because R is domain. Hence $x/s = 0$. □

In particular for any $S \subset R$ multiplicatively closed subset of a domain integral R, one has

$$R \subseteq R_S \subseteq \mathrm{Quot}(R).$$

The total field of fractions of a domain R is the smallest field containing R as we will see on the next proposition.

Proposition 1.9. *Let R be an integral domain and K be a field containing R Then there exists a field homomorphism $\psi : \mathrm{Quot}(R) \longrightarrow K$, which makes the following diagram commute.*

$$\begin{tikzcd}
& \mathrm{Quot}(R) \arrow[dr, "\psi"] & \\
R \arrow[ur, "\phi"] \arrow[rr, "i_K"] & & K
\end{tikzcd}$$

Proof: Remember that $\mathrm{Quot}(R) = R_S$, where $S = R \setminus \{0\}$. As $i_K(S) \subseteq K^\times$, by universal property, there is $\psi : \mathrm{Quot}(R) \longrightarrow K$ which makes the diagram commute. Since ψ is a non-zero ring homomorphism between fields, ψ is injective, thus one can consider $\mathrm{Quot}(R)$ as subfield of K. □

1.3 Adjoint Matrix

Definition 1.10. *Let R be a ring and $A = [a_{ij}]$ be an $n \times n$ matrix com coefficients in R. Consider A_{ij} the determinant of the $(n-1) \times (n-1)$ matrix obtained by deleting the i-th row of A and the j-th column of A. Define $M_{ij} = (-1)^{i+j} A_{ij}$ the (i,j)-cofactor of A and let $C = [M_{ij}]$ be the matrix of cofactors of A. The adjoint matrix of A is defined as*

$$\operatorname{adj}(A) = C^T,$$

that is, it is the transpose of cofactors matrix of A.

Proposition 1.11. *Let R be a ring and $A = [a_{ij}]$ be an $n \times n$ matrix com coefficients in R. Then*

$$A \operatorname{adj}(A) = \operatorname{adj}(A) A = \det(A) I_n,$$

where I_n is the $n \times n$ identity matrix.

Proof: Indeed Calling $A \operatorname{adj}(A) = [c_{ij}]$, observe that

$$c_{ij} = \sum_{k=1}^{n} a_{ik} [\operatorname{adj}(A)]_{kj} = \sum_{k=1}^{n} (-1)^{k+j} a_{ik} A_{jk}$$

Using the Laplace expansion formula, observe that if $i = j$, then $c_{ij} = \det(A)$. On other hand, if $i \neq j$, c_{ij} is the determinant of matrix whose i-th row and j-th are equal, thus $c_{ij} = 0$. Hence $c_{ij} = \det(A) \delta_{ij}$, which implies that $A \operatorname{adj}(A) = \det(A) I_n$. The proof of the $\operatorname{adj}(A) A = \det(A) I_n$ is similar. □

1.4 Free modules

Let R be a ring and M a finitely generated R-module. M is said free if there is generating set $\{m_1, \ldots, m_n\}$ of M with the following property: Given $a_1, \ldots, a_n, b_1, \ldots, b_n \in R$, then

$$\sum_{k=1}^{n} a_k m_k = \sum_{k=1}^{n} b_k m_k$$

if and only if $a_1 = b_1,\ a_2 = b_2, \ldots, a_n = b_n$.

Proposition 1.12. *Let R be a ring and M a finitely generated R-module. Then M is free if and only if $M \cong R^n$ for some $n \in \mathbb{N}$. In this case, one says that* $\operatorname{rank}(M) = n$.

Proof: Suppose that M is a free module with $\text{rank}(M) = n$ and let $\{m_1, \ldots, m_n\}$ a basis for M. Define the mapping $\phi : M \longrightarrow R^n$ such that

$$\phi\left(\sum_{k=1}^{n} a_k m_k\right) = (a_1, \ldots, a_n)$$

Since $\{m_1, \ldots, m_n\}$ is a basis, ϕ is well-defined and is one-to-one. Moreover, it is clear that ϕ is surjective. Then ϕ is an R-module isomorphism. □

1.5 Restriction of scalars

Definition 1.13. *Let R, S be rings, $f : R \longrightarrow S$ a ring homomorphism and M a S-module. The module M has a natural structure of R-module defining the following binary operation*

$$\cdot : R \times M \longrightarrow M$$

$$(r, m) \longmapsto f(r)m$$

Note this operations satisfies the following properties

(i): $(rs) \cdot m = f(rs)m = (f(r)f(s))m = f(r)(f(s)m) = r \cdot (f(s)m) = r \cdot (s \cdot m)$ for all $r, s \in R$ and $m \in M$;

(ii): $1_R \cdot m = f(1_R)m = 1_B m = m$ for all $r \in R$ and $m \in M$;

(iii): $(r + s) \cdot m = f(r + s)m = (f(r) + f(s))m = f(r)m + f(s)m = r \cdot m + s \cdot m$ for all $r, s \in R$ and $m \in M$;

(iv): $r \cdot (m + n) = f(r)(m + n) = f(r)m + f(r)n = r \cdot m + r \cdot n$ for all $r \in R$ and $m,\ n \in M$.

This process is called by restriction of scalars.

Proposition 1.14. *Let R, S be rings, $f : R \longrightarrow S$ a ring homomorphism and M, N S-modules. Let $g : M \longrightarrow N$ be homomorphism of S-modules and consider h the underlying map g as morphism of sets. Then h is a homomorphism of R-modules by restricting scalars.*

Proof: It is clear that, given $m, n \in M$, then

$$h(m + n) = g(m + n) = g(m) + g(n) = h(m) + h(n).$$

Now let $r \in R$ and $m \in M$. Then

$$h(r \cdot m) = g(r \cdot m) = g(f(r)m) = f(r)g(m) = r \cdot g(m) = r \cdot h(m).$$

Hence h is a R-module homomorphims. □

Example 1.15. *Let $R \subseteq S$ be rings and M a S-module. Then M has a natural structure of R-module if one considers the inclusion homomorphism $i : R \longrightarrow S$.*

1.6 Torsion

Definition 1.16. *Let R be an integral domain and M an R-module. An element $m \in M$ is said a torsion element if there is $x \neq 0$ in R such that $xm = 0$.*

Proposition 1.17. *Let R be an integral domain and M an R-module. Define*

$$T(M) = \{m \in M \ ; \ m \textit{ is a torsion element of } M\}.$$

Then $T(M)$ is a submodule of M.

Proof: Indeed it is easy to see that $0 \in T(M)$. Let m_1, $m_2 \in T(M)$, so there are $x_1, x_2 \in R \setminus \{0\}$ such that $x_1m_1 = x_2m_2 = 0$. Observe that

$$(x_1x_2)(m_1 - m_2) = x_2(x_1m_1) - x_1(x_2m_2) = 0.$$

As $x_1x_2 \neq 0$, because R is an integral domain, then $m_1 - m_2 \in T(M)$, hence $T(M)$ is a submodule of M. □

Definition 1.18. *Let R be an integral domain. A R-module M is said torsion free if $T(M) = \{0\}$, that is, for all $x \in R$ and $m \in M$, the vanishing of xm implies on $x = 0$ or $m = 0$.*

Definition 1.19. *Let R be an integral domain. Every free module is torsion free.*

Proof: Let M be a finitely generated free module and $\mathcal{B} = \{m_1, \ldots, m_n\}$ a basis of M. Let $m = \sum_{k=1}^{n} a_km_k$ a torsion element of M and let $r \in R \setminus \{0\}$ such that $rm = 0$. Thus

$$rm = \sum_{k=1}^{n}(ra_k)m_k = 0 = \sum_{k=1}^{n} 0m_k.$$

As $\mathcal{B}$ is basis for M, one has that $ra_1 = \cdots = ra_n = 0$. As $r \neq 0$ and R is integral domain, one concludes that $a_1 = \cdots = a_n = 0$ and so $m = 0$. □

Example 1.20. *Consider the rings inclusion $R \subseteq L$, where L is a field. Observe that R is an integral domain and L is an R-module. Let $M \subseteq L$ such that M is an R-submodule of L. Then M is torsion free. Indeed let $r \in R$ and $m \in M \setminus \{0\}$ such that $rm = 0$. As $rm \in L$ and $rm = 0$, one has that $r = 0$.*

Proposition 1.21. *Let $R \subseteq L$ be rings such that L is a field, V a linear space over L and $x_1, \ldots, x_n$ elements of V.*

(i) If $\mathcal{B} := \{x_1, \ldots, x_n\}$ is linearly independent over L, Then $\mathcal{B}$ is linearly independent over R.

(ii) Suppose that $L = \mathrm{Quot}(R)$. If $\mathcal{B}$ is linearly independent over R, Then $\mathcal{B}$ is linearly independent over L.

Proof: (i) : Suppose that $\mathcal{B}$ is linearly dependent over R, then there are $r_1, \ldots, r_n \in R$ not all null such that $r_1m_1 + \cdots r_nm_n = 0$. Since $R \subseteq L$, one concludes that $\mathcal{B}$ is L.D. over L.

(ii) : Suppose that $\mathcal{B}$ is linearly dependent over L, then there are $\alpha_1, \ldots, \alpha_n \in L$ not all null such that

$$\alpha_1m_1 + \cdots \alpha_nm_n = 0.$$

As $L = \mathrm{Quot}(R)$, there are $a_1, \ldots, a_n \in R$ not all null and $b_1, \ldots, b_n \in R \setminus \{0\}$ such that $\alpha_i = a_i/b_i$ for all $i = 1, \ldots, n$. Setting $c_i = b_1 \cdots b_{i-1}b_{i+1} \cdots b_n \neq 0$, one has

$$(c_1a_1)m_1 + \cdots + (c_na_n)m_n = 0$$

Thus $\mathcal{B}$ is linearly dependent over R. □

Example 1.22. *Consider $\mathbb{Z} \subset \mathbb{R}$. Note $\{1, \sqrt{2}\}$ is linearly independent over $\mathbb{Z}$, but not over $\mathbb{R}$. This fact holds because* $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}\mathbb{R}$.

1.7 Finitely generated modules over PIDs

Theorem 1.23. *Let R be a PID and M be a finitely generated R-module. If M is torsion free, then $M \cong R^n$ for some $n \in \mathbb{N}$.*

Theorem 1.24. *Let R be a PID and M be a finitely generated R-module. If N is a submodule of M, then N is free.*

1.8 Field extensions and Galois theory

Let $K \subseteq L$ be fields. Then L can be seen as an algebra over K. In particular, L is a vector space over K. One can say that L is a field extension of K, or, equivalently, that K is a subfield of L. One denotes this field extension as L/K.

Definition 1.25. *Let $K \subseteq L$ be a field extension.*

(i): The degree of extension of L/K, denoted by $[L : K]$, is the dimension of L as K-vector space. One says that this field extension is finite if its degree is finite, that is, if $\dim_K L < \infty$.

(ii): An element $\alpha \in L$ is said algebraic over K if there is a non-constant polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$.

(iii): The extension L/K is said algebraic if every element of L is algebraic over K.

Proposition 1.26. *Let L/K be a field extension. If L/K is finite, then L/K is algebraic.*

Proof: If $[L : K] = 0$, then $L = K$ and this field extension is trivially algebraic. Thus suppose $[L : K] = n \geq 1$. Given $\alpha \in L$, note that $\{1, \alpha, \ldots, \alpha^n\}$ is a subset of L containing $n+1$ elements, so it is linearly dependent over K. Thus there are $a_0, \ldots, a_n \in K$ not all null such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Considering the polynomial $f(x) = \sum_{k=0}^{n} a_k x^k$, observe that $f(x) \in K[x]$ is non-zero and non-constant and $f(\alpha) = 0$, so α is algebraic over K. □

Let L/K be a field extension and $\alpha \in L$ be algebraic over K. Consider the family

$$\Sigma = \{p(x) \in K[x] \ ; \ p(x) \neq 0 \text{ and } p(\alpha) = 0\}.$$

We know that $\Sigma \neq$ by hypothesis and it is easy to see that there is an unique monic polynomial $p(x) \in \Sigma$ of smallest degree possible. Denote this polynomial by $\mathrm{Irr}_K^\alpha(x) \in K[x]$. Defining the ring homomorphism

$$\begin{aligned} \phi : K[x] &\longrightarrow L \\ p(x) &\longmapsto p(\alpha) \end{aligned},$$

one has that ϕ is a ring homomorphism whose image is $K[\alpha]$ and kernel is generated by $\mathrm{Irr}_K^\alpha(x)$. Since $(\mathrm{Irr}_K^\alpha(x))$ is a maximal ideal, one concludes that $K[\alpha] \cong K[x]/(\mathrm{Irr}_K^\alpha(x))$ is field, which contains K as subfield. Moreover, setting $n = \deg(\mathrm{Irr}_K^{\alpha}(x))$, then $K[\alpha]/K$ is an algebraic extension of degree n and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ constitutes a basis for $K[\alpha]/K$.

Definition 1.27. *Let L/K be a field extension. This extension is said simple if there is $\alpha \in L$ such that $L = K[\alpha]$.*

Proposition 1.28. *Let $F \subseteq K \subseteq L$ be a tower of fields. Then*

$$[L : F] = [L : K][K : F],$$

where we adopt $\infty \cdot 0 = 0 \cdot \infty = \infty$.

Proof: Suppose that $[L : K] = m$ and $[K : F] = n$. Let $\mathcal{B}_1 = \{\beta_1, \ldots, \beta_m\}$ basis of L as K-linear space and $\mathcal{B}_2 = \{\alpha_1, \ldots, \alpha_n\}$ basis of K as F-linear space. I claim that

$$\mathcal{B} = \{\beta_i \alpha_j \ ; \ 1 \leq i \leq m, \, 1 \leq j \leq n\}$$

is basis of L as F-linear space. It is simple to verify that $\mathcal{B}$ generates L as F-linear space. Let $a_{ij} \in F$, with $1 \leq i \leq m$, $1 \leq j \leq n$ such that

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} \alpha_j \right) \beta_i = \sum_{i,j} a_{ij} (\beta_i \alpha_j) = 0.$$

Thus, as $\mathcal{B}_1$ is basis of L as K-linear space, one has

$$\sum_{j=1}^{n} a_{ij} \alpha_j = 0$$

for all $1 \leq i \leq m$. Similarly, as $\mathcal{B}_1$ is basis of K as F-linear space, one has that $a_{ij} = 0$ for all $1 \leq i \leq m$, $1 \leq j \leq n$. Thus $\mathcal{B}$ is basis for L as F-linear space and so

$$[L : F] = \dim_F(L) = mn = [L : K][K : F].$$

□

Definition 1.29. *A field K is said algebraically closed if every polynomial non-constant $p(x) \in K[x]$ has a root in K. In particular, every non-constant polynomial $f(x) \in K[x]$ splits into linear factors in $K[x]$.*

Proposition 1.30. *Let F be a field. Then there a field extension $F \subseteq L$ such that L is algebraically closed. Moreover, setting*

$$K = \{x \in L \ ; \ x \textit{ is algebraic over } F\},$$

then K is also an algebraically closed field, is an algebraic extension of F and is unique up to F-isomorphism.

Definition 1.31. *Let L/K be a field extension. An element $\alpha \in L$ is said separable over K if*

- *α is algebraic over K;*
- *$\mathrm{Irr}_K^\alpha(x)$ is a separable polynomial, that is, it does not admit multiple roots.*

Proposition 1.32. *Let K be a field and $f(x) \in K[x]$ be a polynomial in $k[x]$. Then $f(x)$ is separable if and only if $\gcd\big(f(x), f'(x)\big) = 1$.*

Proof: Let L be a field extension of K, which contains all roots of $f(x)$. Then one knows that $f(x)$ splits into linear factors in $L[x]$. Suppose that $f(x)$ has multiple roots in $L[x]$, thus there is $\alpha \in L$ and $g(x) \in L[x]$ such that $f(x) = (x-\alpha)^2 g(x)$. Differentiating $f(x)$, one obtains

$$f'(x) = (x-\alpha)\big(2g(x) + (x-\alpha)g'(x)\big),$$

which implies that $f(x)$ and $f'(x)$ have a non-trivial common factor in $L[x]$. As

$$\gcd_{K[x]}\big(f(x), f'(x)\big) = \gcd_{L[x]}\big(f(x), f'(x)\big),$$

one concludes that $\gcd_{K[x]}\big(f(x), f'(x)\big) \neq 1$.

On the other hand, let F be the algebraic closure of K. It is simple to prove that $\gcd_{F[x]}\big(f(x), g(x)\big) = 1$ if and only if f, g have no common roots. As $\gcd_{K[x]}\big(f(x), g(x)\big) = \gcd_{F[x]}\big(f(x), g(x)\big)$, it is enough to show that if f is separable, then f and f' have no common roots. Let $\alpha \in F$ be a root of f, then $f(x) = (x-\alpha)g(x)$ for some $g(x) \in F[x]$ with $g(\alpha) \neq 0$. Differentiating $f(x)$, we obtain that

$$f'(x) = g(x) + (x-\alpha)g'(x).$$

Thus $f'(\alpha) = g(\alpha) \neq 0$, which implies that f and f' have no common roots. □

Corollary 1.33. *Let K be a field and $f(x) \in K[x]$ a polynomial. If $f(x)$ irreducible in K[x] and $f'(x) \neq 0$, then f is separable.*

Proof: Let $g(x) = \gcd\big(f(x), f'(x)\big)$. Since $g(x)$ divides $f(x)$ and $f(x)$ is irreducible, then $g(x) = 1$ or $g(x)$ is associated to $f(x)$. However, since $g(x)$ also divides $f'(x) \neq 0$, then $\deg(g(x)) \leq \deg(f'(x)) < \deg(f)$, which implies that $g(x)$ can not be associated to f, so $g(x) = 1$. By previous Proposition, one concludes that f is separable. □

Definition 1.34. *A field extension L/K is said separable if all element $\alpha \in L$ is separable over K. In particular, every separable extension is algebraic.*

Proposition 1.35. *Let K be a field of characteristic 0 and L/K a field extension. If L/K is algebraic, then L/K is separable.*

Proof: Indeed let $\alpha \in L$. Since L/K is algebraic, α is algebraic over K and let $\mathrm{Irr}_K^{\alpha}(x)$ be the polynomial minimal of α over K. Since $\mathrm{Irr}_K^{\alpha}(x)$ is irreducible and $\mathrm{Irr}_K^{\alpha,}(x) \neq 0$ because $\mathrm{char}(K) = 0$, then $\mathrm{Irr}_K^{\alpha}(x)$ is separable over K, which implies that α is separable over K. □

Proposition 1.36 (Primitive Element Theorem)**.** *Let L/K be a finite and separable extension, then there exists $\alpha \in L$ such that $L = K(\alpha)$.*

Proposition 1.37. *Let L/K be a finite and separable field extension and $K \subseteq C$, where C is an algebraically closed field, then*

$$|\operatorname{Hom}_K(L, C)| = [L : K]$$

More precisely let $\alpha \in L$ such that $L = K(\alpha)$, then the function

$$\phi : \operatorname{Hom}_K(L, C) \longrightarrow \{\beta \in C \ ; \ \mathrm{Irr}_K^{\alpha}(\beta) = 0\}$$

such that $\phi(f) = f(\alpha)$ is a bijection.

1.9 Norm and trace

Let L/K be a finite field extension. Given $\alpha \in L$, one has that

$$m_\alpha : L \longrightarrow L$$

$$x \longmapsto \alpha x$$

is an K-linear map, because for all x, $y \in L$ and $\lambda \in K$

$$m_\alpha(x+y) = \alpha(x+y) = \alpha x + \alpha y = m_\alpha(x) + m_\alpha(y),$$
$$m_\alpha(\lambda x) = \alpha(\lambda x) = \lambda(\alpha x) = \lambda m_\alpha(x).$$

Definition 1.38. *Let L/K be a finite field extension. The norm and the trace of extension L/K are defined as*

$$\mathrm{N}_{L/K} : L \longrightarrow K \qquad\qquad \mathrm{Tr}_{L/K} : L \longrightarrow K$$
$$\alpha \longmapsto \det(m_\alpha) \qquad\qquad \alpha \longmapsto \mathrm{Tr}(m_\alpha)$$

Proposition 1.39. *Let L/K be a finite field extension with $[L : K] = n$. Given α, $\beta \in L$ and $a \in K$, then*

(i): $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta)$;

(ii): $\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$;

(iii): $\mathrm{N}_{L/K} = a^n$;

(iv): $\mathrm{Tr}_{L/K}(a) = na$.

Proof: (i) : Observe that $m_{\alpha\beta} = m_\alpha \circ m_\beta$, thus $\det(m_{\alpha\beta}) = \det(m_\alpha)\det(m_\beta)$, which implies that

$$\mathrm{N}_{L/K}(\alpha\beta) = \det(m_{\alpha\beta}) = \det(m_\alpha)\det(m_\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta).$$

(ii) : Observe that $m_{\alpha+\beta} = m_\alpha + m_\beta$, thus $\mathrm{Tr}(m_{\alpha+\beta}) = \mathrm{Tr}(m_\alpha) + \mathrm{Tr}(m_\beta)$, which implies that

$$\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}(m_{\alpha+\beta}) = \mathrm{Tr}(m_\alpha) + \mathrm{Tr}(m_\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta).$$

(iii) : Given $a \in K$, observe that $m_a = aI_n$, thus

$$\mathrm{N}_{L/K}(a) = \det(aI_n) = a^n.$$

(iv) : Given $a \in K$, observe that $m_a = aI_n$, thus

$$\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}(aI_n) = na.$$

□

Remark 1.40. *Since $L^\times$ and $K^\times$ are multiplicative groups and $\det(m_\alpha) \neq 0$ for all $\alpha \in L^\times$, the map*

$$\phi = N_{L/K}\big|_{L^\times} : L^\times \longrightarrow K^\times$$

is a group homomorphism.

Let L/K be a finite field extension with $[L : K] = n$ and $\alpha \in L$. Let $f_\alpha(s) = \det(sI_n - m_\alpha)$ be the characteristic polynomial of the linear operator m_α. It is easy to see that

$$f_\alpha(s) = s^n - \mathrm{Tr}_{L/K}(\alpha)s^{n-1} + \cdots + (-1)^n \,\mathrm{N}_{L/K}(\alpha).$$

Proposition 1.41. *Let L/K be a finite and separable field extension and C be an algebraically closed field containing K. Then for all $\alpha \in L$ one has*

(i): $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma\in \mathrm{Hom}_K(L,C)} \sigma(\alpha)$*;*

(ii): $N_{L/K}(\alpha) = \prod_{\sigma\in \mathrm{Hom}_K(L,C)} \sigma(\alpha)$*;*

More precisely

$$f_\alpha(s) = \prod_{\sigma\in \mathrm{Hom}_K(L,C)} (s - \sigma(\alpha))$$

Proposition 1.42. *Let $F \subseteq K \subseteq L$ be a tower of fields such that K/F and L/K are finite field extensions. Then*

(i): $\mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{L/K} = \mathrm{Tr}_{L/F}$*;*

(ii): $\mathrm{N}_{K/F} \circ \mathrm{N}_{L/K} = \mathrm{N}_{L/F}$.

1.10 Normal Extensions

Definition 1.43. *Let L/K be a field extension. L/K is said a normal extension if there is a family of polynomial $\mathcal{P} \subseteq K[x]$ such that*

- *Given $f(x) \in \mathcal{P}$ with $\deg(f(x)) \deg 1$, f splits in linear factors in $L[x]$;*

- *L is generated over K by zeros of all $f(x) \in \mathcal{P}$.*

Proposition 1.44. *Let L/K be a field extension. If L/K is normal, then L/K is algebraic.*

Proof: Let $\{\alpha_i\}_{i\in\Lambda}$ be a basis of L over K such that every α_i is root of some polynomial $f(x) \in \mathcal{P}$. Given $\alpha \in L$, one knows that there exist $i_1, \ldots, i_n \in \Lambda$ and $a_1, \ldots, a_n \in K$ such that such that

$$\alpha = \sum_{k=1}^{n} a_i \alpha_{i_k}.$$

Since $\alpha \in K(\alpha_{i_1}, \ldots, \alpha_{i_n})$ and $K(\alpha_{i_1}, \ldots, \alpha_{i_n})/K$ is finite, then α is algebraic over K. □

Proposition 1.45. *Let L/K be an algebraic field extension and $\overline{K}$ the algebraic closure of K containing L. The following three assertions are equivalent:*

(i): The extension L/K is normal;

(ii): For all $\sigma \in \mathrm{Hom}_K(L, \overline{K})$, one has $\sigma(L) = L$;

(iii): For all $\tau \in \mathrm{Iso}_K(\overline{K}, \overline{K})$, one has $\tau(L) = L$.

Proof: $(i) \implies (ii)$: Suppose that L/K is a normal extension. Let $\sigma \in \mathrm{Hom}_K(L, \overline{K})$. Firstly one will prove that $\sigma(L) \subseteq L$. Since L/K is normal, then there exists $\mathcal{P} \subseteq k[x]$ such that

$$L = K\big(\{\alpha \in \overline{K} \ ; \ \alpha \text{ is root of } f(x) \in \mathcal{P} \ \}\big)$$

Let $\alpha \in \mathcal{B} := \{\beta \in \overline{K} \ ; \ \beta \text{ is root of } f(x) \in \mathcal{P} \ \}$, then there exists $f(x) \in \mathcal{P}$ such that $f(\beta) = 0$. But $f(\sigma(\beta)) = \sigma(f(\beta)) = 0$, which implies that $\sigma(\beta)$ also lies in $\mathcal{B}$ and so $\sigma(\beta) \in L$. Then

$$\sigma(L) = \sigma\big(k(\mathcal{B})\big) = k(\sigma(\mathcal{B})) \subseteq L.$$

Now let $\beta \in \mathcal{B}$ and $f(x) \in \mathcal{P}$ such that $f(\beta) = 0$. Since $f(x)$ splits in linear factors in $L[x]$ and $\mathrm{Irr}_K^{\beta}(x)$ divides $f(x)$ in $L[x]$, then $Irr_K^{\beta}(x)$ splits into linear factors in $L[x]$. Since each $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ acts in $root(f(x)) = \{\alpha \in L \ ; \ f(\alpha) = 0\}$ as a permutation, there is $\gamma \in root(f(x))$ such that $\sigma(\gamma) = \beta$. Thus

$$\sigma(L) = \sigma\big(k(\mathcal{B})\big) = k(\sigma(\mathcal{B})) = L.$$

$(ii) \implies (iii)$: Given $\tau \in \mathrm{Iso}_K(\overline{K}, \overline{K})$, consider $\sigma = \tau\big|_L$. Then $\sigma \in \mathrm{Hom}_K(L, \overline{K})$, so

$$\tau(L) = \sigma(L) = L.$$

$(iii) \Longrightarrow (i)$: Since L/K is algebraic, consider the family of polynomials

$$\mathcal{P} = \{\mathrm{Irr}_K^{\alpha}(x) \in K[x] \ ; \ \alpha \in L\}.$$

Let $f(x) := \mathrm{Irr}_K^{\alpha}(x) \in \mathcal{P}$ with $\deg(f) \geq 1$ and consider $\mathcal{B}_f \subseteq \overline{K}$ the set of all roots of $f(x)$. Given $\beta \in \mathcal{B}_f$, there is $\tau \in \mathrm{Iso}_K(\overline{K}, \overline{K})$ such that $\tau(\alpha) = \beta$. The assertion (iii) tell us that $\beta \in L$ and so $f(x)$ splits into linear factors in $L[x]$. Thus it is clear that L is generated over K by the family of roots of all polynomials $g(x) \in \mathcal{P}$ and so L/K is a normal extension. □

Proposition 1.46. *Let $F \subseteq K \subseteq L$ be a tower of fields. If L/F is a normal extension, then so is L/K.*

Proof: Firstly observe that L/K is algebraic. Now let $\overline{F}$ the algebraic closure of F containing L. Observe that $\overline{F}$ is also the algebraic closure of K, so $\overline{F} = \overline{K}$. Let $\sigma \in \mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, \overline{F})$, then $\sigma \in \mathrm{Hom}_F(L, \overline{F})$. Since L/F is normal, one has that $\sigma(L) = L$. So the hypothesis (ii) of previous preposition, which implies that L/K is normal. □

Remark 1.47. *Let $F \subseteq K \subseteq L$ be a tower of fields. If L/F is a normal extension, it is not necessarily true that K/F is normal. Indeed consider the tower of fields*

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3).$$

Note that $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3)/\mathbb{Q}$ is a normal extension, while $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not.

Let $K \subseteq L \subseteq \overline{K}$ be a chain of fields. Let L^N be a subfield of $\overline{K}$ generated over K by

$$\bigcup_{\phi \in \mathrm{Hom}_K(L, \overline{K})} \phi(L)$$

Observe that $K \subseteq L \subseteq L^N \subseteq \overline{K}$, because the inclusion $i : L \longrightarrow \overline{K}$ lies on $\mathrm{Hom}_K(L, \overline{K})$.

Proposition 1.48. *Let $K \subseteq L \subseteq \overline{K}$ be a chain of fields. Then L^N/K is a normal extension. Moreover, if L/K is finite, then L^N/K is finite.*

1.11 Galois Extension

Definition 1.49. *A field extension L/K is said a Galois extension if L/K is normal and separable. In this case the set* $\mathrm{Hom}_K(L, L)$ *is actually a group with the composition operation, is called Galois Group of L/K and is denoted by* $\mathrm{Gal}(L/K)$.

Proposition 1.50. *Let L/K be a Galois extension. If L/K is finite, then*

$$|\operatorname{Gal}(L/K)| = [L : K].$$

Proof: Indeed since L/K is separable, there is $\zeta \in L$ separable such that $L = K(\zeta)$. Let $f(x) = \operatorname{Irr}_K^{\zeta}(x) \in K[x]$ and $n = \deg(f(x)) = [L : K]$. For each α root of $f(x)$, there is $\sigma \in \operatorname{Gal}(L/K)$ such that $\sigma(\zeta) = \alpha$. Since $f(x)$ is a separable polynomial, then $|\operatorname{Gal}(L/K)| \geq n = [L : K]$.

Now let $\sigma \in \operatorname{Gal}(L/K)$. It is easy to see that σ takes ζ to some root of $f(x)$. Since $L = K(\zeta)$, σ is completely determined by its action on ζ, which implies that $|\operatorname{Gal}(L/K)| \leq n = [L : K]$. Thus

$$|\operatorname{Gal}(L/K)| = [L : K].$$

Theorem 1.51 (Fundamental Theorem of Galois's Theory)**.** *Let L/K be a finite Galois extension. Denote*

$$\mathcal{P} = \{F \subseteq L \ ; \ F \textit{ is field containing } K\};$$
$$\mathcal{H} = \{H \subseteq \operatorname{Gal}(L/K) \ ; \ H \textit{ is subgroup of } \operatorname{Gal}(K/F)\}.$$

Then the maps $\phi : \mathcal{P} \longrightarrow \mathcal{H}$ such that $\phi(F) = \operatorname{Gal}(L/F)$ and $\psi : \mathcal{H} \longrightarrow \mathcal{P}$ such that $\psi(H) = L^H$, where

$$L^H = \{x \in L \ ; \ \sigma(x) = x \, \forall \sigma \in H\},$$

are mutually inverses. Thus there is an one-to-one correspondence between the intermediary field betwemm K and L and the subgroups of Galois group $\operatorname{Gal}(L/K)$. Moreover given a intermediary field $K \subseteq F \subseteq L$, one has that F/K is Galois if and only if $\operatorname{Gal}(L/F)$ is normal subgroup of $\operatorname{Gal}(L/K)$. In this case

$$\frac{\operatorname{Gal}(L/F)}{\operatorname{Gal}(L/K)} \cong \operatorname{Gal}(F/K).$$

1.12 Associate classes representatives

Let R be an UFD and $\mathcal{R} \subseteq R$ such that, for all $a \in R$, there exists an unique $r \in \mathcal{R}$ such that $r \sim a$. Then there exists bijection $\phi : \mathcal{R} \longrightarrow R/R^\times$ such that the following diagram commutes

$$\begin{tikzcd}
 & R \arrow[dr, "\pi"] & \\
\mathcal{R} \arrow[ur, "i"] \arrow[rr, "\phi"] & & R/R^\times
\end{tikzcd}$$

(i): If $R = \mathbb{Z}$, then $\mathcal{R} = \mathbb{N}$ satisfies the property above.

(ii): If $R = k[x]$, where k is a field, then $\mathcal{P} = \{0\} \cup \{f(x) \in k[x] \ ; \ f(x) \text{ is monic}\}$ satisfies the property above.

Let $\mathcal{P} = \{p \in \mathcal{R} \ ; \ p \text{ is irreducible}\}$ and define

$$\mathbb{N}^{\oplus \mathcal{P}} = \{(n_p)_{p\in\mathcal{P}} \ ; \ |\{p \in \mathcal{P} \ ; \ n_p \neq 0\}| < \infty\}$$

Observe that $(\mathbb{N}^{\oplus\mathcal{P}}, +)$ is a commutative monoid for the operation of operation

$$(n_p)_{p\in\mathcal{P}} + (m_p)_{p\in\mathcal{P}} = (n_p + m_p)_{p\in\mathcal{P}}.$$

Proposition 1.52. *Let R be an UFD and $\mathcal{P}$ be a set of associate classes representatives of R. Consider $\mathcal{P} \subseteq \mathcal{R}$ the subset of prime elements of $\mathcal{R}$. Then there is a monoid isomorphism $\phi : R^\times \times \mathbb{N}^{\oplus\mathcal{P}} \longrightarrow R \setminus \{0\}$ such that*

$$\phi(u, (n_p)_{p\in\mathcal{P}}) = u \prod_{p\in\mathcal{P}} p^{n_p}.$$

Proof: It is trivial.

Let R be an UFD, $\mathcal{P}$ be a set of associate classes representatives of R and $\mathcal{P} \subseteq \mathcal{R}$ the subset of prime elements of $\mathcal{R}$. Given $p \in \mathcal{P}$, consider the function $v_p : R \setminus \{0\} \longrightarrow \mathbb{N}$ such that

$$v_p\left(u \prod_{q\in\mathcal{P}} p^{n_q}\right) = n_p.$$

Note that $v_p(r) = \max\{n \in \mathbb{N} \ ; \ p^n | r\}$. Extend this function to R by defining $v_p(0) = \infty$.

Proposition 1.53. *Let R be an UFD, $\mathcal{P}$ a set of associate classes representatives of R and $\mathcal{P} \subseteq \mathcal{R}$ the subset of prime elements of $\mathcal{R}$. Given $p \in \mathcal{P}$, consider the function $v_p : R \longrightarrow \mathbb{N} \cup \{0\}$ as defined above. Then*

(i) For all $r, s \in R$, one has $v_p(rs) = v_p(r) + v_p(s)$;

(ii) For all $r, s \in R$, one has $v_p(r+s) \geq \min\{v_p(r), v_p(s)\}$.

Proof: Let

$$r = u \prod_{q \in \mathcal{P}} q^{n_q} \qquad \text{and} \qquad s = v \prod_{q \in \mathcal{P}} q^{m_q}.$$

(i) : Then

$$rs = (uv) \prod_{q \in \mathcal{P}} q^{n_q + m_q},$$

which implies $v_p(rs) = n_p + m_p = v_p(r) + v_p(s)$.

(ii) : Similarly, observe that

$$r + s = p^{\min\{m_p, n_p\}} \left(u p^{n_p - \min\{m_p, n_p\}} \prod_{q \neq p \in \mathcal{P}} q^{n_q} + v p^{m_p - \min\{m_p, n_p\}} \prod_{q \neq p \in \mathcal{P}} q^{m_q} \right)$$

Thus $p^{\min\{m_p, n_p\}}$ divides $r + s$, which implies that

$$v_p(r+s) \geq \min\{m_p, n_p\} = \min\{v_p(r), v_p(s)\}.$$

Definition 1.54. *Let R be an UFD, $\mathcal{P}$ a set of associate classes representatives of R and $\mathcal{P} \subseteq \mathcal{R}$ the subset of prime elements of $\mathcal{R}$. Given $r, s \in R$, one defines the greatest common divisor of r and s by*

$$\gcd(r, s) := \prod_{p \in \mathcal{P}} p^{\min\{v_p(r), v_p(s)\}}.$$

Similarly, one defines the least common multiple of r and s by

$$(r, s) := \prod_{p \in \mathcal{P}} p^{\max\{v_p(r), v_p(s)\}}.$$

Proposition 1.55. *Let R be an UFD, $\mathcal{P}$ a set of associate classes representatives of R and $\mathcal{P} \subseteq \mathcal{R}$ the subset of prime elements of $\mathcal{R}$. Let $a \in R \setminus \{0\}$ and $m \in \mathbb{N}$. Then there is $u \in R^\times$ and $b \in R$ such that $a = ub^m$ if and only if, for all $p \in \mathcal{P}$, one has $v_p(a)|m$.*

Proposition 1.56. *Let R be an UFD, $\mathcal{P}$ a set of associate classes representatives of R and $\mathcal{P} \subseteq \mathcal{R}$ the subset of prime elements of $\mathcal{R}$. Let $a,\ b,\ c \in R \setminus \{0\}$ and $m \in \mathbb{N}$. Suppose that $ab = c^m$ and $\gcd\{a, b\} = 1$, then there exist $u,\ v \in R^\times$ and $x, y \in R$ such that $a = ux^m$ and $b = vy^m$*

Definition 1.57. *Let R be an UFD, $\mathcal{P}$ a set of associate classes representatives of R and $\mathcal{P} \subseteq \mathcal{R}$ the subset of prime elements of $\mathcal{R}$. The function $\phi : R^\times \times \bigoplus_{p\in\mathcal{P}} \mathbb{Z} \longrightarrow \mathrm{Quot}(R)^\times$ such that*

$$\phi(u, (n_p)_{p\in\mathcal{P}}) = u \prod_{p\in\mathcal{P}} p^{n_p}.$$

gives a groups isomorphism

Thus for all $p \in \mathcal{P}$ one can define $v_p : \mathrm{Quot}(R)^\times \longrightarrow \mathbb{Z}$ such that

$$v_p\left(u \prod_{p\in\mathcal{P}} p^{n_p}\right) = n_p.$$

Moreover, if one extends this function by defining $v_p(0) = \infty$, one gets the

$$\begin{aligned} \phi_p : \mathrm{Quot}(R) &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ r &\longmapsto v_p(r). \end{aligned}$$

Chapter 2

Algebraic Integers

2.1 Gaussian Integers

Definition 2.1. *Let i be the imaginary number. The set*

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

is called the set of Gaussian integers.

It is easy to see that $(\mathbb{Z}[i], +, \cdot)$ is a subring of the field of complex numbers. In particular, $\mathbb{Z}$ is an integral domain. Moreover the conjugation map

$$\phi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$$

$$z \longmapsto \overline{z}$$

is clearly an involution in $\mathbb{Z}[i]$, In particular $\phi \in \mathrm{Aut}(\mathbb{Z}[i])$. Now we are going to define a norm function in $\mathbb{Z}[i]$.

Definition 2.2. *Let $\mathbb{Z}[i]$ be the ring of Gaussian integers. One defines the norm function in $\mathbb{Z}[i]$ by*

$$\mathrm{N} : \mathbb{Z}[i] \longrightarrow \mathbb{N}$$

$$z \longmapsto z\overline{z}$$

Proposition 2.3. *Let N be the norm function in $\mathbb{Z}[i]$, then* *(i):* $\mathrm{N}(z) = 0$ *if and only if* $z = 0$*;*

(ii): For any $z,\ w \in \mathbb{Z}[i]$*, one has* $\mathrm{N}(zw) = \mathrm{N}(z)\,\mathrm{N}(w)$.

Proof: (i) : If $z = 0$, it is clear that $\mathrm{N}(z) = 0$. Now suppose that $\mathrm{N}(z) = \mathrm{N}(a + bi) = 0$, then $a^2 + b^2 = 0$. Since $\mathbb{N} \subseteq \mathbb{R}$ and $\mathbb{R}$ is an ordered field, one has that $a = b = 0$, which implies that $z = 0$.

(ii) : Given $z,\ w \in \mathbb{Z}[i]$, one has

$$\mathrm{N}(zw) = zw\overline{zw} = zw\overline{z}\overline{w} = z\overline{z}w\overline{w} = \mathrm{N}(z)\,\mathrm{N}(w).$$

□

Corollary 2.4. *Let* $z \in \mathbb{Z}[i]$*. The following assertions are equivalent*

(i): *z is an unity element in* $\mathbb{Z}[i]$*;*

(ii): $\mathrm{N}(z) = 1$*;*

(iii): $z \in \{1, -1, i, -i\}$.

Proof: $(i) \implies (ii)$: Suppose that $z \in \mathbb{Z}[i]^\times$. Thus there is $w \in \mathbb{Z}[i]$ such that $zw = 1$. Applying the norm function, one has

$$\mathrm{N}(z)\,\mathrm{N}(w) = \mathrm{N}(zw) = \mathrm{N}(1) = 1.$$

Since $\mathrm{N}(z),\ \mathrm{N}(w) \in \mathbb{N}$, one has $\mathrm{N}(z) = 1$.

$(ii) \implies (iii)$: If $\mathrm{N}(z) = \mathrm{N}(a + bi) = a^2 + b^2 = 1$, then $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$, which implies that $z \in \{1, -1, i, -i\}$.

$(iii) \implies (i)$: Trivial. □

Proposition 2.5. *Let* $z = a+bi \in \mathbb{Z}[i]$*. Then Norm function applied to z coincides with* $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(z)$

Proof: Indeed consider $\mathcal{B} = \{1, i\}$ the canonical basis of $\mathbb{Q}(i)$ as $\mathbb{Q}$-linear space. Thus

$$m_z(1) = z = a + bi;$$

$$m_z(i) = iz = -b + ia.$$

Thus the matrix of m_z with respect the basis $\mathcal{B}$ is

$$[m_z]_{\mathcal{B}} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

Thus $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(z) = \det([m_z]_{\mathcal{B}}) = a^2 + b^2 = \mathrm{N}(z)$. □

Proposition 2.6. *The ring* $(\mathbb{Z}[i], \mathrm{N})$ *is an Euclidean domain.*

Proof: We already saw that $\mathrm{N}(zw) = \mathrm{N}(z)\,\mathrm{N}(w)$ for any $z, w \in \mathbb{Z}[i]$. In particular for any $z, w \in \mathbb{Z}[i]$, one has $\mathrm{N}(zw) \leq \mathrm{N}(z)\,\mathrm{N}(w)$.

Now let $z = a + bi,\ w = u + vi \in \mathbb{Z}[i]$ with $w \neq 0$. Consider the number

$$\gamma = \frac{a+bi}{u+vi} = \frac{au+bv}{u^2+v^2} + \frac{bu-av}{a^2+b^2} i \in \mathbb{Q}[i].$$

If $\gamma \in \mathbb{Z}[i]$, consider $r = 0$ and $q = \gamma$. Thus $z = wq$. On the other hand if $\gamma \notin \mathbb{Z}[i]$, thinking geometrically there is $q \in \mathbb{Z}[i]$ such that such that the Euclidean distance from γ is less or equal to $\sqrt{2}/2$. Thus

$$\mathrm{N}\left(\frac{z}{w} - q\right) = \left\|\frac{z}{w} - q\right\|^2 \leq 1/2.$$

Considering $r = z - qw$, one has that $r \neq 0$ and

$$\mathrm{N}(r) = N(z - qw) = \left\| w\left(\frac{z}{w} - q\right)\right\|^2 = \mathrm{N}(w)\|\gamma - q\|^2 \leq \mathrm{N}(w)/2 \leq \mathrm{N}(w).$$

□

In particular $\mathbb{Z}[i]$ is a PID and an UFD.

Theorem 2.7 (Fermat's Theorem)**.** *For all prime number $p \neq 2$, one has*

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

Proof: Let p be a prime number different from 2 and suppose that $p = a^2 + b^2$ for some $a,\ b \in \mathbb{Z}$. Observe that p is necessarily odd, so a and b necessarily need to have opposite parity. Supposing $a = 2n$ and $b = 2m + 1$ for some $n,\ m \in \mathbb{Z}$, one concludes that

$$a^2 + b^2 = (2n)^2 + (2m+1)^2 = 4(n^2 + m^2 + m) + 1,$$

thus, since $p \equiv a^2 + b^2 \mod 4$ and $a^2 + b^2 \equiv 1 \mod 4$, by transitivity one gets that $p \equiv 1 \mod 4$.

On the other hand let p be a prime number different from 2 and suppose that $p \equiv 1 \mod 4$. By Wilson theorem, one knows that there is $x \in \mathbb{Z}$ such that

$$x^2 \equiv -1 \mod p.$$

This implies that p divides $x^2 + 1 = (x+i)(x-i)$ in $\mathbb{Z}$. Since $\mathbb{Z} \subseteq \mathbb{Z}[i]$, one also has that p divides $x^2 + 1$ in $\mathbb{Z}[i]$. If p was irreducible in $\mathbb{Z}[i]$, we would have that $p|(x+i)$ or $p|(x-i)$, which implies that $x \pm i = (a+bi)p = pa + pbi$ for some a, $b \in \mathbb{Z}$, which is not possible.

Thus p is not irreducible. Thus there is α, $\beta \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ such that $p = \alpha\beta$. Applying the norm function, one obtains

$$p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$$

Since $\mathrm{N}(\alpha), \mathrm{N}(\beta) \neq 1$ because α and β are not unity elements, then $\mathrm{N}(\beta) = \mathrm{N}(\alpha) = p$. Hence, denoting $\alpha = a + bi$, one concludes that

$$a^2 + b^2 = \mathrm{N}(\alpha) = p.$$

A natural question is to find a set of class of irreducible elements modulo the associate elements.

Lemma 2.8. *Let $z \in \mathbb{Z}[i]$ be an Gaussian integer. If $\mathrm{N}(z)$ is a prime element in $\mathbb{Z}$, then z is irreducible in $\mathbb{Z}[i]$.*

Proof: Suppose that $N(z) = p$ is a prime number. Let $z = \alpha\beta$, where α, $\beta \in \mathbb{Z}[i]$. Applying the norm function, one has

$$\mathrm{N}(\alpha)\,\mathrm{N}(\beta) = \mathrm{N}(\alpha\beta) = \mathrm{N}(z) = p.$$

Since p is irreducible in $\mathbb{Z}$, one concludes that $\mathrm{N}(\alpha) = 1$ or $\mathrm{N}(\beta) = 1$, which implies that α or β is unity element in $\mathbb{Z}[i]$. □

Observe that

1. $\mathbb{Z}^\times \subseteq \mathbb{Z}[i]^\times$;

2. $\mathbb{Z} \setminus (\mathbb{Z}^\times \cup \{0\}) \subseteq \mathbb{Z}[i] \setminus (\mathbb{Z}[i]^\times \cup \{0\})$.

Let $a \in \mathbb{Z} \setminus (\mathbb{Z}^{\times} \cup \{0\})$. If a is reducible, then a is reducible in $\mathbb{Z}[i]$. Furthermore the associate integers in $\mathbb{Z}$ are associates in $\mathbb{Z}[i]$. And what about the prime numbers?

One already knows that if p is a prime number with $p \equiv 1 \mod 4$, then p is reducible in $\mathbb{Z}[i]$. Moreover, since $2 = (1+i)(1-i)$, one has that 2 is also reducible in $\mathbb{Z}[i]$. Now suppose that $p \equiv 3 \mod 4$. If $p = \alpha\beta$, where α, $\beta \in \mathbb{Z}[i]$. Applying the norm function, one has

$$p^2 = \mathrm{N}(\alpha)\,\mathrm{N}(\beta).$$

If p was reducible in $\mathbb{Z}[i]$, then we would have that $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = p$. Denoting $\alpha = a + bi$, we would obtain that $a^2 + b^2 = p$, which is a contradicition since $p \equiv 3 \mod 4$.

Proposition 2.9. *Let $\pi \in \mathbb{Z}[i]$ be an irreducible element. Then π is associate to one and only one of the following Gaussian integers.*

- *$p \in \mathbb{Z}$ prime element with $p \equiv 3 \mod 4$;*
- *$1 + i$;*
- *$a + bi$, where $a^2 + b^2 = p$ with p prime in $\mathbb{Z}$ and $p \equiv 1 \mod 4$, with $a > |b| > 0$.*

Proof: Firstly it is easy to observe that each pair of these three kind of elements consists of non-associated elements. Let $\pi \in \mathbb{Z}[i]$ be an irreducible element. Applying the norm function, one obtains

$$\pi\overline{\pi} = \mathrm{N}(\pi) = p_1 \cdots p_n,$$

where $p_1, \dots, p_n$ are prime elements in $\mathbb{Z}$. Since π is irreducible, one has that $\pi | p_i$ for some $i = 1, \dots, n$. Let $p := p_i$. Hence there is $\alpha \in \mathbb{Z}[i]$ such that $p = \alpha\pi$. Applying the norm function again, one concludes that $\mathrm{N}(\pi) \in \{p, p^2\}$. Suppose that $\mathrm{N}(\phi) = p$ and denote $\pi = a + bi$

- If $p = 2$, then $\pi = 1 + i$ modulo associate classes;
- If $p \equiv 1 \mod 4$, then $N(\pi) = a^2 + b^2 = p$. Thus $\pi = a + bi$ such that $a^2 + b^2 = p$ and $p \equiv 1 \mod 4$
- If $p \equiv 3 \mod 4$, then $N(\pi) = a^2 + b^2 = p$ and $p \equiv 3 \mod 4$, which we already saw that is impossible.

Finally suppose that $N(\pi) = \pi^2$. Since $p = \pi\alpha$, then

$$p^2 = \mathrm{N}(p) = \mathrm{N}(\pi\alpha) = \mathrm{N}(\pi)\,\mathrm{N}(\alpha) = p^2\,\mathrm{N}(\alpha)$$

Thus $\mathrm{N}(\alpha) = 1$, which implies that $\alpha \in \{\pm 1, \pm i\}$, which implies that π is associated to p and $p \equiv 3$ mod 4. □

2.2 Integrality

Definition 2.10. *Let $A \subseteq B$ be a ring extension and $b \in B$*

(i) One says that b is integral over A if there is a monic polynomial $f(x) \in A[x]$ such that $f(b) = 0$;

(ii) The integral closure of A in B, denoted bu $\overline{A}^B$, is the set of all elements of B which are integral over A, that is

$$\overline{A}^B = \{x \in B \ ; \ x \textit{ is integral over } A\}.$$

(iii) B is said integral over if all element of B is integral over A, that is, if $\overline{A}^B = B$;

(iv) A is said integrally closed in B if $\overline{A}^B = A$.

Remark 2.11. *Given $A \subseteq B$ be a ring extension, it is clear that $A \subseteq \overline{A}^B \subseteq B$, because every element $a \in A$ is zero of the monic polynomial $f(x) = x - a \in A[x]$.*

Proposition 2.12. *Let $A \subseteq B \subseteq C$ be a tower of rings. Then*

(i): $\overline{A}^B = \overline{A}^C \cap B$;

(ii): $\overline{A}^B \subseteq \overline{A}^C$

Proof: (i) : Suppose that $x \in \overline{A}^B$, then $x \in B \subseteq C$ and x is integral over A, which implies that $x \in \overline{A}^C \cap B$. On the other hand suppose that $x \in \overline{A}^C \cap B$, then $x \in B$ and x is root of a monic polynomial in $A[x]$. Thus $x \in \overline{A}^B$.

(ii) : Just note $\overline{A}^B = \overline{A}^C \cap B \subseteq \overline{A}^C$. □

Definition 2.13. *The set of elements of $\mathbb{C}$ which are integral over $\mathbb{Z}$ is simply denoted by $\overline{\mathbb{Z}}$. Let K be a field between $\mathbb{Q}$ and $\overline{\mathbb{Q}}$. We denote by $\mathcal{O}_K$ the elements of K which are integral over $\mathbb{Z}$, that is*

$$\mathcal{O}_K = \{x \in K \ ; \ x \text{ is integral over } \mathbb{Z}\}.$$

By Proposition 2.12, one has that $\mathcal{O}_K = \overline{\mathbb{Z}}^K = \overline{\mathbb{Z}}^{\mathbb{C}} \cap K = \overline{\mathbb{Z}} \cap K$.

Proposition 2.14. *Let $A \subseteq B$ be a ring extension and $b \in B$. The following assertions are equivalent.*

1. *b is integral over A;*

2. *$A[b]$ is a finitely generated A-module;*

3. *There is an A-subalgebra D of B such that $b \in D$ and D is a finitely generated A-module.*

Proof: $(i) \implies (ii)$: One knows that every element of $A[b]$ is of form $f(b)$ for some polynomial $f(x) \in A[x]$. Suppose that b is integral over A, then there is a monic polynomial $g(x) \in A[x]$ such that $g(b) = 0$. Since $g(x)$ is monic, there are $q(x)$, $r(x) \in A[x]$ such that

$$f(x) = g(x)q(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x)) := n$. Suppose without lost of generality that $r(x) \neq 0$. Thus

$$f(b) = r(b) = \sum_{k=0}^{n-1} a_k b^k,$$

which implies that $f(b) \in \sum_{k=0}^{n-1} Ab^k$. Then $A[b] = \sum_{k=0}^{n-1} Ab^k$ is a finitely generated A-module.

$(ii) \implies (iii)$: Take $D := A[b]$.

$(iii) \implies (i)$: Let $\gamma_1, \ldots, \gamma_n$ be a generating set of D as A-module. Since $b \in D$, one has that $\gamma_i b \in D$ for all $1 \leq i \leq n$, thus there are $a_{ij} \in A$, $1 \leq i, j \leq n$ such that

$$b\gamma_i = \sum_{k=1}^{n} a_{ik}\gamma_k,$$

or, equivalently

$$\sum_{k=1}^{n} (b\delta_{ki} - a_{ik})\gamma_k = 0$$

for all $1 \leq i \leq n$. Consider the matrix $A = [b\delta_{ij} - aij]_{ij} = bI_n - C$, where $C = [a_{ij}]$. By adjoint matrix identity, we have $\operatorname{adj}(A)A = A\operatorname{adj}(A) = \det(A)I_n$. Since

$$A \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{bmatrix} = 0$$

one concludes that $\det(A)\gamma_1 = \cdots = \det(A)\gamma_n = 0$. Finally, since $1 \in D$, there are $c_1, \ldots, c_n \in A$ such that $1 = \sum_{k=1}^{n} b_k\gamma_k$, which implies

$$\det(A) = \det(A) \cdot 1 = \det(A)\sum_{k=1}^{n} b_k\gamma_k = \sum_{k=1}^{n} b_k\big(\det(A)\gamma_k\big) = 0.$$

Now, considering $f(x) = \det(xI_n - C)$, one has that $f(x)$ is a monic polynomial in $A[x]$ and $f(b) = \det(bI_n - C) = \det(A) = 0$, so b is integral over A. □

Corollary 2.15. *Let $A \subseteq B$ be a ring extension and $b_1, \ldots, b_n \in B$. Then $b_1, \ldots, b_n$ are integral over A if and only if $A[b_1, \ldots, b_n]$ is a finitely generated A-module.*

Proof: Suppose that $b_1, \ldots, b_n$ are integral over A. We will prove by induction on n that $A[b_1, \ldots, b_n]$ is a finitely generated A-module. The case $n = 1$ was already proved. Suppose that it holds for $n-1$, that is, $A[b_1, \ldots, b_{n-1}]$ is a finitely generated A-module. Let $b_1, \ldots, b_n$ be integral elements of B over A. Since $A \subseteq A[b_1, \ldots, b_{n-1}] \subseteq B$, b_n is also integral over $A[b_1, \ldots, b_{n-1}]$. Thus $A[b_1, \ldots, b_{n-1}][b_n] = A[b_1, \ldots, b_{n-1}, b_n]$ is a finitely generated $A[b_1, \ldots, b_{n-1}]$-modulo. Finally, since $A[b_1, \ldots, b_{n-1}]$ is finitely generated A-module, one concludes that $A[b_1, \ldots, b_{n-1}, b_n]$ is finitely generated A-module and the statement follows by induction principle.

Conversely suppose that $A[b_1, \ldots, b_n]$ is a finitely generated A-module. Since $b_i \in A[b_1, \ldots, b_n] \subseteq B$, by implication $(iii) \implies (i)$, one concludes that b_i is integral over A. □

Corollary 2.16. *Let $A \subseteq B$ be a ring extension and $b_1, \ldots, b_n \in B$. Then $A[b_1, \ldots, b_n] \subseteq \overline{A}^B$ if and only if $b_1, \ldots, b_n$ are integral over A.*

Proof: If $A[b_1, \ldots, b_n] \subseteq \overline{A}^B$, then $b_i \in A[b_1, \ldots, b_n] \subseteq \overline{A}^B$, so b_i is integral over A for each $i = 1, \ldots, n$. Conversely if $b_1, \ldots, b_n$ are integral over A, then $A[b_1, \ldots, b_n]$ is a finitely generated A-module. By implication $(iii) \implies (i)$, one concludes that each element of $A[b_1, \ldots, b_n]$ is integral over A, thus $A[b_1, \ldots, b_n] \subseteq \overline{A}^B$. □

Corollary 2.17. *Let $A \subseteq B$ be a ring extension. Then $\overline{A}^B$ is a ring extension of A.*

Proof: Since $A \subseteq \overline{A}^B$, it is enough to show that $\overline{A}^B$ is a subring of B. Given x, $y \in B$ integral elements over A, we have that $A[x, y] \subseteq B$ is a finitely generated A-module. Thus, since $x \pm y$, $xy \in A[x, y]$, one concludes that $x \pm y$, xy are integral elements over A. Thus $\overline{A}^B$ is closed by addition, subtraction and multiplication, which means that $\overline{A}^B$ is a subring of B. □

Corollary 2.18. *Let $A \subseteq B$ be a ring extension. Then B is a finitely generated A-module if and only if B is a finitely generated A-algebra and B is integral over A.*

Proof Suppose that B is a finitely generated A-module A and let $b_1, \ldots, b_n$ be a generating set of B as A-module. Then $B = A[b_1, \ldots, b_n]$, which implies that B is a finitely generated A-algebra. Moreover, since B is finitely generated A-module, b is integral over A for all $b \in B$, hence B is integral over A.

Conversely suppose that B is a finitely generated A-algebra and B is integral over A. Then $B = A[b_1, \ldots, b_n]$ for some $b_1, \ldots, b_n \in B$. Since each b_i is integral over A, one concludes that $B = A[b_1, \ldots, b_n]$ is finitely generated A-module. □

Corollary 2.19. *Let $A \subseteq B \subseteq C$ be tower of rings and $c \in C$. Suppose that c is integral over B and that B is integral over A. Then c is integral over A.*

Proof: Since c is integral over B, there are $b_1, \ldots, b_n \in B$ such that

$$c^n + b_1 c^{n-1} + \cdots + b_{n-1} c + b_n = 0.$$

Consider the ring $A \subseteq D := A[b_1, \ldots, b_n] \subseteq C$. Since B is integral over A, D is a finitely generated A-module. Since c is integral over D, one has that $D[c] = A[b_1, \ldots, b_n, c]$ is a finitely generated $A[b_1, \ldots, b_n]$-module. Hence $A[b_1, \ldots, b_n, c]$ is a finitely generated A-module, which implies that c is integral over A. □

Corollary 2.20. *Let $A \subseteq B \subseteq C$ be tower of rings. Then*

$$\overline{\overline{A}^B}^C = \overline{A}^C.$$

Proof: Suppose that $r \in \overline{A}^C$, then r is root of a monic polynomial $A[x]$. Since $A \subseteq \overline{A}^B$, we also have that r root of a monic polynomial in $\overline{A}^B[x]$, so $r \in \overline{\overline{A}^B}^C$, which implies that $\overline{A}^C \subseteq \overline{\overline{A}^B}^C$. On the other hand, since $A \subseteq \overline{A}^B \subseteq C$ and $\overline{A}^B$ is integral over A, then

$$\overline{\overline{A}^B}^C \subseteq \overline{A}^C.$$

□

Corollary 2.21. *Let $A \subseteq B$ be a ring extension. Then $\overline{A}^B$ is integral over A and is integrally closed in B.*

Proof: By own definition $\overline{A}^B$ is integral over A, because each element of $\overline{A}^B$ is integral over A. Now $A \subseteq \overline{A}^B \subseteq B$. By previous corollary, taking $C = B$, one obtains

$$\overline{\overline{A}^B}^B = \overline{A}^B,$$

which implies that $\overline{A}^B$ is integrally closed in B. □

Definition 2.22. *Let A be an integral domain and $K = \mathrm{Quot}(A)$ its total field of fractions. A is said integrally closed if A is integrally closed in K, that is, if $\overline{A}^K = A$.*

Proposition 2.23. *Let A be an integral domain. If A is an UFD, then A is integrally closed. In particular Euclidean Domains and PID's are integrally closed.*

Proof: Let $z = r/s \in K$ integral over A. Since A is UFD, one can suppose without lost of generality that $\gcd(r, s) = 1$. Let $a_1, \dots, a_n \in A$ such that

$$\left(\frac{r}{s}\right)^n + a_1\left(\frac{r}{s}\right)^{n-1} + \cdots + a_{n-1}\left(\frac{r}{s}\right) + a_n = 0.$$

Multiplying the equation above by s^n, one gets

$$r^n + a_1 r^{n-1} s + \cdots + a_{n-1} r s^{n-1} + a_n s^n = 0.$$

Thus s divides r^n. The hypothesis $\gcd(r, s) = 1$ forces s be an unity element, thus $z = r/s = rs^{-1} \in A$. □

Example 2.24. *Since $\mathbb{Z}[i]$ is an Euclidean domain, then $\mathbb{Z}[i]$ is integrally closed in its total field of fractions $\mathrm{Quot}(\mathbb{Z}[i]) = \mathbb{Q}(i)$. Thus*

$$\overline{\mathbb{Z}[i]}^{\mathbb{Q}(i)} = \mathbb{Z}[i].$$

Proposition 2.25. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a finite extension and consider B the integral closure of L over A. Then, given $\beta \in L$, there are $a \in A \setminus \{0\}$ and $b \in B$ such that $\beta = b/a$.*

Proof: Let $\beta \in L$. Since β is algebraic over K and $K = \mathrm{Quot}(A)$, there is a non-zero polynomial $f(x) \in A[x]$ such that $f(\beta) = 0$. Denoting $f(x) = \sum_{k=0}^{n} a_k x^k$, then

$$a_n\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0 = 0.$$

Multiplying by a_n^{n-1}, one gets the following equation

$$(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + \cdots + a_1a_n^{n-2}(a_n\beta) + a_0a_n^{n-1} = 0.$$

This implies that $a_n\beta$ is integral over A, thus there exists $b \in B$ such that $a_n\beta = b$, so $\beta = b/a$. □

Corollary 2.26. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a finite extension and consider B the integral closure of L over A. Given $\beta_1, \ldots, \beta_n \in L$, there is $a \in A \setminus \{0\}$ such that $a\beta_i \in B$ for all $i = 1, \ldots, n$.*

Proof: Indeed, by previous Proposition, there are $a_i \in A \setminus \{0\}$ such that $a_i\beta_i \in B$ for all $i = 1, \ldots, n$. Considering $a := a_1 \cdots a_n \in A \setminus \{0\}$, one obtains $a\beta_i \in B$ for all $i = 1, \ldots, n$. □

Corollary 2.27. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a finite extension and consider B the integral closure of L over A. Then there are a basis $\beta_1, \ldots, \beta_n$ of L/K such that $\beta_i \in B$ for all $i = 1, \ldots, n$.*

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of L/K. By previous corollary, we know that there is $a \in A \setminus \{0\}$ such that $\{a\alpha_1, \ldots, a\alpha_n\} \subseteq B$. Setting $\beta_i = a\alpha_i$, it is easy to see that $\{\beta_1, \ldots, \beta_n\}$ also is basis of L/K. □

Corollary 2.28. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a finite extension and consider B the integral closure of L over A. Then $\mathrm{Quot}(B) = L$.*

Proof: Since every element of L is quotient of elements of B and L is a field, it follows that $\mathrm{Quot}(B) = L$. □

Corollary 2.29. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a finite extension and consider B the integral closure of L over A. If A is integrally closed, then so is B.*

Proof: In fact

$$\overline{B}^L = \overline{\overline{A}^K}^L = \overline{A}^L = B.$$

□

2.3 Discriminant

Definition 2.30. *Let L/K be a finite field extension and $\operatorname{Tr}_{L/K} : L \longrightarrow K$ the trace function of this extension. The trace form is the application*

$$T_{L/K} : L \times L \longrightarrow K$$
$$(\alpha, \beta) \longmapsto \operatorname{Tr}_{L/K}(\alpha\beta)$$

Proposition 2.31. *Let L/K be a finite field extension. Then the trace form of this extension is K-bilinear and symmetric.*

Proof: Given $\alpha, \beta \in L$

$$T_{L/K}(\alpha, \beta) = \operatorname{Tr}_{L/K}(\alpha\beta) = \operatorname{Tr}_{L/K}(\beta\alpha) = T_{L/K}(\beta, \alpha).$$

Thus $T_{L/K}$ is symmetric. Now let $\alpha_1, \ldots, \alpha_n$ be a basis of L over K and $\alpha \in L$. Consider $A = [a_{ij}]$ the matrix of m_α with respect to this basis. This implies that

$$\alpha\alpha_i = \sum_{k=1}^{n} a_{ki}\alpha_k.$$

Now given $\lambda \in K$, one has

$$\lambda\alpha\alpha_i = \sum_{k=1}^{n} (\lambda a_{ki})\alpha_k.$$

Thus the matrix of $m_{\lambda\alpha}$ is λA, which implies that $\operatorname{Tr}_{L/K}(\lambda\alpha) = \lambda \operatorname{Tr}_{L/K}(\alpha)$. Finally, given $\alpha, \beta, \gamma \in L$ and $\lambda \in K$, we get

$$\begin{aligned} T_{L/K}(\alpha + \lambda\beta, \gamma) = \operatorname{Tr}_{L/K}((\alpha + \lambda\beta)\gamma) = \operatorname{Tr}_{L/K}(\alpha\gamma + \lambda\beta\gamma) = \operatorname{Tr}_{L/K}(\alpha\gamma) + \operatorname{Tr}_{L/K}(\lambda\beta\gamma) \\ = T_{L/K}(\alpha, \gamma) + \lambda T_{L/K}(\beta, \gamma). \end{aligned}$$

Similarly one proves that $T_{L/K}(\alpha, \beta + \lambda\gamma) = T_{L/K}(\alpha, \beta) + \lambda T_{L/K}(\alpha, \gamma)$ and one concludes the K-bilinearity of $T_{L/K}$. □

Definition 2.32. *Let L/K be a separable finite field extension and $\alpha_1, \dots, \alpha_n$ a basis of L over K. Let T denote the trace form of L/K. The discriminant of this this basis is defined by*

$$d(\alpha_1, \dots, \alpha_n) = \det \begin{bmatrix} T(\alpha_1, \alpha_1) & T(\alpha_1, \alpha_2) & \cdots & T(\alpha_1, \alpha_n) \\ T(\alpha_2, \alpha_1) & T(\alpha_2, \alpha_2) & \cdots & T(\alpha_2, \alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ T(\alpha_n, \alpha_1) & T(\alpha_n, \alpha_2) & \cdots & T(\alpha_n, \alpha_n) \end{bmatrix}.$$

Observe the discriminant for any basis chosen is in K, because the matrix $[T(\alpha_i, \alpha_j)]_{1 \le i,j \le n}$ has coefficients in K. Now suppose that $[L : K] = n$ and let $\overline{K}$ be the algebraic closure of K containing L. Since the field extension is separable, then $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$ contains n elements. Observe that

$$T(\alpha_i, \alpha_j) = \mathrm{Tr}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j).$$

Considering the matrix $U = [\sigma_i(\alpha_j)]_{1 \le, i, \le n}$, one observes that

$$[U^t U]_{ij} = \sum_{k=1}^{n} [U^t]_{ik}[U]_{kj} = \sum_{k=1}^{n} [U]_{ki}[U]_{kj} = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = T(\alpha_i, \alpha_j).$$

Thus $d(\alpha_1, \dots, \alpha_n) = \det[T(\alpha_i, \alpha_j)] = \det(U^t U) = \det(U)^2 = \big(\det[\sigma_i(\alpha_j)]\big)^2$ and one has the following result

Proposition 2.33. *Let L/K be a separable finite field extension with $[L : K] = n$ and $\alpha_1, \dots, \alpha_n$ a basis of L over K. Consider $\overline{K}$ the algebraic closure of K containing L and denote $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_n\}$. Then*

$$d(\alpha_1, \dots, \alpha_n) = \det \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}^2$$

In particular, if θ is a primitive element of L/K, then $d(1, \theta, \dots, \theta^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\theta) - \sigma_j(\theta))^2$.

Proof: The part already was proved. Let's prove the second one. Observe that $\sigma_i(\theta^j) = \sigma_i(\theta)^j$.

Thus

$$d(1,\theta,\ldots,\theta^{n-1}) = \det \begin{bmatrix} 1 & \sigma_1(\theta) & \cdots & \sigma_1(\theta)^{n-1} \\ 1 & \sigma_2(\theta) & \cdots & \sigma_2(\theta)^{n-1} \\ 1 & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\theta) & \cdots & \sigma_n(\theta)^{n-1} \end{bmatrix}^2 = \left(\prod_{1\leq i<j\leq n} (\sigma_i(\theta)-\sigma_j(\theta)) \right)^2 = \prod_{1\leq i<j\leq n} (\sigma_i(\theta)-\sigma_j(\theta))^2$$

□

A natural question is: Given two bases $\alpha_1,\ldots,\alpha_n$ and $\beta_1,\ldots,\beta$ of a finite field extension L/K, what is the relation between $d(\alpha_1,\ldots,\alpha_n)$ and $d(\beta_1,\ldots,\beta_n)$?

Proposition 2.34. *Let L/K be a separable finite field extension with $[L:K]=n$, $\alpha=\{\alpha_1,\ldots,\alpha_n\}$ and $\beta=\{\beta_1,\ldots,\beta_n\}$ bases of L over K. Let $A=[I_n]_\alpha^\beta$ be the basis change matrix, then*

$$d(\beta_1,\ldots,\beta_n) = \det(A)^2 d(\alpha_1,\ldots,\alpha_n).$$

In particular $d(\gamma_1,\ldots,\gamma_n)\neq 0$ for any basis $\{\gamma_1,\ldots,\gamma_n\}$ of L over K.

Proof: Denote $A=[a_{ij}]_{1\leq i,j\leq n}$. Then

$$\beta_i = \sum_{k=1}^n a_{ki}\alpha_k$$

for all $1\leq i\leq n$. Denoting by $D_\alpha = [T(\alpha_i,\alpha_j)]_{1\leq i,j\leq n}$ and $D_\beta = [T(\beta_i,\beta_j)]_{1\leq i,j\leq n}$, then

$$\begin{aligned}[D_\beta]_{ij} = T(\beta_i,\beta_j) = T\left(\sum_{k=1}^n a_{ki}\alpha_k, \sum_{l=1}^n a_{lj}\alpha_l\right) &= \sum_{k=1}^n\sum_{l=1}^n a_{ki}a_{lj}T(\alpha_k,\alpha_l) = \sum_{k=1}^n\sum_{l=1}^n [A]_{ki}[A]_{lj}T(\alpha_k,\alpha_l) \\ = \sum_{k=1}^n\sum_{l=1}^n [A]_{ki}[A]_{lj}T(\alpha_k,\alpha_l) = \sum_{k=1}^n [A]_{ki}[D_\alpha A]_{kj} &= \sum_{k=1}^n [A^t]_{ik}[D_\alpha A]_{kj} = [A^tD_\alpha A]_{ij}.\end{aligned}$$

Hence

$$d(\beta_1,\ldots,\beta_n) = \det(D_\beta) = \det(A^tD_\alpha A) = \det(A)^2 d(\alpha_1,\ldots,\alpha_n).$$

Finally let $\{\gamma_1,\ldots,\gamma_n\}$ be a basis of L/K. Since L/K is separable, let θ be a primitive element of this extension. Thus there is a non-singular matrix A such that

$$d(\gamma_1,\ldots,\gamma_n) = \det(A)^2 \prod_{1\leq i<j\leq n} (\sigma_i(\theta)-\sigma_j(\theta))^2,$$

where $\mathrm{Hom}_K(L,\overline{K}) = \{\sigma_1,\ldots,\sigma_n\}$. Since $\prod_{1\leq i<j\leq n}(\sigma_i(\theta)-\sigma_j(\theta))^2\neq 0$, the statement follows. □

Proposition 2.35. *Let A be an integrally closed integral domain and $K = \operatorname{Quot}(A)$. Let L/K be a finite field extension and consider B the integral closure of L over A. Given $\beta \in L$ and $p(x)$ the minimal polinomial of β over K, then $\beta \in B$ if and only if $p(x) \in A[x]$.*

Proof: Suppose that $p(x) \in A[x]$. Since the minimal polynomial is monic by definition, then, by definition, one has β is integral over A.

On the other hand suppose β is integral over A and let $f(x) \in A[x]$ such that $f(\beta) = 0$. Since $p(x)$ is the minimal polynomial of β over K, there is $g(x) \in K[x]$ such that $f(x) = p(x)g(x)$. Let $\overline{L}$ be the integral closure of L. Note that if $\gamma \in \overline{L}$ is zero of $p(x)$, then γ is zero of $f(x)$, which implies that every zero of $p(x)$ is integral over A. Thus

$$p(x) = \prod_{k=1}^{n} (x - \gamma_k) = \sum_{k=1}^{n} r_k x^k,$$

where $r_i \in A[\gamma_1, \ldots, \gamma_n]$ for all $i = 0, \ldots, n$. Finally, since A is integrally closed and $\gamma_1, \ldots, \gamma_n \in \overline{A}^{\overline{L}}$, then

$$r_i \in \overline{A}^{\overline{L}} \cap K = \overline{A}^{K} = A$$

for all $i = 0, \ldots, n$, which implies that $p(x) \in A[x]$. □

Proposition 2.36. *Let A be an integrally closed integral domain and $K = \operatorname{Quot}(A)$. Let L/K be a separable finite field extension and consider B the integral closure of L over A. Let $T = \operatorname{Tr}_{L/K}$ and $\mathrm{N} = \mathrm{N}_{L/K}$ be the trace and norm functions, respectively. Then, for all $b \in B$, $T(b) \in A$ and $\mathrm{N}(b) \in A$.*

Proof: Let C be the integral closure of $\overline{K}$ in A. Since every element $\sigma \in \operatorname{Hom}_K(L, \overline{K})$ fixes K, then $\sigma(b)$ is also integral over A. Thus

$$T(b) = \sum_{\sigma \in \operatorname{Hom}_K(L,\overline{K})} \sigma(b) \in C \qquad \text{and} \qquad \mathrm{N}(b) = \prod_{\sigma \in \operatorname{Hom}_K(L,\overline{K})} \sigma(b) \in C$$

As A is integrally closed and $T(b), \mathrm{N}(b) \in K$, one concludes that

$$T(b), \mathrm{N}(b) \in C \cap K = \overline{A}^{\overline{K}} \cap K = \overline{A}^{K} = A.$$

□

Proposition 2.37. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a separable finite field extension and consider B the integral closure of L over A. Consider $\mathrm{N} = \mathrm{N}_{L/K}$ the norm function and $b \in B$. Then $b \in B^\times$ if and only if $\mathrm{N}(b) \in A^\times$.*

Proof: Suppose that $b \in B^\times$, then there is $b^{-1} \in B$ such that $b^{-1}b = bb^{-1} = 1$. Since N is multiplicative and $\mathrm{N}(1) = 1$, we obtain

$$\mathrm{N}(b)\,\mathrm{N}(b^{-1}) = \mathrm{N}(bb^{-1}) = \mathrm{N}(1) = 1 = \mathrm{N}(1) = \mathrm{N}(b^{-1}b) = \mathrm{N}(b^{-1})\,\mathrm{N}(b).$$

Thus $\mathrm{N}(b)$ is unity in A. Conversely suppose that $\mathrm{N}(b)$ is unity in A, then there is $a \in A$ such that $a\,\mathrm{N}(b) = 1$. Since the extension is separable, let $\overline{K}$ the algebraic closure of K containing L and let $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1 = inc, \sigma_2, \ldots, \sigma_n\}$. Thus

$$1 = a\,\mathrm{N}(b) = ab\prod_{k=2}^{n}\sigma_k(b) = b \cdot \underbrace{\left(a\prod_{k=2}^{n}\sigma_k(b)\right)}_{\gamma} = b\gamma.$$

Thus $\gamma = b^{-1} \in \mathrm{Quot}(B) = L$. Since $\gamma \in \overline{A}^{\overline{K}}$

$$\gamma \in \overline{A}^{\overline{K}} \cap L = \overline{A}^{L} = B,$$

which implies that $b \in B^\times$. □

Definition 2.38. *Let L/K be a finite field extension and $\alpha \in L$. The characteristic polynomial $\mathrm{charpol}_K^\alpha(x)$ of α over K is the polynomial characteristic of linear operator*

$$m_\alpha : L \longrightarrow L$$

$$x \longmapsto \alpha x$$

Lemma 2.39. *Let L/K be a finite and separable field extension and $\alpha \in L$. Then the polynomial characteristic of x over K the $[L : K(x)]$-power of $\mathrm{Irr}_K^x(t)$.*

Proof: Indeed let $1, \ldots, x^{m-1}$ be a basis of $K(x)/K$, and if $\alpha_1, \ldots, \alpha_d$ is a basis of $L/K(x)$, then

$$\alpha_1, \alpha_1 x, \ldots, \alpha_1 x^{m-1}; \ldots, \alpha_d, \alpha_d x, \ldots, \alpha_d x^{m-1}$$

is basis of L/K. The matrix of the linear transformation m_x with respect to this basis has only blocks along the diagona, each of them equal to

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & -c_m \\ 1 & 0 & 0 & \cdots & -c_{m-1} \\ 0 & 1 & 0 & \cdots & -c_{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -c_1 \end{bmatrix},$$

where

$$\operatorname{Irr}_K^x(t) = t^m + c_1 t^{m-1} + \cdots + c_m.$$

Since there are d blocks, one concludes that $\operatorname{charpol}_K^x(t) = \operatorname{Irr}_K^x(t)^d$. □

Proposition 2.40. *Let A be an integral domain and $K = \operatorname{Quot}(A)$. Let L/K be a separable finite field extension and consider B the integral closure of L over A. Let $\beta \in L$ and consider $f(x)$ the characteristic polynomial of β over K. Then β is integral over A if and only if $f(x) \in A[x]$.*

Proof: If β is integral over A, we already saw that $\operatorname{Irr}_K^\beta(x) \in A[x]$. Since $p(x) = (\operatorname{Irr}_K^\beta(x))^d$ for some $d \in \mathbb{N}$, one concludes that $f(x) \in A[x]$.

Conversely if $f(x) \in A[x]$, then β is integral over A. In fact, by definition, $f(x)$ is a monic polynomial and, by Cayley-Hamilton Theorem, $f(m_\beta) = 0$. Since

$$f(\beta) = f(m_\beta)(1) = 0,$$

one concludes that β is integral over A. □

Lemma 2.41. *Let A be an integrally closed integral domain and $K = \operatorname{Quot}(A)$. Let L/K be a separable finite field extension and consider B the integral closure of L over A. Let $\alpha_1, \ldots, \alpha_n$ be a basis of L/K such that $\alpha_i \in B$ for all $i = 1, \ldots, n$ and $d = d(\alpha_1, \ldots, \alpha_n)$. Then*

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Proof: Let $\alpha \in B$, then there is $r_1, \ldots, r_n \in K$ such that $\alpha = \sum_{k=1}^n r_k \alpha_k$. Given $1 \leq i \leq n$, observe that

$$\operatorname{Tr}(\alpha_i \alpha) = \sum_{j=1}^n r_k \operatorname{Tr}(\alpha_i \alpha_j).$$

Thus

$$\begin{bmatrix} \mathrm{Tr}(\alpha_1\alpha) \\ \mathrm{Tr}(\alpha_2\alpha) \\ \vdots \\ \mathrm{Tr}(\alpha_n\alpha) \end{bmatrix} = \begin{bmatrix} \mathrm{Tr}(\alpha_{11}) & \mathrm{Tr}(\alpha_{12}) & \cdots & \mathrm{Tr}(\alpha_{1n}) \\ \mathrm{Tr}(\alpha_{21}) & \mathrm{Tr}(\alpha_{22}) & \cdots & \mathrm{Tr}(\alpha_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\alpha_{n1}) & \mathrm{Tr}(\alpha_{n2}) & \cdots & \mathrm{Tr}(\alpha_{nn}) \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix} = M \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix}$$

Using the adjoint matrix identity, one has $M\,\mathrm{adj}(M) = \mathrm{adj}(M)M = \det(M)I_n = d(\alpha_1, \ldots, \alpha_n)I_n = dI_n$. Since $\mathrm{Tr}(\alpha_i\alpha) \in A$ for all $1 \leq i \leq n$, one concludes that $dr_i \in A$ for all $1 \leq i \leq n$. Finally

$$d\alpha = d\left(\sum_{k=1}^{n} r_k\alpha_k\right) = \sum_{k=1}^{n} \underbrace{dr_k}_{\in A} \alpha_k \in A\alpha_1 + \cdots + A\alpha_n.$$

□

Lemma 2.42. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a field extension and consider B the integral closure of L over A.*

(i): If M is a free finitely generated A-submodule of L, then

$$\mathrm{rank}_A(M) = \dim_K(\mathrm{Span}_K(M)).$$

(ii): If $\gamma \in L \setminus \{0\}$ and If M is a free finitely generated A-submodule of L, then

$$m : M \longrightarrow \gamma M$$
$$m \longmapsto \gamma m$$

is an A-module isomorphism.

Proof: (i) : Let $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ be a basis of M as A-module. I claim that $\mathcal{B}$ also is basis of $\mathrm{Span}_K(M)$ as K-linear space. In fact, trivially $\mathcal{B}$ generates $\mathrm{Span}_K(M)$ as K-linear space. Now let $r_1/s_1, \ldots, r_n/s_n \in K$ such that

$$\frac{r_1}{s_1}\alpha_1 + \cdots + \frac{r_n}{s_n}\alpha_n = 0.$$

Let $s = s_1 \cdots s_n$. Multiplying the equation above by s, one gets

$$\left(s\frac{r_1}{s_1}\right)\alpha_1 + \cdots + \left(s\frac{r_n}{s_n}\right)\alpha_n = 0,$$

where $sr_i/s_i \in A$ for all $i = 1, \dots, n$. Since $\mathcal{B}$ is basis of M as A-module and $s \neq 0$, then $r_i/s_i = 0$ for all $i = 1, \dots, n$. Thus $\mathcal{B}$ is also basis of $\mathrm{Span}_K(M)$ as K-linear space.

(ii): It is clear that γM is also an A-module and that m is a surjective A-linear mapping. If $m(x) = m(y)$, then $\gamma x = \gamma y$. Since $\gamma \neq 0$ and L is a field, one concludes that $x = y$, which implies that m is one-to-one and so an isomorphism. □

Theorem 2.43. *Let A be an integral domain and $K = \mathrm{Quot}(A)$. Let L/K be a separable finite field extension and consider B the integral closure of L over A. Let M be a non-zero finitely generated B-submodule of L.*

- *(i): If A is Noetherian and integrally closed ring, then M is a finitely generated A-module. In particular B is a finitely generated A-module.*
- *(ii): If A is a PID, then M is a free module with $\mathrm{rank}_A(M) = [L : K]$. In particular B is a free finitely generated A-module.*

Proof: Let $\mu_1, \dots, \mu_r$ be a set of generators of M as B-module. Since $M \neq 0$, one can suppose without lost of generality that $r \geq 1$ and $\mu_i \neq 0$ for all $i = 1, \dots, r$. We know that there exists $a \in A \setminus \{0\}$ such that $a\mu_i \in B$ for all $1 \leq i \leq r$, which implies $aM \subseteq B$. Let $\beta \in aM$, then

$$\beta = a \sum_{k=1}^{r} b_j \mu_j = \sum_{k=1}^{r} b_j (a\mu_j) \in B$$

Thus, if $\alpha_1, \dots, \alpha_n$ is a basis of L/K such that $d(\alpha_1, \dots, \alpha_n)B = dB \subseteq A\alpha_1 + \cdots + A\alpha_n$, then

$$daM \subseteq dB \subseteq A\alpha_1 + \cdots + A\alpha_n.$$

Since $\alpha_1, \dots, \alpha_n$ is basis of L/K, then $A\alpha_1 + \cdots + A\alpha_n \cong A^n$ is a free finitely generated A-module.
(i): Since A is a Noetherian ring, A^n is a finitely generated A-module, thus daM also is a finitely generated A-module. Since daM is isomorphic to M as A-module, one concludes that M also is a finitely generated A-module.
(ii): Since A^n is a free finitely generated A-module and A is a PID, then daM also is a finitely generated free module and with $\mathrm{rank}(daM) \leq n = [L : K]$. Similarly, since daM is isomorphic to M as A-module, one concludes that M is a free finitely generated A-module $\mathrm{rank}_A(M) = \mathrm{rank}(daM) \leq n$.

In particular, B is a free finitely generated A-module and $\operatorname{rank}_A(B) \leq n$. Finally, since

$$\operatorname{rank}_A(B) = \dim_K(\operatorname{Span}_K(B)) = \dim_K(L) = n,$$

and $\mu_i B \subseteq M$, then

$$n = \operatorname{rank}_A(B) = \operatorname{rank}(\mu_i B) \leq \operatorname{rank}_A(M)$$

and so $\operatorname{rank}_A(M) = n$. □

Definition 2.44. *Let A be an integral domain and $K = \operatorname{Quot}(A)$. Let L/K be a finite field extension and consider B the integral closure of L over A. If B is a free finitely generated A-module and $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ is a basis of B over A, then $\mathcal{B}$ is called an integral basis of L/K.*

Remark 2.45. *Since $\operatorname{Span}_K(B) = L$, an integral basis is indeed a basis of L as K-linear space.*

Now let $K/\mathbb{Q}$ be a finite field extension and $\mathcal{M} \subseteq K$ be a non-zero finitely generated $\mathcal{O}_K$-submodule of K. We know that $\mathcal{M}$ is an free abelian group with $\operatorname{rank}_{\mathbb{Z}}(\mathcal{M}) = [K : \mathbb{Q}] := n$.

Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be basis of $\mathcal{M}$ over $\mathbb{Z}$ and so basis of K as $\mathbb{Q}$-linear space. Observe that there are $r_{ij} \in \mathbb{Z}$ with $1 \leq i, j \leq n$ such that

$$\beta_i = \sum_{k=1}^{n} r_{ij}\alpha_i.$$

Calling $M = [r_{ij}]$, then $d(\beta_1, \ldots, \beta_n) = d(\alpha_1, \ldots, \alpha_n)\det(M)^2$. However $\det(M)$ is unit in $\mathbb{Z}$, which implies that

$$d(\beta_1, \ldots, \beta_n) = d(\alpha_1, \ldots, \alpha_n).$$

Definition 2.46. *Let $K/\mathbb{Q}$ be a finite field extension. If $\mathcal{M}$ is a nonzero finitely generated $\mathcal{O}_K$-submodule of L. Then*

(i): The discriminant of M, denoted by $d(M)$, is defined by $d(M) = d(\alpha_1, \ldots, \alpha_n)$, where $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of K over $\mathbb{Q}$.

(ii): The discriminant of extension $K/\mathbb{Q}$, denoted by d_K, is the discriminant of $\mathcal{O}_K$.

Proposition 2.47. *Let $K/\mathbb{Q}$ be a finite field extension and $\mathcal{N} \subseteq \mathcal{M} \subseteq K$ be non-zero finitely generated $\mathcal{O}_K$-submodules of K. Then*

$$d(\mathcal{N}) = [\mathcal{M} : \mathcal{N}]^2 d(\mathcal{M}).$$

Proof: Note that $\mathcal{M}$ and $\mathcal{N}$ are free modules over $\mathbb{Z}$ with $\text{rank}_{\mathbb{Z}}(\mathcal{M}) = \text{rank}_{\mathbb{Z}}(\mathcal{N}) = [L : K] = n$. Since $\text{rank}_{\mathbb{Z}}(\mathcal{M})$, $\text{rank}_{\mathbb{Z}}(\mathcal{N}) < \infty$, then $\text{rank}_{\mathbb{Z}}(\mathcal{M}/\mathcal{N}) < \infty$. Moreover

$$\text{rank}_{\mathbb{Z}}(\mathcal{M}/\mathcal{N}) = \text{rank}_{\mathbb{Z}}(\mathcal{M}) - \text{rank}_{\mathbb{Z}}(\mathcal{N}) = 0.$$

Thus $\mathcal{M}/\mathcal{N}$ is a torsion abelian group, which implies that there are $a_1, \ldots, a_n \in \mathbb{Z}$ such that

$$\frac{\mathcal{M}}{\mathcal{N}} \cong \frac{\mathbb{Z}}{a_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{a_n\mathbb{Z}}.$$

Let $\beta_1, \ldots, \beta_n$ be a basis of $\mathcal{M}$ over $\mathbb{Z}$. Observe then that $a_1\beta_1, \ldots, a_n\beta_n$ is basis of $\mathcal{N}$ over $\mathbb{Z}$. Since $M = diag(a_1, \ldots, a_n)$ is change basis matrix of $\{\beta_1, \ldots, \beta_n\}$ to $\{a_1\beta_1, \ldots, a_n\beta_n\}$, then

$$d(\mathcal{N}) = d(a_1\beta_1, \ldots, a_n\beta_n) = \det(M)^2 d(\beta_1, \ldots, \beta_n) = (a_1 \cdots a_n)^2 d(\mathcal{M})$$

However $[\mathcal{M} : \mathcal{N}] = |\mathcal{M}/\mathcal{N}| = a_1 \cdots a_n$, thus the identity follows. □

2.4 Quadratic Extensions of $\mathbb{Q}$

Proposition 2.48. *Let $q \in \mathbb{Q}$. Then $f(x) = x^2 - q$ is irreducible in $\mathbb{Q}[x]$ if and only if q is not square of a rational number.*

Proof: Suppose that r is square of a rational number, then $r = s^2$ for some $s \in \mathbb{Q}$. Thus

$$f(x) = x^2 - r = x^2 - s^2 = (x - s)(x + s)$$

is a reducible polymial in $\mathbb{Q}[x]$. Conversely if $f(x)$ is reducible in $\mathbb{Q}[x]$, there exist $a, b \in \mathbb{Q}$ such that

$$f(x) = x^2 - r = (x - a)(x - b),$$

which implies that $a + b = 0$ and $ab = -r$. So $r = -a(-a) = a^2$ is square a rational number. □

Thus there is a map Θ between $\mathbb{Q} \setminus \mathbb{Q}^2$ and the family of quadratic extensions of $\mathbb{Q}$.

$$\Theta : r \longmapsto \mathbb{Q}(r)$$

This map is surjective, because every extension of $\mathbb{Q}$ is obtained by adjoining a non-rational complex number r such that $r^2 \in \mathbb{Q}$. Defining

$$\mathcal{D} = \{d \in \mathbb{Z} \ ; \ d \neq 1, d \text{ is square free}\}.$$

then one has the following Proposition

Proposition 2.49. *Let $\mathcal{F}_2$ be the family of all field extension of $\mathbb{Q}$ of degree 2, then there is an one-to-one correspondence*

$$\phi : \mathcal{D} \longrightarrow \mathcal{F}_2$$

$$d \longmapsto \mathbb{Q}(\sqrt{d})$$

Proof: Indeed let $q \in \mathbb{Q} \backslash \mathbb{Q}^2$, then we can write $q = r/s$ such that $\gcd(r, s) = 1$ and $s \geq 1$. Moreover there exist $r', r'', s', s'' \in \mathbb{Z}$ such that r'', s'' are perfect squares, r', s' are square free and $r = r'r''$, $s = s's''$. Thus

$$\sqrt{q} = \sqrt{\frac{r'r''}{s's''}} = \frac{\sqrt{r''}}{\sqrt{s''}}\frac{\sqrt{r'}}{\sqrt{s'}} = \frac{\sqrt{r''}}{\sqrt{s''}s'}\sqrt{r's'}.$$

Since $\sqrt{r''}/(\sqrt{s''}s') \in \mathbb{Q}$, then

$$\mathbb{Q}(\sqrt{q}) = \mathbb{Q}(\sqrt{r's'}),$$

where $r's'$ is square free, which implies the map ψ is surjective. Now let $d_1, d_2 \in \mathcal{D}$ and suppose $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$. Thus there are a, $b \in \mathbb{Q}$ such that $\sqrt{d_1} = a + b\sqrt{d_2}$. Taking the 2-power, one concludes that $ab = 0$. Since $\sqrt{d_1}$ is irrational, we get a contradiction if $b = 0$. Thus

$$\sqrt{d_2} = b\sqrt{d_1}$$

Taking the 2-power again, one concludes that $d_2 = b^2 d_1$. Since d_2 and d_1 are square-free, one concludes that $b^2 = 1$, which implies $d_1 = d_2$. □

Lemma 2.50. *Let $d \in \mathcal{D}$ and a, $b \in \mathbb{Q}$. Suppose that $m = 2a$ and $n = a^2 - db^2 \in \mathbb{Z}$.*

(i): If m is even, then a, $b \in \mathbb{Z}$.

(ii): If m is odd, then there is $k \in \mathbb{Z}$ such that $m = (2k + 1)/2$ and $d \equiv 1 \mod 4$

Proof: (i) : Suppose that m is even, so $a = m/2$ is integer. Now observe that $db^2 = a^2 - n = k \in \mathbb{Z}$. Denote $b = r/s$ with $\gcd(r, s) = 1$ and $s \geq 1$. Thus $dr^2 = ks^2$. Suppose that $s \neq 1$, thus there exists p prime such that $p^2 | dr^2$. However, since $\gcd(r, s) = 1$, then $p^2 | d$, which gives a contradiction, because d is square free. Then $s = 1$ and $b \in \mathbb{Z}$

(ii): Suppose that m is odd, then there exists $v \in \mathbb{Z}$ such that $m = 2v + 1$. Thus

$$a = \frac{m}{2} = \frac{2v + 1}{2}.$$

Thus $db^2 = a^2 - n = v^2 + v + 1/4 - n$, which implies $db^2 = t + 1/4$, where $t = v^2 + v - n \in \mathbb{Z}$. Suppose that $b = r/s$ with $\gcd(r, s) = 1$. Thus $4dr^2 = 4s^2t + s^2$, thus $s^2 \equiv 0 \mod 4$, which implies that $s \equiv 0 \mod 2$ and so $s = 2h$. Since $\gcd(r, s) = 1$, we still have $\gcd(r, h) = 1$.

2.5 Ideals

Lemma 2.51. *Let $K/\mathbb{Q}$ be a finite field extension and denote $\mathrm{N} : K \longrightarrow \mathbb{Q}$ the norm function. Then*

(i) $\mathrm{N}(x) = 0$ *if and only if* $x = 0$.

(ii) Given $x \in \mathcal{O}_K$, $|\,\mathrm{N}(x)| = 1$ *if and only if* $x \in \mathcal{O}_K^\times$.

Proof: (i) : Note that $\mathrm{N}(x) = \det([m_x]) = 0$ if and only if the operator m_x is singular and m_x is singular if and only if $x = 0$.

(ii) : It follows from Proposition 2.37. □

Proposition 2.52. *Let $K/\mathbb{Q}$ be a finite field extension and $\alpha \in \mathcal{O}_K \setminus (\mathcal{O}^\times \cup \{0\})$. Then there are $r \geq 1$ and $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$ irreducible elements such that $\alpha = \alpha_1\alpha_2 \cdots \alpha_r$. In particular, $\mathcal{O}_K$ is a factorization domain.*

Proof: Denote $N = N_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q}$. Remember that the norm function$N(\gamma) \in \mathbb{Z}$ for all $\gamma \in \mathcal{O}_K$. Since α is not irreducible, then $|\,\mathrm{N}(\alpha)| \geq 2$. One will prove this result by induction on $|N(\alpha)|$. Let $k \geq 2$ and suppose that if $2 \leq |\,\mathrm{N}(\alpha)| < k$, then α is finite product of irreducible elements. Now suppose that $\mathrm{N}(\alpha) = k$. If α is irreducible, we are done. If not, then $\alpha = \beta\gamma$, where $\beta, \gamma \in \mathcal{O}_K \setminus (\mathcal{O}_K^\times \cup \{0\})$. Thus

$$\mathrm{N}(\alpha) = \mathrm{N}(\beta\gamma) = \mathrm{N}(\beta)\,\mathrm{N}(\gamma).$$

Since neither β nor γ are unit elements in $\mathcal{O}_K$, then $|\,\mathrm{N}(\beta)| \geq 2$ and $|\,\mathrm{N}(\gamma)| \geq 2$, which implies that

$$2 \leq \mathrm{N}(\beta) < k \qquad\qquad 2 \leq \mathrm{N}(\gamma) < k.$$

By induction hypothesis, β and γ are finite product of irreducible elements, so the statement follows. □

Example 2.53. *Consider $K = \mathbb{Q}(\sqrt{-5})$. Note that $K/\mathbb{Q}$ is a Galois extension and*

$$\mathrm{Gal}(K/\mathbb{Q}) = \{1_K,\ a + b\sqrt{-5} \longmapsto a - b\sqrt{-5}\}$$

Thus $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q}$ is such that $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2$. Observe that

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

Using the norm function, we can prove that each of factors above is irreducible in $\mathcal{O}_K$, so we conclude that $\mathcal{O}_K$ is not necessarily an unique factorization domain.

Inspired by the discovery of complex numbers, Kummer thought that ring of integers of any finite extension K of $\mathbb{Q}$ would admit an embedding into a bigger domain of "ideal numbers", where the unique factorization property into "ideal prime numbers" would hold. For instance, in the example of

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

the factors of 21 would be composed of ideal prime numbers $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ subject to the rules

$$3 = \mathfrak{p}_1\mathfrak{p}_2, \quad 7 = \mathfrak{p}_3\mathfrak{p}_4, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, \quad 1 - 2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4$$

This would resolve the above non-uniqueness into the wonderfully unique factorization

$$21 = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4).$$

The Kummer's concept of "ideal numbers" was later replaced by that of ideals of the ring $\mathcal{O}_K$ under the following reason: Whatever an ideal number $\mathfrak{a}$ should be defined to be, it ought to be linked ti certain numbers $a \in \mathcal{O}_K$ by the divisility relation $\mathfrak{a}|a$ satisfying the following rules, for all $a, b, \lambda \in \mathcal{O}_K$, then

$$\mathfrak{a}|a \quad \text{and} \quad \mathfrak{a}|b \quad \Longrightarrow \quad \mathfrak{a}|(a \pm b); \quad \mathfrak{a}|a \quad \Longrightarrow \quad \mathfrak{a}|\lambda a$$

and an ideal number $\mathfrak{a}$ should be determined by the totality of its divisors in $\mathcal{O}_K$

$$\mathfrak{a} = \{a \in \mathcal{O}_K \ ; \ \mathfrak{a}|a\}.$$

But in view of the rules for divisibility, this set is an ideal of $\mathcal{O}_K$.

Proposition 2.54. *Let $K/\mathbb{Q}$ be a finite field extension and $\mathcal{O}_K = \overline{\mathbb{Z}}^K$. Then*

(i): $\mathcal{O}_K$ is a Noetherian ring;

(ii): $\mathcal{O}_K$ is an integrally closed integral domain;

(iii): $\dim(\mathcal{O}_K) = 1$.

Proof: (i) : Since $\mathbb{Z}$ is a Noetherian ring and $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, then $\mathcal{O}_K$ is a Noetherian module. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$, thus $\mathfrak{a}$ is a submodule of $\mathcal{O}_K$, thus $\mathfrak{a}$ is finitely generated $\mathbb{Z}$-module. In particular $\mathfrak{a}$ is finitely generated $\mathcal{O}_K$-module, which implies that $\mathfrak{a}$ is a finitely generated ideal. Thus $\mathcal{O}_K$ is a Noetherian ring

(ii) : Since $\mathcal{O}_K$ is a subring of a field, $\mathcal{O}_K$ is an integral domain. Moreover, as $\mathrm{Quot}(\mathcal{O}_K) = K$ and $\mathcal{O}_K = \overline{\mathbb{Z}}^K$, then

$$\overline{\mathcal{O}_K}^K = \overline{\overline{\mathbb{Z}}^K}^K = \overline{\mathbb{Z}}^K = \mathcal{O}_K.$$

Which implies that $\mathcal{O}_K$ is an integrally closed integral domain.

(iii): Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Now $\mathcal{O}_K \cap \mathbb{Z} = (p)$ for some prime number p. Let $y \in \mathfrak{p}$, $y \neq 0$ and

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

be an equation with $a_i \in \mathbb{Z}$ and $a_n \neq 0$. Note that $a_n = -(y^n + a_1 y^{n-1} + \cdots + a_{n-1} y) \in \mathcal{O}_K \cap \mathbb{Z}$. Thus observe that $\mathcal{O}_K/\mathfrak{p}$ is an integral extension of $\kappa = \mathbb{Z}/p\mathbb{Z}$. Since κ is a field, one concludes that $\mathcal{O}_K/\mathfrak{p}$ also is a field, which implies that $\mathfrak{p}$ is maximal. □

Definition 2.55. *Let A be an integral domain. A is called a Dedekind domain if A is Noetherian, integrally closed and if A has Krull dimension* 1*.*

Definition 2.56. *Let A be an integral domain and B an A-algebra. Define*

$$Mod_A(B) = \{M \subseteq B \ ; \ M \textit{ is } A\textit{-submodule of } B\}.$$

Moreover given $M \in Mod_A(B)$, define

$$\widehat{M} = \{b \in B \ ; \ bM \subseteq A\}.$$

Proposition 2.57. *Let A be an integral domain and B an A-algebra. Given M, $N \in Mod_A(B)$, then*

(i): $\widehat{M} \in Mod_A(B)$;

(ii): If $M \subseteq A$, *then* $A \subseteq \widehat{M}$;

(iii): $\widehat{0} = B$;

(iv): Defining

$$MN := \left\{ \sum_{k=1}^{n} x_k y_k \ ; \ x_k \in M,\, y_k \in N,\, n \in \mathbb{N} \right\},$$

then $M\widehat{M} \subseteq A$;

(v): If $N \subseteq M$, *then* $\widehat{M} \subseteq \widehat{N}$.

Proof: Trivial □

Lemma 2.58. *Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Given A-ideals I, J, if $IJ \subseteq \mathfrak{p}$, then $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.*

Proof: Suppose by contradiction that $I \not\subseteq \mathfrak{p}$ and $J \not\subseteq \mathfrak{p}$, then there are x, $y \in A$ such that $x \in I \setminus \mathfrak{p}$ and $y \in J \setminus \mathfrak{p}$. By hypothesis, $xy \in IJ \subseteq \mathfrak{p}$. Using the primality of $\mathfrak{p}$, one concludes that $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, which is a contradiction. □

Corollary 2.59. *Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Given a finite family $I_1, \dots, I_n$ of ideals of A, if*

$$\prod_{k=1}^{n} I_k \subseteq \mathfrak{p},$$

then $I_k \subseteq \mathfrak{p}$ for some $k = 1, \dots, n$.

Proof: It is trivial. Proceed by induction on number of ideals. □

Lemma 2.60. *Let $\mathcal{O}$ be a Dedekind domain and $\mathfrak{a}$ be a nonzero $\mathcal{O}$-ideal. Then there exist nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ such that*

$$\prod_{k=1}^{n} \mathfrak{p}_k \subseteq \mathfrak{a}.$$

Proof: Suppose that this property does not hold in general and let

$$\mathfrak{M} = \{\mathfrak{a} \subseteq \mathcal{O} \ ; \ \text{There are no prime ideals } \mathfrak{p}_1, \dots, \mathfrak{p}_n \text{ such that } \mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}\}.$$

Thus $\mathfrak{M} \neq \emptyset$ and we can equip this set with inclusion order. Since $\mathcal{O}$ is a Noetherian ring, $\mathfrak{M}$ has a maximal element $\mathfrak{q}$. Observe that $\mathfrak{q}$ can not be a prime ideal, then there is $a, b \in \mathcal{O} \setminus \mathfrak{q}$ such that $ab \in \mathfrak{q}$. Consider the ideals $I = \mathfrak{q} + (a)$ and $J = \mathfrak{q} + (b)$. Thus

$$IJ = (\mathfrak{q} + (a))(\mathfrak{q} + (b)) \subseteq \mathfrak{q},$$

By maximality of $\mathfrak{q}$ in $\mathfrak{M}$, there are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n, \mathfrak{p}'_1, \dots, \mathfrak{p}'_m$ such that

$$\prod_{k=1}^{n} \mathfrak{p}_k \subseteq I_1 \qquad \text{and} \qquad \prod_{k=1}^{m} \mathfrak{p}'_k \subseteq I_2.$$

Then

$$\left(\prod_{k=1}^{n} \mathfrak{p}_k\right)\left(\prod_{k=1}^{m} \mathfrak{p}'_k\right) \subseteq I_1 I_2 \subseteq \mathfrak{q},$$

which contradicts the fact that $\mathfrak{q} \in \mathfrak{M}$. Thus $\mathfrak{M} = \emptyset$ and the statement follows. □