UFRJ

Algebraic Number Theory

Kevin Alves Vasconcellos

These notes were written during the course of Algebraic Number Theory in first semester of 2021 at Federal University of Rio de Janeiro. They contain the resolution of almost all exercises of two first chapters of book *Algebraic Number Fields* of Gerald J. Janusz, first edition and some exercises of the second edition. I hope this material may be useful for someone. 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

Subrings of Fields

1.1 Localization

Lemma I: Let R and T be commutative rings and S be a multiplicatively closed subset of R. Let $g : R \longrightarrow T$ be a ring homomorphism satisfying the following properties:

(i) $g(S) \subseteq T^{\times} := \{x \in T \ ; \ x \text{ is invertible}\}$;

(ii) Given $a \in R$, if $g(a) = 0$, then there is $s \in S$ such that $sa = 0$;

(iii) Every element of T is of form $g(a)g(s)^{-1}$ for some $a \in R$ and $s \in S$.

Then there is unique isomorphism $h : R_S \longrightarrow T$ making the following diagram

$$\begin{tikzcd}
R \arrow[rr, "\phi"] \arrow[dr, "g"'] & & R_S \arrow[dl, "h"] \\
& T &
\end{tikzcd}$$

commutes.

Proof: By the universal property of localization, there is a unique ring homomorphism $h : R_S \longrightarrow T$ which makes the diagram above commute. It is enough to prove that h is an isomorphism. We also know that $h(x/s) = g(x)g(s)^{-1}$ for every $x/s \in R_S$, so by property (iii), it is clear that h is surjective. Let's prove now that h is injective. Suppose that $h(x/s) = 0$, thus $g(x)g(s)^{-1} = 0$. Since $g(s)^{-1}$ is invertible, multiplying by its inverse, we get that $g(x) = 0$. However, by hypothesis (ii), we can find $t \in S$ such that $tx = 0$, which implies that $s/x = 0$. Thus h is a ring isomorphism. □

Question 1: Let R be an integral domain and S a multiplicative set in R; Let $S^* = S \cup \{1\}$. Show that $R_S \cong R_{S^*}$.

Proof: Indeed, since S is multiplicatively closed subset of R, it's clear that $S^* = S \cup \{1\}$ will be too. Define the following mapping

$$g : R \longrightarrow R_{S^*}$$

$$x \longmapsto x/1.$$

It's clear that it's is an ring homomorphism. In order to show that $R_{S^*} \cong R_S$, it's enough to apply the previous Lemma.

(i) Since $S \subseteq S^*$, then, for every $s \in S$, we have $g(s)$ is invertible in R_{S^*};

(ii) If $g(x) = 0$, then $x/1 = 0$. So there is $s \in S^*$ such that $sx = 0$. If $s \in S$, there's nothing to prove. If not $s = 1$, so $r = 0$, which implies that $sr = 0$ for every $r \in S$.

(iii) Given $x/s \in R_{S^*}$, then: If $s \neq 1$, $x/s = g(x)g(s)^{-1}$. If $s = 1$, observe that $x/1 = xt/t$ for every $t \in S$, thus

$$x/1 = xt/t = g(xt)g(t)^{-1}.$$

So, by the previous Lemma, we conclude that $R_S \cong R_{S^*}$. □

Question 2: The ideal $\mathfrak{p}$ of a commutative ring R is prime if and only if the factor ring $R/\mathfrak{p}$ is an integral domain.

Proof: Suppose that $\mathfrak{p}$ is a prime ideal of R. Let $\overline{a}, \overline{b} \in R/\mathfrak{p}$ such that $\overline{a}\overline{b} = \overline{ab} = \overline{0}$. Thus we have that $ab \in \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal of R, we get that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, thus we conclude that $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, respectively. Hence $R/\mathfrak{p}$ is an integral domain.

On the other hand, suppose that $R/\mathfrak{p}$ is an integral domain. Let $a, b \in R$ such that $ab \in \mathfrak{p}$. It will be proved that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. In fact, consider $\overline{a}$ and $\overline{b}$ the image of a and b in $R/\mathfrak{p}$, respectively. Since $ab \in \mathfrak{p}$, we have that

$$\overline{a}\overline{b} = \overline{ab} = \overline{0} \text{ in } R/\mathfrak{p}.$$

Since $R/\mathfrak{p}$ is an integral domain, we conclude that $\overline{a} = 0$ or $\overline{b} = 0$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, respectively. Hence $\mathfrak{p}$ is a prime ideal of R. □

Lemma II: Let $(R, \mathfrak{m})$ be a local ring. Then there is a ring isomorphism between R and $R_{\mathfrak{m}}$.

Proof: In fact, consider the ring homomorphism

$$g : R \longrightarrow R$$

$$x \longmapsto x.$$

Note that $g(R \smallsetminus \mathfrak{m}) = R \smallsetminus \mathfrak{m} = R^{\times}$. Thus, by the universal property, there is a ring homomorphism $h : R_{\mathfrak{m}} \longrightarrow R$ such that the following diagram commute

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, "g"'] & & R_{\mathfrak{m}} \arrow[dl, "h"] \\ & R & \end{tikzcd}$$

where ϕ is the natural localization mapping. In order to show that h is a ring isomorphism, it's enough to check the conditions of Lemma I. In fact,

(i) $g(R \smallsetminus \mathfrak{m}) = R \smallsetminus \mathfrak{m} = R^{\times}$;

(ii) Since g is the identity, if $g(x) = 0$, then $1.x = 0$;

(iii) Given $x \in R$, note that $x \in \operatorname{Im}(h)$, because $h(x/1) = g(x)g(1)^{-1} = x * 1 = 1$.

Thus h is an ring isomorphism and then $R_{\mathfrak{m}} \cong R$. □

Lemma III: Let R be a ring and S be a multiplicatively subset of R. Given an exact sequence of R-modules

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0. \end{tikzcd}$$

Then the following sequence

$$\begin{tikzcd} 0 \arrow[r] & M'_S \arrow[r, "f_S"] & M_S \arrow[r, "g_S"] & M''_S \arrow[r] & 0 \end{tikzcd}$$

is exact, where

$$f_S : M'_S \longrightarrow M_S \qquad\qquad g_S : M_S \longrightarrow M''_S$$

$$\frac{x}{s}r \longmapsto \frac{f(x)}{s} \qquad\qquad \frac{x}{s}r \longmapsto \frac{g(x)}{s}.$$

In particular, the localization in S is an exact covariant functor between the category of R-modules and the category of R_S-modules.

Proof: Firstly we have to prove that the mapping f_S and g_S are, in fact, well-defined R_S-module homomorphisms. It is enough to prove to f_S, because the case g_s is similar.. Note that if $m/s = m'/s'$, then there is $t \in S$ such that

$$t(s'm - sm') = 0 \qquad \text{that is} \qquad ts'm = tsm'.$$

Thus

$$ts'f(m) = f(ts'm) = f(tsm') = tsf(m') \qquad \text{that is} \qquad t(s'f(m) - sf(m')) = 0.$$

Then $f(m)/s = f(m')/s'$ and so f_S is well-defined. Now we will prove that f_S is a R_S-module homomorphism. Indeed, given $m/s, n/t \in M_S$, we have

$$f_S\left(\frac{m}{s} + \frac{n}{t}\right) = f_S\left(\frac{tm+sn}{ts}\right) = \frac{f(tm+sn)}{ts} = \frac{tf(m)}{ts} + \frac{sf(n)}{ts} = \frac{f(m)}{s} + \frac{f(n)}{t} = f_S\left(\frac{m}{s}\right) + f_S\left(\frac{n}{t}\right).$$

Now, given $r/s \in R_S$ and $m/t \in M_S$, we have

$$f_S\left(\frac{r}{s}\frac{m}{t}\right) = f_S\left(\frac{rm}{st}\right) = \frac{rf(m)}{st} = \frac{r}{s}\frac{f(m)}{t} = \left(\frac{r}{s}\right)f_S\left(\frac{m}{t}\right).$$

Thus f_S is R_S-module homomorphism well-defined. Now it remains to prove that the wished sequence is exact.

- f_S is injective, because if $f_S(m/s) = f(m)/s = 0$, then there is $t \in S$ such that $tf(m) = f(tm) = 0$. Since f is injective, then $tm = 0$, which implies that $m/s = 0$;

- $\operatorname{Im}(f_S) = \operatorname{Ker}(g_S)$. In fact, given any $m/s \in M'_S$, we have

  $$(g_S \circ f_S)\left(\frac{m}{s}\right) = g_S\left(\frac{f(m)}{s}\right) = \frac{(g \circ f)(m)}{s} = \frac{0}{s} = 0;$$

  Thus $\operatorname{Im}(f_S) \subseteq \operatorname{Ker}(g_S)$. On the other hand, given $m/s \in \operatorname{Ker}(g_S)$, then $g_S(m/s) = g(m)/s = 0$, thus there is $t \in S$ such that $tg(m) = g(tm) = 0$. Thus $tm \in \operatorname{Ker}(g)$. Since $\operatorname{Ker}(g) = \operatorname{Im}(f)$, there is $n \in M'$ such that $f(n) = tm$. Hence

  $$f_S\left(\frac{n}{ts}\right) = \frac{f(n)}{ts} = \frac{tm}{ts} = \frac{m}{s}.$$

  Thus $\operatorname{Ker}(g_S) \subseteq \operatorname{Im}(f_S)$, which implies that $\operatorname{Im}(f_S) = \operatorname{Ker}(g_S)$;

- g_S is surjective. In fact, Let $u/t \in M''_S$. Since g is surjective, there is $m \in M$ such that $g(m) = u$. Thus

  $$g_S\left(\frac{m}{t}\right) = \frac{f(m)}{t} = \frac{u}{t}.$$

  Thus g_s is surjective.

Then we conclude that the wished sequence is exact. Now, doing simple verifications, it is possible to conclude that the localization in S is, in fact, an exact covariant functor $\mathcal{F}$ between the category of R-modules and the category R_S-modules, where, given $M \in \mathbf{mod}_R$ and $f \in \operatorname{Hom}_R(M,N)$, we have

$$\mathcal{F}(M) = M_S \qquad \text{and} \qquad \mathcal{F}(f) = f_S \in \operatorname{Hom}_{R_S}(M_S, N_S).$$

□

Question 3: Let R be an integral domain and $\mathfrak{m}$ be a maximal ideal of R. Show there is an isomorphism between the fields $R/\mathfrak{m}$ and $R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}$.

Proof: Consider the following exact sequence R-modules

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{m}R \arrow[r, "i"] & R \arrow[r, "\pi"] & R/\mathfrak{m} \arrow[r] & 0. \end{tikzcd}$$

Since the localization is an exact functor, the following complex is also exact

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{m}R_\mathfrak{m} \arrow[r, "i"] & R_\mathfrak{m} \arrow[r, "\pi"] & (R/\mathfrak{m})_\mathfrak{m} \arrow[r] & 0. \end{tikzcd}$$

Thus there is $R_\mathfrak{m}$-module isomorphism which is also a ring isomorphism

$$\frac{R_\mathfrak{m}}{\mathfrak{m}R_\mathfrak{m}} \cong \left(\frac{R}{\mathfrak{m}}\right)_\mathfrak{m} = \left(\frac{R}{\mathfrak{m}}\right)_M.$$

where M is the image of $\mathfrak{m}$ in $R/\mathfrak{m}$. Finally note that, since $R/\mathfrak{m}$ is a local ring, because it is a field and the localization of a local ring at the maximal ideal is the same ring, we conclude that

$$\frac{R_\mathfrak{m}}{\mathfrak{m}R_\mathfrak{m}} \cong \left(\frac{R}{\mathfrak{m}}\right)_M = \frac{R}{\mathfrak{m}}.$$

□

Question 4: If S is a multiplicative set in a Noetherian domain R, then R_S is also Noetherian.

Proof: In order to show that R_S is a Noetherian ring, it is enough to show that every prime ideal of R_S is finitely generated by Cohen Theorem.. Let $\mathfrak{q}$ be a prime ideal of R_S. Thus $\mathfrak{q} \cap R$ is an ideal of R. Since R is a Noetherian ring, $\mathfrak{q} \cap R$ is finitely generated, that is, there are $x_1, \dots, x_n \in R$ such that

$$\mathfrak{q} \cap R = (x_1, \dots, x_n) \subseteq R$$

Thus

$$\mathfrak{q} = (\mathfrak{q} \cap R)R_s = (x_1/1, \dots, x_n/1) \subseteq R_S.$$

So $\mathfrak{q}$ is finitely generated. □

1.2 Integral Dependence

Question 1: Prove that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{3})$ is just $\mathbb{Z} + \mathbb{Z}\sqrt{3}$.

Proof: Note that $\sqrt{3}$ is integral over $\mathbb{Z}$, because $\sqrt{3}$ satisfies the following linear dependence equation

$$f(X) = X^2 - 3 \in \mathbb{Z}[X].$$

Denote $S := \overline{\mathbb{Z}}^{\mathbb{Q}(3)}$ the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{3})$. Since S is a subring of $\mathbb{Q}(\sqrt{3})$ containing $\mathbb{Z}$, we have

$$\mathbb{Z} + \mathbb{Z}\sqrt{3} \subseteq S,$$

It remains now to prove that $\mathbb{Z} + \mathbb{Z}\sqrt{3} = S$.

Note that $\mathbb{Z} \subseteq \mathrm{Quot}(\mathbb{Z}) = \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$. Thus, if $b \in \mathbb{Q}(\sqrt{3})$ is integral over $\mathbb{Z}$, then b is algebraic over $\mathbb{Q}$ and the minimal polynomial $p(X) \in \mathbb{Q}[X]$ of b is actually in $\mathbb{Z}[X]$ since $\mathbb{Z}$ is integrally closed. Let $x = \alpha + \beta\sqrt{3}$ be an integral element over $\mathbb{Z}$ with $\beta \neq 0$. We will prove that $x \in \mathbb{Z} + \mathbb{Z}\sqrt{3}$. Indeed, note that $[\mathbb{Q}(x) : \mathbb{Q}] = 2$. Thus the minimal polynomial of x is

$$p(X) = (X - (\alpha + \beta\sqrt{3}))(X - (\alpha - \beta\sqrt{3})) = X^2 + 2\alpha X + (\alpha^2 + 3\beta^2).$$

Thus $2\alpha \in \mathbb{Z}$ and $\alpha^2 + 3\beta^2 \in \mathbb{Z}$. Since $2\alpha \in \mathbb{Z}$, then $\alpha = m/2$ for some $m \in \mathbb{Z}$

- If m is even, then $\alpha \in \mathbb{Z}$ and so $3\beta^2 \in \mathbb{Z}$. Since

  $$\beta^2 = t/3$$

  for some $t \in \mathbb{Z}$ and 3 is not a perfect square, we conclude necessarily that $t/3$ must be integer. Moreover, since $\beta \in \mathbb{Q}$ a priori, certainly $\beta \in \mathbb{Z}$.

- If m is odd, then $m = 2k + 1$ for some $k \in \mathbb{Z}$, which implies that

  $$\alpha^2 + 3\beta^2 = \frac{4k^2 + 4k + 1}{4} + 3\beta^2 = \frac{1}{4} + k^2 + k + 3\beta^2 \in \mathbb{Z}.$$

  Thus $\frac{1}{4} + 3\beta^2 \in \mathbb{Z}$, which implies that there is $m \in \mathbb{Z}$ such that

  $$\beta^2 = \frac{4m - 1}{12},$$

  that is, $12\beta^2 = 4m - 1 \in \mathbb{Z}$. Since 12 is not a perfect square and $12\beta^2 \in \mathbb{Z}$, we have that $\beta^2 \in \mathbb{Z}$ and, again, since $\beta \in \mathbb{Q}$, we conclude $\beta \in \mathbb{Z}$. Finally, since $\mathbb{Z}\sqrt{3} \subseteq S$, we have $\alpha \in S$. However $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$ and this is contradiction, because $S \cap \mathbb{Q} = \mathbb{Z}$

Thus just the first case is possible, then $\alpha + \beta\sqrt{3} \in \mathbb{Z} + \mathbb{Z}\sqrt{3}$ and we conclude that $S = \mathbb{Z} + \mathbb{Z}\sqrt{3}$. □

Question 2: Prove that the ring $\mathbb{Z}[\sqrt{5}]$ is not integrally closed.

Proof: In fact, note that $\mathrm{Quot}(\mathbb{Z}[\sqrt{5}]) = \mathbb{Q}(\sqrt{5})$, because $\mathbb{Q}(\sqrt{5})$ is the smallest field containing $\mathbb{Z}[\sqrt{5}]$. Consider the golden ratio number

$$\varphi = \frac{1}{2}(1 + \sqrt{5}) \in \mathbb{Q}(\sqrt{5}).$$

Note that $\varphi \notin \mathbb{Z}[\sqrt{5}]$, because if there is $m, n \in \mathbb{Z}$ such that

$$m + n\sqrt{5} = \frac{1}{2} + \frac{\sqrt{5}}{2},$$

then, since $\sqrt{5}$ is irrational number, we deduce $m = 1/2$, which is a contradiction.

On the other hand, φ is one of the zeros of the following polynomial

$$p(X) = X^2 - X - 1 \in (\mathbb{Z}[\sqrt{5}])[X].$$

Thus φ is integral over $\mathbb{Z}[\sqrt{5}]$ and so $\mathbb{Z}[\sqrt{5}]$ is not integrally closed. □

Question 3: Let K be be a field and $\{R_i\}_{i\in L}$ be a family of subrings of K. If R_i is integrally closed in K for each $i \in L$, then $\bigcap_{i\in L} R_i$ is also integrally closed.

Proof: Fistly, note that, since $\bigcap_{i\in L} R_i \subseteq R_i$, we have

$$\mathrm{Quot}\left(\bigcap_{i\in L} R_i\right) \subseteq \mathrm{Quot}(R_i) \subseteq K.$$

Thus, denoting $S := \bigcap_{i\in L} R_i$, if $x \in \overline{S}$, then $x \in K$ and there are $a_1, \dots, a_n \in S$ such that

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

Thus $f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n \in S[X]$ is the equation of integral dependence of x. Since $S[X] \subseteq R_i[X]$ for every $i \in L$, then, in particular, $f(X)$ is the equation of integral dependence of x in R_i for each $i \in L$. Since each R_i is integrally closed in K and $x \in K$, we conclude $x \in \overline{R_i} = R_i$ for every $i \in L$. Thus

$$x \in S = \bigcap_{i\in L} R_i.$$

Thus $\overline{S} \subseteq S$ and so $\bigcap_{i\in L} R_i$ is integrally closed. □

Question 4: Let d be a square-free integer. Show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ is

$$\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}[\sqrt{d}] \qquad\qquad \text{if } d \equiv 2, 3 \bmod 4,$$

and

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} \qquad\qquad \text{if } d \equiv 1 \bmod 4.$$

Proof:

Case: $d \equiv 2, 3 \mod 4$:

Observe that $\sqrt{d}$ is integral over $\mathbb{Z}$, since $\sqrt{d}$ is root of the monic polynomial

$$f(X) = x^2 - d \in \mathbb{Z}[X].$$

Since $\overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}$ is a subring of $\mathbb{Q}(\sqrt{d})$ containing $\mathbb{Z}$, we conclude that

$$\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}.$$

Now it remains to prove that $\mathbb{Z} + \mathbb{Z}\sqrt{d} = \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}$.

In fact, Let $z = \alpha + \beta\sqrt{d} \in \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}$, where $\alpha, \beta \in \mathbb{Q}$. Since $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$, because d is square-free, the minimal polynomial $f(X) \in \mathbb{Q}[X]$ of z over $\mathbb{Q}$ has degree 2. Moreover, since $\mathbb{Z}$ is integrally closed, $f(X) \in \mathbb{Z}[X]$. Since $\alpha - \beta\sqrt{d}$ is the another root of $f(X)$, then

$$f(X) = (X - (\alpha + \beta\sqrt{d}))(X - (\alpha - \beta\sqrt{d})) = X^2 - 2\alpha X + (\alpha^2 - \beta^2 d) \in \mathbb{Z}[X].$$

So $2\alpha \in \mathbb{Z}$ and $\alpha^2 - \beta^2 d \in \mathbb{Z}$. Since $2\alpha \in \mathbb{Z}$, then $\alpha = m/2$ for some $m \in \mathbb{Z}$

- If m is even, $\alpha \in \mathbb{Z}$, thus $d\beta^2 \in \mathbb{Z}$. Since d is square-free, the fact that $d\beta^2 \in \mathbb{Z}$ implies that $\beta \in \mathbb{Z}$, so $z \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

- If m is odd, then $m = 2k + 1$ for some $k \in \mathbb{Z}$. Since

$$\left(\frac{2k+1}{4}\right) + \beta^2 d = k^2 + k + \frac{1}{4} + \beta^2 d \in \mathbb{Z},$$

  we conclude that

$$\frac{1}{4} + \beta^2 d \in \mathbb{Z}$$

  Thus $4\beta^2 d = 4k - 1$ for some $k \in \mathbb{Z}$. Since d is square-free, then $\beta = n/2$ for some $n \in \mathbb{Z}$.

  - If n is even, $\beta \in \mathbb{Z}$, thus we have $4d\beta^2 = 4k - 1$. However, $4d\beta^2 \equiv 0 \mod 4$, while $4k - 1 \equiv 3 \mod 4$, implying in a contradiction.

  - If n is odd, since k also odd and $\alpha^2 - \beta^2 d \in \mathbb{Z}$, we have
$$\frac{4k^2+4k+1}{4} - d\frac{4n^2+4n+1}{4} = k^2 + k - dn^2 - dn + \frac{1-d}{4} \in \mathbb{Z}$$
which implies that $d \equiv 1 \mod 4$, implying in a contradiction.

In both cases, from the assumption in m odd, we derive a contradiction. Then m is even, so $\beta \in \mathbb{Z}$ and $z \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Then

$$\overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} + \mathbb{Z}\sqrt{d}.$$

Case $d \equiv 1 \mod 4$:

From the hypothesis $d \equiv 1 \mod 4$, we conclude that $z = \frac{1}{2}(1+\sqrt{d})$ is root of the following monic polynomial

$$x^2 - x + \left(\frac{1-d}{4}\right) \in \mathbb{Z}[X].$$

Since $\overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}$ is a subring of $\mathbb{Q}(\sqrt{d})$ containing $\mathbb{Z}$, we conclude that

$$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) \subseteq \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}.$$

Now it remains to prove that $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) = \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}$.

In fact, Let $z = \alpha + \beta\frac{1}{2}(1+\sqrt{d}) \in \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})}$, where $\alpha, \beta \in \mathbb{Q}$. Since $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$, because d is square-free, the minimal polynomial $f(X) \in \mathbb{Q}[X]$ of z over $\mathbb{Q}$ has degree 2. Moreover, since $\mathbb{Z}$ is integrally closed, we have $f(X) \in \mathbb{Z}[X]$. Moreover, since $\alpha + \beta\frac{1}{2}(1-\sqrt{d})$ is the another root of $f(X)$, then

$$f(X) = \left(X - \left(\alpha + \beta\frac{1}{2}(1+\sqrt{d})\right)\right)\left(X - \left(\alpha + \beta\frac{1}{2}(1-\sqrt{d})\right)\right) = X^2 - (2\alpha+\beta)X + \alpha\beta + \alpha^2 + \frac{\beta^2}{4} + \beta^2 d \in \mathbb{Z}[X].$$

So

$$2\alpha + \beta \in \mathbb{Z} \qquad \text{and} \qquad \frac{4\alpha\beta + 4\alpha^2 + \beta^2}{4} + \beta^2 d \in \mathbb{Z}$$

Since $2\alpha + \beta \in \mathbb{Z}$, then $4\alpha^2 + 4\alpha\beta + \beta^2 \in \mathbb{Z}$

- If $2\alpha + \beta$ is odd, then $4\alpha\beta + 4\alpha^2 + \beta^2$ is also odd. Then, since
$$\frac{4\alpha\beta + 4\alpha^2 + \beta^2}{4} + \beta^2 d \in \mathbb{Z},$$
we conclude that there are $k \in \mathbb{Z}$ such that $4\beta^2 d = 4k - 1$. However, since d is square-free and $4\beta^2 d \in \mathbb{Z}$, we have that $\beta = n/2$ for some $n \in \mathbb{Z}$.

- If n is even, then $\beta \in \mathbb{Z}$. But we have a contradiction, because $4\beta^2 d$ is even, while $4k-1$ is odd.
- If n is odd, then $n = (2t+1)/2$ for some $t \in \mathbb{Z}$. Thus

$$4t^2 d + 4td + d = 4k - 1,$$

which is a contradiction, because $d \equiv 1 \mod 4$

- If $2\alpha + \beta$ is even, then

$$\frac{4\alpha\beta + 4\alpha^2 + \beta^2}{4} \in \mathbb{Z},$$

and so $\beta^2 d \in \mathbb{Z}$. Since d is square-free, we conclude that $\beta \in \mathbb{Z}$. Now, since $2\alpha + \beta$ is even, we have two possibilities.

- If β is even, so $\alpha \in \mathbb{Z}$ and we conclude that

$$z \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right).$$

- If β is odd, so $\alpha = t/2$ for some $t \in \mathbb{Z}$ odd. However

$$\frac{4\alpha\beta + 4\alpha^2 + \beta^2}{4} = \frac{2\beta + t^2 + t^2/4}{4} \text{ can not be integer}$$

since $2\beta^2 + t^2 \in \mathbb{Z}$ and $t^2/4$ is not integer.

Thus we conclude that

$$z \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right).$$

Then

$$\overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{d})} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right).$$

1.3 Discrete Valuations Rings and Dedekind Rings

Question 1: If I is an ideal of R, we write $x \equiv y \mod I$ to mean $x - y \in I$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct, nonzero prime ideals of a Dedekind ring R; $a_1, \ldots, a_n \in \mathbb{Z}_{\geq 1}$ and $y_1, \ldots, y_n$ any elements of R. Show that there exists an $x \in R$ such that

$$\begin{aligned} x &\equiv y_1 \mod \mathfrak{p}_1^{a_1} \\ x &\equiv y_2 \mod \mathfrak{p}_2^{a_2} \\ &\vdots \\ x &\equiv y_n \mod \mathfrak{p}_n^{a_n} \end{aligned}$$

Proof: In fact, since R is a Dedekind domain, we have $\dim(R) = 1$, so each nonzero prime ideal is maximal. Since $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct, nonzero prime ideals of R, they are two-by-two coprime. By Lemma 3.8, we also have that $\mathfrak{p}_1^{a_1}, \ldots, \mathfrak{p}_n^{a_n}$ are coprime. Thus, by the Chinese Reimainder Theorem, the natural ring homomorphism

$$\begin{aligned}\phi : R &\longrightarrow \tfrac{R}{\mathfrak{p}_1^{a_1}} \times \cdots \times \tfrac{R}{\mathfrak{p}_n^{a_n}}\\ x &\longmapsto (\overline{x}, \ldots, \overline{x})\end{aligned}$$

is surjective. Thus, given $y_1, \ldots, y_n \in R$, there is $x_0 \in R$ such that

$$\phi(x_0) = (\overline{x_0}, \ldots, \overline{x_0}) = (\overline{y_1} \ldots, \overline{y_n}).$$

Then

$$\begin{aligned}x_0 &\equiv y_1 \mod \mathfrak{p}_1^{a_1}\\ x_0 &\equiv y_2 \mod \mathfrak{p}_2^{a_2}\\ &\vdots\\ x_0 &\equiv y_n \mod \mathfrak{p}_n^{a_n}.\end{aligned}$$

□

Question 2: Let R be an integral domain with quotient field K and let M be an R-submodule of a finite dimensional K-vector space, prove that

$$M = \bigcap_{\mathfrak{p} \in \mathrm{MaxSpec}(R)} M_{\mathfrak{p}}.$$

Proof: Firstly observe that, since M is an R-submodule of a K-vector space, given $m \in M$ and $s \in R$, if $sm = 0$, then $s = 0$ or $m = 0$. Thus, given $\mathfrak{p} \in \mathrm{MaxSpec}(R)$, the natural mapping

$$\begin{aligned}\phi_{\mathfrak{p}} : M &\longrightarrow M_{\mathfrak{p}}\\ m &\longmapsto \tfrac{m}{1}\end{aligned}$$

is injective, because, if $\phi_{\mathfrak{p}}(m) = m/1 = 0$, there is $s \in R \setminus \mathfrak{p}$ such that $sm = 0$, which implies that $m = 0$, because $s \neq 0$. Then we can see M as subspace of $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{MaxSpec}(R)$, whence we have

$$M \subseteq \bigcap_{\mathfrak{p} \in \mathrm{MaxSpec}(R)} M_{\mathfrak{p}}.$$

Now let $x \in \bigcap_{\mathfrak{p} \in \operatorname{MaxSpec}(R)} M_{\mathfrak{p}}$. Consider the ideal

$$I = \{z \in R \ ; \ zx \in M\}.$$

Given $\mathfrak{p} \in \operatorname{MaxSpec}(R)$, we have that $x = m/s$, where $m \in M$ and $s \in R \setminus \mathfrak{p}$. Note that $sx = m/1 \in M$, thus $s \in I$ and then $I \nsubseteq \mathfrak{p}$. Since this last conclusion is true for any $\mathfrak{p} \in \operatorname{MaxSpec}(R)$, we conclude that $I = R$, hence $1 \in I$ and then $x = 1.x \in M$. So

$$\bigcap_{\mathfrak{p} \in \operatorname{MaxSpec}(R)} M_{\mathfrak{p}} \subseteq M$$

and then

$$M = \bigcap_{\mathfrak{p} \in \operatorname{MaxSpec}(R)} M_{\mathfrak{p}}.$$

□

1.4 Fractional Ideals and the Class Group

Question 1: Show that the multiplication and inversion behave properly with respect the localization. That is, if S is a multiplicatively subset of R and $\mathcal{M}$ is a fractional ideal of R, then $\mathcal{M}_S = \mathcal{M}R_S$ is a fractional ideal of R_S and we have $(\mathcal{M}^{-1})_S = (\mathcal{M}_S)^{-1}$. Moreover, if $\mathcal{M}$ and $\mathcal{N}$ are fractional ideals of R, then $(\mathcal{M}\mathcal{N})_S = \mathcal{M}_S\mathcal{N}_S$.

Proof: Let S be a multiplicatively closed subset of R.

Claim 1: $\mathcal{M}_S = \mathcal{M}R_S$ is a fractional ideal of R_S.

In fact, by definition, an element of $\mathcal{M}_S$ is of form m/s, where $m \in \mathcal{M}$ and $s \in S$, thus $m/s = m * 1/s \in \mathcal{M}R_S$. On the other hand, if $x \in \mathcal{M}R_S$, then there are $m_1, \ldots, m_n \in \mathcal{M}$ and $s_1, \ldots, s_n \in S$ such that

$$x = \frac{m_1}{s_1} + \cdots + \frac{m_n}{s_n}.$$

Setting $s = s_1 \cdots s_n$ and $\hat{s}_i = s_1 \cdots s_{i-1} \cdot s_{i+1} \cdots s_n$ for each $i = 1, \ldots, n$, we have that

$$x = \frac{\hat{s}_1 m_1 + \cdots + \hat{s}_n m_n}{s} \in \mathcal{M}_S.$$

Then we conclude that $\mathcal{M}_S = \mathcal{M}R_S$. Moreover, note that since $K = \operatorname{Quot}(R)$ is the smallest field containing R and $R \subseteq R_S \subseteq K$, then $K = \operatorname{Quot}(R_S)$. Thus $\mathcal{M}_S$ is R_S-submodule of K. Finally, since $\mathcal{M}$ is an R-module which is finitely generated, then, if $\{m_1, \ldots, m_n\}$ is a set of generators of $\mathcal{M}$, we conclude that

$$\left\{\frac{m_1}{1} \ldots, \frac{m_n}{1}\right\} \subseteq \mathcal{M}_S$$

is a set of generators of $\mathcal{M}_S$ as R_S-module, thus $\mathcal{M}_S$ is a fractional ideal of R.

Claim 2: $(\mathcal{M}_S)^{-1} = (\mathcal{M}^{-1})_S$.

In fact, let $m/s \in (\mathcal{M}_S)^{-1}$ and $\{x_1, \ldots, x_n\}$ a set of generators of $\mathcal{M}$ as R-module. Since $m/s \in (\mathcal{M}_S)^{-1}$, we have for all $1 \leq i \leq n$

$$\frac{x_i}{1}.\frac{m}{s} \in R_S$$

Thus, for each $i \in \{1, \ldots, n\}$, there are $r_i \in R$, $t_i \in S$ such that

$$x_i.\frac{m}{s} = \frac{r_i}{t_i}.$$

Setting $t := t_1 \ldots t_n$, note that, given $x = \sum_{i=1}^n a_i x_i$ be an element arbitrary of $\mathcal{M}$, we have

$$tm\left(\sum_{i=1}^n a_i x_i\right) = \sum_{i=1}^n a_i(mtx_i) \in R.$$

Then $tm \in \mathcal{M}^{-1}$. Then

$$\frac{m}{s} = \frac{tm}{ts} \in (\mathcal{M}^{-1})_S.$$

On the other hand, let $m/s \in (\mathcal{M}^{-1})_S$, where $m \in \mathcal{M}^{-1}$ and $s \in S$. Given $n/t \in \mathcal{M}_S$, we have

$$\frac{n}{t}.\frac{m}{s} = \frac{nm}{st} = \frac{1}{st}.\frac{nm}{1} \in R_S,$$

because $nm \in R$. Thus we conclude that $m/s \in (\mathcal{M}_S)^{-1}$.

Claim 3: $(\mathcal{M}\mathcal{N})_S = \mathcal{M}_S\mathcal{N}_S$

In fact, given $m/s \in (\mathcal{M}\mathcal{N})_S$, then $m \in \mathcal{M}\mathcal{N}$ and $s \in S$. Since $m \in \mathcal{M}\mathcal{N}$, there are $m_1, \ldots, m_t \in \mathcal{M}$ and $n_1, \ldots, n_t \in \mathcal{N}$ such that

$$\frac{m}{s} = \frac{\sum_{i=1}^t m_i n_i}{s} = \sum_{i=1}^t \left(\frac{m_i n_i}{s}\right) = \sum_{i=1}^t \left(\frac{m_i}{s}\frac{n_i}{1}\right) \in \mathcal{M}_S\mathcal{N}_\mathrm{S}.$$

On the other hand, given $m/s \in \mathcal{M}_S\mathcal{N}_S$, then there are $m_1, \ldots, m_l \in \mathcal{M}$, $n_1, \ldots, n_l \in \mathcal{M}$, $s_1, \ldots, s_l, t_1, \ldots, t_l \in S$ such that

$$\frac{m}{s} = \sum_{i=1}^l \left(\frac{m_i}{s_i} \cdot \frac{n_i}{t_i}\right) = \sum_{i=1}^l \left(\frac{m_i n_i}{s_i t_i}\right).$$

Setting $s = s_1 \cdots s_l \cdot t_1 \cdots t_l$ and $a_i = s_1 t_1 \cdots s_{i-1} t_{i-1} \cdot s_{i+1} t_{i+1} \cdots s_n t_n$, we have

$$\frac{m}{s} = \sum_{i=1}^{l} \left(\frac{m_i n_i}{s_i t_i} \right) = \frac{\sum_{i=1}^{l} a_i m_i n_i}{s} \in (\mathcal{M}\mathcal{N})_S.$$

Thus $(\mathcal{M}\mathcal{N})_S = \mathcal{M}_S \mathcal{N}_S$. □

Question 2: Let R be a Dedekind domain. Show that $C(R)$ has order 1 if and only if R is a PID.

Proof: Suppose that $C(R)$ has order 1. Since $C(R) = I(R)/P(R)$, where $I(R)$ is the group of fractional ideals of R and $P(R)$ is its subgroup of all principal fractional ideals, we conclude that $I(R) = P(R)$, so every fractional ideal of R is principal. In particular, every ideal of R is principal, then R is a PID. On the other hand, suppose that R is a PID. In order to show that $C(R)$ has order 1, it is enough to show that every fractional ideal of R is principal. Let $\mathcal{M}$ be a fractional ideal of R, then M is a nonzero finitely generated R-submodule of $K = \operatorname{Quot}(R)$. Let $\{r_1/s_1, \ldots, r_n/s_n\}$ be a set of generators of $\mathcal{M}$ as R-module. It is easy to see that, setting $s = s_1 \cdots s_n$, we have $s\mathcal{M} \subseteq R$. I claim that $I = s\mathcal{M}$ is an ideal of R. In fact, we have that $0 = s \cdot 0 \in s\mathcal{M} \subseteq R$. Moreover, given $z_1 = sm_1$, $z_2 = sm_2 \in s\mathcal{M}$, then

$$z_1 + z_2 = sm_1 + sm_2 = s(m_1 + m_2) \in s\mathcal{M} \subseteq R$$

and

$$-z_1 = -sm_1 = s(-m_1) \in s\mathcal{M} \subseteq R.$$

Now, given $r \in R$, we have

$$rz_1 = r(sm_1) = s(rm_1) \in s\mathcal{M} \subseteq R.$$

Thus $s\mathcal{M}$ is an ideal of R. Since R is a PID and $s\mathcal{M}$ is nonzero, there is $r \neq 0$ such that $s\mathcal{M} = Rr$. Thus, setting $y = r/s \neq 0$, we conclude that

$$\mathcal{M} = R\left(\frac{r}{s}\right) = Ry.$$

Thus $\mathcal{M}$ is a principal fractionary ideal of R. □

Question 5: Let $R = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$. Show that R is not a UFD (and so not a PID).

Proof: In fact, note that

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

I will show that 3 and 7 [1] is are prime elements in $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ and that 3 is not a prime factor of $1-2\sqrt{-5}$ and $(1+2\sqrt{-5})$.

- 3: Suppose that

  $$3 = (a+b\sqrt{-5}))(c+d\sqrt{-5}) = ac-5bd+\sqrt{-5}(ad+bc)$$

  Then

  $$\begin{cases} ad+bc=0 \\ ac-5bd=3 \end{cases}$$

  I claim that $b=0$. In fact, suppose that $b\neq 0$, then $c=(-ad)/b$ and thus $3b=d(-a^2-5b^2)$. Note that $-a^2-5b^2\leq 0$. If $-a^2-5b^2=0$, then $a=b=0$ and we would get a contradiction with the second equation. Then $-a^2-5b^2<0$. Looking the equation $3b=d(-a^2-5b^2)$, we realize that, since $b\neq 0$, then $d\neq 0$, and so we have two possibilities

  - $b>0$ and $d<0$;
  - $b<0$ and $d>0$.

  Since, in both cases $ac=3+5bd<0$, we have two possibilities

  - $a>0$ and $c<0$;
  - $a<0$ and $c>0$.

  If we check the four possible combinations, we conclude that $ad+bc\neq 0$, getting a contradiction. Then $b=0$. This implies that $ad=0$ and $ac=3$, which implies that $d=0$ Then

  $$3 = (a+b\sqrt{-5}))(c+d\sqrt{-5}) = ac.$$

  Now, since 3 is irreducible in $(\mathbb{Z},+,*)$, we can suppose c is 1 and we conclude that $a+b\sqrt{-5}=3$. So 3 is a prime element in $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$.

- 7: Suppose that

  $$7 = (a+b\sqrt{-5}))(c+d\sqrt{-5}) = ac-5db+\sqrt{-5}(ad+bc)$$

[1] Actually, we do not need to prove that 7 is a prime element of $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$. Since I had a lot of work to prove it, I felt sorry for erasing it.

Then

$$\begin{cases} ad + bc = 0 \\ ac - 5bd = 7 \end{cases}$$

I claim that $b = 0$. In fact, suppose that $b \neq 0$, then $c = (-ad)/b$ and thus $7b = d(-a^2 - 5b^2)$. Note that $-a^2 - 5b^2 \leq 0$. If $-a^2 - 5b^2 = 0$, then $a = b = 0$ and we would get a contradiction with the second equation. Then $-a^2 - 5b^2 < 0$. Looking the equation $7b = d(-a^2 - 5b^2)$, we realize that, since $b \neq 0$, then $d \neq 0$, and so we have two possibilities

- $b > 0$ and $d < 0$
- $b < 0$ and $d > 0$

In both cases, we have $ac = 7 + 5bd = 2$ or $ac = 7 + 5bd < 0$. If $ac = 2$, then we have four possibilities

- $a = 2$ and $c = 1$
- $a = -2$ and $c = -1$
- $a = 1$ and $c = 2$
- $a = -1$ and $c = -2$

For each case above, we would get that $b = -2d$ or $d = -2b$ by switching at the first equation of system. If $b = -2d$, then, using that $7b = d(-a^2 - 5b^2)$, we would have that $14 = a^2 + 5b^2$. The unique solution possible is when $b = \pm 1$, however, if $b = \pm 1$, then $d \notin \mathbb{Z}$, a contradiction. On other hand, if $d = -2b$, then

$$\frac{7}{2} = a^2 + 5b^2,$$

which is impossible, then it is not possible that $ac = 2$, whence $ac = 7 + 5bd < 0$. Now, repeating the same argument used in case for $n = 3$, we also conclude that 7 is also a prime element in $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

Now I claim that $1 + 2\sqrt{-5}$ and $1 - 2\sqrt{-5}$ do not have 3 as factor. Indeed

- $1 + 2\sqrt{-5}$: Suppose that

$$1 + 2\sqrt{-5} = 3(a + b\sqrt{-5}) = 3a + 3b\sqrt{-5}.$$

This would imply that $a = 1/3$ and $b = 2/3$, which is a contradiction, because, by hypothesis, $a, b \in \mathbb{Z}$.

- $1-2\sqrt{-5}$: Suppose that

  $$1-2\sqrt{-5}=3(a+b\sqrt{-5})=3a+3b\sqrt{-5}.$$

  This would imply that $a=1/3$ and $b=-2/3$, which is a contradiction, because, by hypothesis, $a,b\in\mathbb{Z}$.

Since 3 is a prime element in $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ and 3 doesn't divide $1+2\sqrt{-5}$ and $1-2\sqrt{-5}$, we conclude that these numbers do not have 3 in their possible factorizations, which implies that $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ is not a unique factorization domain.

Let's calculate the norm function $N:\mathbb{Q}\longrightarrow\mathbb{Q}$ of the extension $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. In order to do this, consider $B=\{1,\sqrt{-5}\}$ a basis of $\mathbb{Q}(\sqrt{-5})$ over $\mathbb{Q}$. Thus, given $a+b\sqrt{-5}\in\mathbb{Q}(\sqrt{-5})$, we have

$$\begin{gathered}1\cdot(a+b\sqrt{-5})=a\cdot 1+b\cdot\sqrt{-5},\\ \sqrt{-5}\cdot(a+b\sqrt{-5})=(-5b)\cdot 1+a\cdot\sqrt{-5}.\end{gathered}$$

Thus the matrix of the multiplication $m_{a+b\sqrt{-5}}:\mathbb{Q}(\sqrt{-5})\longrightarrow\mathbb{Q}(\sqrt{-5})$ by $a+b\sqrt{-5}$ on the basis B is

$$\left[m_{a+b\sqrt{-5}}\right]_B^B=\begin{bmatrix}a & -5b\\ b & a\end{bmatrix}.$$

Then

$$N(a+b\sqrt{-5})=\det\begin{bmatrix}a & -5b\\ b & a\end{bmatrix}=a^2+5b^2.$$

Consider the ideal $I=(3,1+\sqrt{-5})$ of $\mathbb{Z}[\sqrt{-5}]$. I claim that I is not a principal ideal. Indeed, suppose by contradiction that I is principal, thus there is $z\in\mathbb{Z}[\sqrt{-5}]$ such that

$$(z)=(3,1+\sqrt{-5}).$$

Thus there are $\alpha_1,\alpha_2\in\mathbb{Z}[\sqrt{-5}]$ such that

$$\begin{cases}3=z\alpha_1\\ 1+\sqrt{-5}=z\alpha_2\end{cases}$$

Using the norm function and its multiplicative property, we have that

$$\begin{gathered}9=N(3)=N(z\alpha_1)=N(z)N(\alpha_1),\\ 6=N(1+\sqrt{-5})=N(z\alpha_2)=N(z)N(\alpha_2).\end{gathered}$$

Since $N|_{\mathbb{Z}[\sqrt{-5}]}$ has image contained in $\mathbb{Z}$, we conclude that $N(z)$ divides 9 and $N(z)$ divides 6. Thus, by elementary number theory, we conclude that $N(z)$ divides the $\gcd(9,6) = 3$. However, there is not $z' \in \mathbb{Z}[\sqrt{-5}]$ such that $N(z') = 3$. Thus $N(z) = 1$, which implies that $z = \pm 1$, that is, z is unit in $\mathbb{Z}[\sqrt{-5}]$, implying that $I = \mathbb{Z}[\sqrt{-5}]$. However I will prove now that this fact is impossible. Suppose that there are $a + b\sqrt{-5}$, $x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ such that

$$3(a + b\sqrt{-5}) + (1 + 1\sqrt{-5})(x + y\sqrt{-5}) = 1.$$

Thus we get the following system of equations

$$\begin{cases} 3a + x - 5y = 1 \\ 3b + x + y = 0 \end{cases}$$

Multiplying the second equation by 2 and summing it with the first equation, we obtain

$$3(a + 2b + x - y) = 1,$$

which is impossible, since $a + 2b + x - y \in \mathbb{Z}$. Thus we conclude that $I \neq \mathbb{Z}[\sqrt{-5}]$ and we get a contradiction, so I is not a principal ideal of $\mathbb{Z}[\sqrt{-5}]$. □

1.5 Norms and Traces

This section does not contain exercises.

1.6 Extension of Dedekind Rings

Question 1: Let $R \subseteq R' \subseteq R''$ be Dedekind domains and let $\mathfrak{P}$ be a nonzero prime ideal of R''. Prove the multiplicative property of ramification numbers

$$e(\mathfrak{P}/R) = e(\mathfrak{P}/R')e(\mathfrak{P} \cap R'/R).$$

Proof: Firstly, note that $\mathfrak{P} \cap R'$ is a non-zero prime ideal of R', thus, by definition of the ramification index, we have

$$((\mathfrak{P} \cap R') \cap R)R' = I.(\mathfrak{P} \cap R')^{e(\mathfrak{P} \cap R'/R)},$$

where I is a product of prime ideals of R', all ideals distinct of $\mathfrak{P} \cap R'$. On the other hand, we also have

$$(\mathfrak{P} \cap R')R'' = J\mathfrak{P}^{e(\mathfrak{P}/R')},$$

where J é finite product of prime ideals of R'', all ideals distinct of $\mathfrak{P}$. Note that

$$(\mathfrak{P} \cap R)R' = ((\mathfrak{P} \cap R') \cap R)R',$$

Thus, if $(\mathfrak{P} \cap R)R'' = K.\mathfrak{P}^{e(\mathfrak{P}/R)}$, where K is a ideal of R'' which is a product of prime ideals of R'', all primes distinct of $\mathfrak{P}$, we obtain

$$\begin{aligned} K.\mathfrak{P}^{e(\mathfrak{P}/R)} = (\mathfrak{P} \cap R)R'' = ((\mathfrak{P} \cap R)R')R'' = (I.(\mathfrak{P} \cap R')^{e(\mathfrak{P} \cap R'/R)})R'' = IR''.\big((\mathfrak{P} \cap R')^{e(\mathfrak{P} \cap R'/R)}R''\big)\big) \\ = IR''.((\mathfrak{P} \cap R')R'')^{e(\mathfrak{P} \cap R'/R)} = IR''.(JR'')^{e(\mathfrak{P} \cap R'/R)}(\mathfrak{P}^{e(\mathfrak{P}/R')})^{e(\mathfrak{P} \cap R'/R)} \\ = IR''.(JR'')^{e(\mathfrak{P} \cap R'/R)}.\mathfrak{P}^{e(\mathfrak{P}/R')e(\mathfrak{P} \cap R'/R)}, \end{aligned}$$

Since R'' is Dedekind Domain, using the uniqueness of factorization in prime ideals, it is enough to prove that IR'' and JR'' have no $\mathfrak{P}$ in their factorization. However, $JR'' = J$ is finite product of prime ideals of R'', all ideals distinct of $\mathfrak{P}$. Moreover

$$I = \mathfrak{q}_1^{n_1} \cdot \cdots \cdot \mathfrak{q}_t^{n_t},$$

where $\mathfrak{q}_i$ are prime ideals of R', all ideals distinct of $\mathfrak{P} \cap R'$. So

$$IR'' = (\mathfrak{q}_1^{n_1} R'') \cdot \cdots \cdot (\mathfrak{q}_t^{n_t} R'').$$

If $\mathfrak{P}$ appeared in the factorization of some $\mathfrak{q}_i^{n_i} R''$, then $\mathfrak{P} \cap R$ would appear in the factorization of I, which is a contradiction. Thus, by uniqueness of exponents, we conclude

$$e(\mathfrak{B}/R) = e(\mathfrak{B}/R')e(\mathfrak{B} \cap R'/R).$$

□

Question 2: Let $R \subseteq R' \subseteq R''$ be Dedekind Domains and $\mathfrak{P}$ be a nonzero prime ideal of R''. Prove the property multiplicative of relative degree

$$f(\mathfrak{P}/R) = f(\mathfrak{P}/R')f(\mathfrak{P} \cap R'/R).$$

Proof: Let $\{v_\lambda\}_{\lambda \in L}$ be a basis of $R''/\mathfrak{P}$ as $R'/(\mathfrak{P} \cap R')$-vector space, where $f(\mathfrak{P}/R') = \text{Card}(L)$ and let $\{u_\lambda\}_{\lambda \in L'}$ be a basis of $R'/(\mathfrak{P} \cap R')$ as $R/((\mathfrak{P} \cap R') \cap R) = R/((\mathfrak{P} \cap R)$-vector space, where $f(\mathfrak{P} \cap R'/R) = \text{Card}(L')$. I claim that $\{v_\lambda u_\gamma\}_{(\lambda,\gamma) \in L \times L'}$ is a basis of $R''/\mathfrak{P}$ as $R/(\mathfrak{P} \cap R)$-vector space. Indeed, given $x \in R''/\mathfrak{P}$, there are $\alpha_1, \ldots, \alpha_n \in R'/(\mathfrak{P} \cap R')$ and $v_{\lambda_1}, \ldots, v_{\lambda_n} \in \{v_\lambda\}_{\lambda \in L}$ such that

$$x = \sum_{k=1}^{n} \alpha_k v_{\lambda_k}.$$

Now, since $\alpha_i \in R'/(\mathfrak{P} \cap R')$, for each $i = 1, \ldots, n$ there are $\beta_1^i, \ldots, \beta_{m_i}^i \in R/(\mathfrak{P} \cap R)$ and $u_{\lambda_1^i}, \ldots, u_{\lambda_{m_i}^i} \in \{u_\lambda\}_{\lambda \in L'}$ such that

$$\alpha_i = \sum_{j=1}^{m_i} \beta_j^i u_{\lambda_j^i}.$$

Then we have that

$$x = \sum_{k=1}^{n} \alpha_k v_{\lambda_k} = \sum_{k=1}^{n} \left(\sum_{j=1}^{m_k} \beta_j^k u_{\lambda_j^k} \right) v_{\lambda_k} = \sum_{k=1}^{n} \sum_{j=1}^{m_k} \beta_j^k (u_{\lambda_j^k} v_{\lambda_k}).$$

Thus $\{v_\lambda u_\gamma\}_{(\lambda,\gamma) \in L \times L'}$ spans $R''/\mathfrak{P}$ as $R/(\mathfrak{P} \cap R)$-vector space. Now it is enough to prove that $\{v_\lambda u_\gamma\}_{(\lambda,\gamma) \in L \times L'}$ is a subset linearly independent of $R''/\mathfrak{P}$ as $R/(\mathfrak{P} \cap R)$-vector space. In fact, let

$$\sum_{\lambda \in L} \sum_{\gamma \in L'} \alpha_{\lambda\gamma} v_\lambda u_\gamma = 0$$

be a null linear combination, where $\operatorname{Card}(\{(\lambda, \gamma) \in L \times L' \ ; \ \alpha_{\lambda\gamma} \neq 0\}) < \infty$. Note that

$$\sum_{\lambda \in L} \sum_{\gamma \in L'} \alpha_{\lambda\gamma} v_\lambda u_\gamma = \sum_{\lambda \in L} \left(\sum_{\gamma \in L'} \alpha_{\lambda\gamma} u_\gamma \right) v_\lambda = 0$$

Since $\{v_\lambda\}_{\lambda \in L}$ is linearly independent as $R'/(\mathfrak{P} \cap R')$-vector space and $\sum_{\gamma \in L'} \alpha_{\lambda\gamma} u_\gamma \in R'/(\mathfrak{P} \cap R')$, we have that

$$\sum_{\gamma \in L'} \alpha_{\lambda\gamma} u_\gamma = 0$$

for each $\lambda \in L$. Similarly, since $\{u_\gamma\}_{\gamma \in L'}$ is linearly independent as $R/(\mathfrak{P} \cap R)$-vector space and $\alpha_{\lambda\gamma} \in R/(\mathfrak{P} \cap R)$ for all $(\lambda, \gamma) \in L \times L'$, we conclude that $\alpha_{\lambda\gamma} = 0$ for each $(\lambda, \gamma) \in L \times L'$. Then $\{v_\lambda u_\gamma\}_{(\lambda,\gamma) \in L \times L'}$ is a basis of $R''/\mathfrak{P}$ as a $R/(\mathfrak{P} \cap R)$-vector space and

$$f(\mathfrak{P}/R) = [R''/\mathfrak{P} : R/(\mathfrak{P} \cap R)] = \operatorname{Card}(L \times L') = \operatorname{Card}(L) \operatorname{Card}(L') = f(\mathfrak{P}/R') f(\mathfrak{P} \cap R'/R).$$

□

Question 3: Let $R = \mathbb{Z}$ be the ring of integers and R' be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$, where d is a square free integer, $d \neq 1, d \neq 0$. Let p be a prime ideal integer. Prove that the ideal pR' must have one of the factorizations

$$(a)\, pR' = \mathfrak{P} \qquad (b)\, pR' = \mathfrak{P}\mathfrak{Q} \qquad (c)\, pR' = \mathfrak{P}^2$$

Proof: In fact, by Theorem 6.1, the R' is a Dedekind Domain. Since $\operatorname{char}(\mathbb{Q}) = 0$, the field extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is separable. Thus, by Corollary 6.7, given a prime integer $p \in \mathbb{Z}$, we have that

$$pR' = \mathfrak{P}_1^{e_1} \cdot \cdots \cdot \mathfrak{P}_g^{e_g}$$

with

$$2 = [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i,$$

where $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ belong to Spec(R'), $e_1, \dots, e_g$ are non-negative integers and $f_i = [R'/\mathfrak{P}_i : \mathbb{Z}/(p)]$ for all $i = 1, \dots, g$. Now it is enough to analyse the possibilities

- If $e_1 = 1$, then f_1 can admit two values: $f_1 = 1$ or $f_1 = 2$:
  - If $f_1 = 2$, then pR' is exactly a prime ideal of R, that is
  $$pR' = \mathfrak{P}_1 := \mathfrak{P}.$$
  - If $f_1 = 1$, then $f_1 e_1 = 1 < 2$, thus we can assume without lost of generality that $e_2 = 1$ and $f_2 = 1$, thus
  $$pR' = \mathfrak{P}_1 \mathfrak{P}_2 := \mathfrak{P}\mathfrak{O}.$$
- If $e_1 = 2$, then we have necessarily that $f_1 = 1$ and so
$$pR' = \mathfrak{P}_1^2 := \mathfrak{P}^2.$$

□

Exercise 4 (Exercise 1 of second edition of the book): Show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$ is the ring $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2}\ ;\ a, b \in \mathbb{Z}\}$ and conclude that $\mathbb{Z}[\sqrt{2}]$ is a Dedekind Domain.

Proof: In fact, note that $\sqrt{2}$ is integral over $\mathbb{Z}$, because it is root of the following monic polynomial

$$f(X) = X^2 - 2 \in \mathbb{Z}[X]$$

Since the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$ has ring structure and it contains $\mathbb{Z}$, we conclude that $\mathbb{Z}[\sqrt{2}] \subseteq \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{2})}$. Now let $z = a + b\sqrt{2} \in \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{2})}$ and consider the polynomial

$$f(X) = (X - (a + b\sqrt{2}))(X - (a - b\sqrt{2})) = X^2 - 2aX + a^2 - 2b^2$$

Thus, since $\mathbb{Z}$ is integrally closed, we conclude by Proposition 2.5 that $2a \in \mathbb{Z}$ and $a^2 - 2b^2 \in \mathbb{Z}$. Since $2a \in \mathbb{Z}$, then $a = t/2$ for some $t \in \mathbb{Z}$.

- If t is even, then $a \in \mathbb{Z}$ and $2b^2 \in \mathbb{Z}$. Thus $b^2 = m/2$ for some m integer. However, since 2 is not a perfect square, we conclude that $b^2 \in \mathbb{Z}$. Since the square of rational non-integer number is non-integer, we conclude that $b \in \mathbb{Z}$ and so $z = a + b\sqrt{2} \in \mathbb{Z}(\sqrt{2})$ and so $\mathbb{Z}(\sqrt{2}) = \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{2})}$

- On the other hand, suppose that t is odd, then $a = k + 1/2$ for some $k \in \mathbb{Z}$. Thus $k^2 + k + 1/4 - 2b^2 \in \mathbb{Z}$. Thus there is $m \in \mathbb{Z}$, such that $2b^2 = (4m+1)/4$, that is,
$$b^2 = \frac{4m+1}{8}.$$
Since 8 is not a perfect square and 2 doesn't divide $4m+1$, we conclude that there is not $b \in \mathbb{Q}$ with this property, because we would need that the numerator were even to reduce the denominator to 4 or 1, thus it is impossible that t be odd.

Then we conclude that $\mathbb{Z}(\sqrt{2}) = \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{2})}$. Since $\mathbb{Z}$ is Dedekind domain and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is finite, we conclude by Theorem 6.1 that $\mathbb{Z}(\sqrt{2})$ is a Dedekind domain. □

Question 5: (Question 2 of the second edition of the book): Let $\mathbb{F}_p$ be a field of p elements for a prime p and let K be the field of fractions $\mathbb{F}_p(t)$ of rational fractions with coefficients in $\mathbb{F}_p$. Let R be the following ring
$$R = \left\{ \frac{a(t)}{b(t)} \in \mathbb{F}_p(t) \ ; \ a(t), b(t) \in \mathbb{F}_p[t], \ b(0) \neq 0 \right\}.$$
Show that R is a discrete valuation domain with field of fractions $\mathbb{F}_p(t)$.

Proof: Since $\mathbb{F}_p$ is a field, we have that $\mathbb{F}_p[t]$ is an Euclidean domain and so a principal ideal domain. Thus we conclude that $\mathbb{F}_p[t]$ is a Dedekind domain. I claim that
$$\mathfrak{P} = \{b(t) \in \mathbb{F}_p[t] \ ; \ b(0) = 0\}$$
is a prime ideal of $\mathbb{F}_p[t]$. Indeed, $0 \in \mathbb{F}_p[t]$, given $b_1(t), b_2(t) \in \mathfrak{P}$, we have that
$$(b_1 + b_2)(0) = b_1(0) + b_2(0) = 0$$
and
$$(-b_1)(0) = -b_1(0) = 0.$$
So $(\mathfrak{P}, +)$ is an Abelian group. Moreover, given $a(t) \in \mathbb{F}_p[t]$ and $b(t) \in \mathfrak{P}$, then
$$(a \cdot b)(0) = a(0)b(0) = 0.$$
Moreover, $\mathfrak{P}$ is clearly a proper ideal of $\mathbb{F}_p[t]$ and given $a(t), b(t) \in \mathbb{F}_p[t]$, if $a(t)b(t) \in \mathfrak{P}$, then $a(0)b(0) = 0$, which implies that $a(t) \in \mathfrak{P}$ or $b(t) \in \mathfrak{P}$. Thus $\mathfrak{P}$ is a prime ideal of $\mathbb{F}_p[t]$. Now note that
$$S = \mathbb{F}_p[t] \setminus \mathfrak{P} = \{b(t) \in \mathbb{F}_p[t] \ ; \ b(0) \neq 0\}.$$
Since $\mathbb{F}_p[t]$ is Dedekind domain and $\mathfrak{P}$ is a nonzero prime ideal of $\mathbb{F}_p[t]$, we conclude that $R = (\mathbb{F}_p[t])_S = (\mathbb{F}_p[t])_{\mathfrak{P}}$ is a discrete valuation ring with field of fractions $\mathbb{F}_p(t)$. □

1.7 Discriminant

Question 1: Let d be a square free integer and R' be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$. As continuation of Question 3 in section 6, determine which of the three possible factorizations of pR' actually occurs. Prove the following.

(a) Suppose that (p) divides $\Delta(R'/\mathbb{Z})$. Then $pR' = \mathfrak{P}^2$ for some nonzero prime ideal $\mathfrak{P}'$ of R'.

(b) Suppose that p is odd and (p) does not divide $\Delta(R'/\mathbb{Z})$. Then $pR' = \mathfrak{P}\mathfrak{Q}$ with $\mathfrak{P} \neq \mathfrak{Q}$ if and only if d is a quadratic residue module p, that is, $X^2 - d$ has a root in $\mathbb{Z}/(p)$.

(c) Suppose that $p = 2$ and (p) does not divide $\Delta(R'/\mathbb{Z})$. Then necessarily $d \equiv 1 \bmod 4$. Show that $2R' = \mathfrak{P}\mathfrak{Q}$ if $d \equiv 1 \pmod 8$ and $2R' = \mathfrak{P}$ is prime if $d \equiv 5 \pmod 8$.

Proof: (a) Consider $\Delta(R'/\mathbb{Z}) = \mathfrak{P}_1^{n_1} \dots \mathfrak{P}_g^{n_g}$, where $\mathfrak{P}_i$ is a prime ideal of R' for all $1 \leq i \leq g$ and $\mathfrak{P}_i \neq \mathfrak{P}_j$ if $i \neq j$. If pR' divides $\Delta(R'/\mathbb{Z})$, then

$$pR' = \mathfrak{P}_1^{a_1} \dots \mathfrak{P}_g^{a_g}, \quad \text{with } \; 0 \leq a_i \leq n_i \;\; \forall i \in \{1, \dots, g\}$$

This means that $\Delta(R'/\mathbb{Z}) \subseteq pR'$. By Theorem 7.3, we have that (p) is a ramified prime of $\mathbb{Z}$ in R', thus, by Question 3 in section 6, we conclude that $pR' = \mathfrak{P}^2$ for some nonzero prime ideal $\mathfrak{P}$ of R'.

(b) Since (p) does not divide $\Delta(R'/\mathbb{Z})$, we have that (p) does not contain $\Delta(R'/\mathbb{Z})$. Again by Theorem 7.3, we conclude that (p) is not a ramified prime of $\mathbb{Z}$ in R'. Thus, by Question 3 in section 6, we we conclude that $pR' = \mathfrak{P}$ or $pR' = \mathfrak{P}\mathfrak{Q}$, where $\mathfrak{P}$, $\mathfrak{Q}$ are prime ideals of R'. However, By Question 4 of Section 2, we have that

$$R' = \mathbb{Z}[\sqrt{d}] \qquad \text{or} \qquad R' = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

Since $[R' : \mathbb{Z}[\sqrt{d}]] \leq 2$ and p is an odd prime number, we have that p does not divide $[R' : \mathbb{Z}[\sqrt{d}]]$. Thus, we can apply the Theorem 7.6. If $f(X) = X^2 - d \in \mathbb{Z}[X]$ has a root in $\mathbb{Z}/(p)$, we conclude that there are $a, b \in \mathbb{Z}/(p)$ such that

$$\overline{f}(X) = (X-a)(X-b) \in \left(\frac{\mathbb{Z}}{(p)}\right)[X],$$

which implies that there exist $\mathfrak{P} \neq \mathfrak{Q} \in \operatorname{Spec}(R')$ such that

$$pR' = \mathfrak{P}\mathfrak{Q}.$$

On other hand, if $f(X) = X^2 - d \in \mathbb{Z}[X]$ does not have root in $\mathbb{Z}/(p)$, then $f(X) = X^2 - d$ is irreducible in $(\mathbb{Z}/(p))[X]$. So, by Theorem 7.6, we conclude that

$$pR' = \mathfrak{P}$$

for some $\mathfrak{P} \in \operatorname{Spec}(R')$. Then, we conclude that $pR' = \mathfrak{P}\mathfrak{Q}$ with $\mathfrak{P} \neq \mathfrak{Q}$ if and only if d is a quadratic residue module p.

(c) Firstly let's calculate the $\Delta(R'/\mathbb{Z})$. In order to do it, we have to divide in two cases: $d \equiv 1 (\operatorname{mod} 4)$ and $d \equiv 2, 3 (\operatorname{mod} 4)$.

- Suppose that $d \equiv 1 (\operatorname{mod} 4)$. We already know that

$$R' = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Thus $\beta = \{1, (1+\sqrt{d})/2\}$ is an integral basis of extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Let's now calculate the trace function of this extension. Note that

$$[m_{a+b\sqrt{d}}]_\beta^\beta = \begin{bmatrix} a-b & (bd-b)/2 \\ 2b & a+b \end{bmatrix}.$$

Thus

$$\operatorname{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a+b\sqrt{d}) = \operatorname{Tr}\begin{bmatrix} a-b & (bd-b)/2 \\ 2b & a+b \end{bmatrix} = 2a.$$

Then the discriminant $\Delta(R'/\mathbb{Z})$ is given by

$$\Delta(R'/\mathbb{Z}) = \det\begin{bmatrix} \operatorname{Tr}(1) & \operatorname{Tr}((1+\sqrt{d})/2) \\ \operatorname{Tr}((1+\sqrt{d})/2) & \operatorname{Tr}(((1+\sqrt{d}/2)^2) \end{bmatrix}\mathbb{Z} = \det\begin{bmatrix} 2 & 1 \\ 1 & (1+d)/2 \end{bmatrix}\mathbb{Z} = d\mathbb{Z}.$$

- Suppose now that $d \equiv 2, 3 (\operatorname{mod} 4)$. We have already known that

$$R' = \mathbb{Z}[\sqrt{d}].$$

Thus $\beta = \{1, \sqrt{d}\}$ is an integral basis of extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Also we have already known that the trace function of this extension is given by

$$\begin{aligned} \operatorname{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} : \mathbb{Q}(\sqrt{d}) &\longrightarrow \mathbb{Q} \\ a+b\sqrt{d} &\longmapsto 2a \end{aligned}$$

Then the discriminant $\Delta(R'/\mathbb{Z})$ is given by

$$\Delta(R'/\mathbb{Z}) = \det\begin{bmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\sqrt{d}) \\ \operatorname{Tr}(\sqrt{d}) & \operatorname{Tr}((\sqrt{d})^2) \end{bmatrix}\mathbb{Z} = \det\begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix}R = 4d\mathbb{Z}.$$

Summing up, we have the following

$$\Delta(R'/\mathbb{Z}) = \begin{cases} d\mathbb{Z} & \text{if } d \equiv 1 (\operatorname{mod} 4); \\ (4d)\mathbb{Z} & \text{if } d \equiv 2, 3 (\operatorname{mod} 4). \end{cases}$$

Returning to the question, since $p = 2$ and $2\mathbb{Z}$ does not divide $\Delta(R'/\mathbb{Z})$, then $\Delta(R'/\mathbb{Z})$ is not contained in $2\mathbb{Z}$, so necessarily we have that d is odd, $d \equiv 1(\operatorname{mod} 4)$ and

$$R' = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

Since $d \equiv 1(\operatorname{mod} 4)$, we have that $d = 1 + 4k$ for some $k \in \mathbb{Z}$. If k is even, then

$$d \equiv 1(\operatorname{mod} 8).$$

If k is odd, then $k - 1$ is even and $d = 5 + 4(k - 1)$, then

$$d \equiv 5(\operatorname{mod} 8).$$

Remember that, if R' is the integral closure of ring extension $\mathbb{Z} \subseteq \mathbb{Q}(\sqrt{2})$, then, given S a multiplicatively subset of $\mathbb{Z}$, we have that R'_S is the integral closure of extension $\mathbb{Z}_S \subseteq \mathbb{Q}(\sqrt{2})_S = \mathbb{Q}(\sqrt{2})$. Thus, given the multiplicative subset $S = \mathbb{Z} \setminus 2\mathbb{Z}$ of $\mathbb{Z}$, in order to apply the Theorem 7.6, we will prove that

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]_S = \mathbb{Z}_{(2)}\left[\frac{1+\sqrt{d}}{2}\right].$$

However it is clear. Indeed, calling $\delta = (1 + \sqrt{d})/2$, given

$$\frac{a + b\delta}{s} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]_S$$

we can rewrite it as

$$\frac{a}{s} + \frac{b}{s}\delta \in \mathbb{Z}_{(2)}\left[\frac{1+\sqrt{d}}{2}\right].$$

Then

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]_S \subseteq \mathbb{Z}_{(2)}\left[\frac{1+\sqrt{d}}{2}\right].$$

The other inclusion is trivial. Thus we can apply the Theorem 7.6. Moreover, it is easy to see that

$$f(X) = X^2 - X - \left(\frac{d-1}{4}\right)$$

is the minimal polynomial of $(1+\sqrt{d})/2$ over $\mathbb{Q}$. If $d \equiv 1(\bmod 8)$, then the image of $f(x)$ in $\mathbb{F}_2[X]$ is

$$\overline{f}(X) = X^2 - X = X(X-1).$$

Then, by Theorem 7.6, we conclude that

$$2\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathfrak{P}\mathfrak{Q},$$

where $\mathfrak{P}$, $\mathfrak{Q}$ are distinct prime ideals of R'. On the other hand, if $d \equiv 5(\bmod 8)$, then the image of $f(x)$ in $\mathbb{F}_2[X]$ is

$$\overline{f}(X) = X^2 - X - 1.$$

which is an irreducible polynomial in $\mathbb{F}_2[X]$, because it does not have root in $\mathbb{F}_2$. Thus, by Theorem 7.6, we conclude that

$$2\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathfrak{P},$$

where $\mathfrak{P}$ is a prime ideal of R'. □

1.8 Norms of Ideals

Question 1: Let $R = \mathbb{Z}[\sqrt{-1}]$ and z_1, $z_2 \in R$ with $z_2 \neq 0$. Show that there exist q, $r \in R$ such that

$$z_1 = z_2 q + r \qquad \text{and} \qquad 0 \leq N(r) < N(z_2).$$

Conclude that R is a Principal Ideal Domain.

Proof: Indeed, it is clear that $\mathbb{Q}(i)/\mathbb{Q}$ is a Galois extension, with Galois group $G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma\}$, where $\sigma : \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i)$ is the conjugation mapping. Thus the norm function of this extension evaluated in $z = x + iy$ can be calculated as

$$N(x+yi) = 1(x+yi)\cdot\sigma(x+yi) = (x+yi)(x-yi) = x^2+y^2.$$

Now we will prove that, given z_1, $z_2 \in R$ with $z_2 \neq 0$, there exist q, $r \in R$ such that $z_1 = z_2 q + r$ with $0 \leq N(r) < N(z_2)$. In fact, note that, if $z_1 = a + bi$ and $z_2 = c + di$ in $\mathbb{Z}[i]$, then

$$\frac{z_1}{z_2} = \frac{ac+bd}{c^2+d^2} + \left(\frac{bc-ad}{c^2+d^2}\right) i \in \mathbb{Q}[i].$$

Thus there are α, $\beta \in \mathbb{Q}$ such that $z_1/z_2 = \alpha + \beta i$. By elementary real analysis, we can choose λ, $\gamma \in \mathbb{Z}$ such that

$$|\lambda - \alpha| \leq \frac{1}{2} \qquad \text{and} \qquad |\gamma - \beta| \leq \frac{1}{2}.$$

Considering $q := \lambda + \gamma i \in \mathbb{Z}[i]$, note that

$$z_1 = (q - q + \alpha + \beta i)z_2 = qz_2 + (\alpha + \beta i - q)z_2.$$

Let $r := (\alpha + \beta i - q)z_2$. Note that $r \in \mathbb{Z}[i]$, because

$$r = (\alpha + \beta i)z_2 - qz_2 = z_1 - qz_2 \in \mathbb{Z}[i].$$

Moreover, we have that

$$\begin{aligned} 0 \leq N(r) = N(\alpha + \beta i - q)N(z_2) = N(z_2)N\big((\alpha - \lambda) + (\beta - \gamma)i\big) = N(z_2)[(\alpha - \lambda)^2 + (\beta - \gamma)^2] \\ \leq \frac{1}{4}N(z_2) + \frac{1}{4}N(z_2) = \frac{1}{2}N(z_2) < N(z_2). \end{aligned}$$

Finally I claim that $\mathbb{Z}[i]$ is a Principal Ideal Domain. Indeed, let $\mathfrak{A}$ be an ideal of $\mathbb{Z}[i]$. If $\mathfrak{A} = 0$, then $\mathfrak{A} = (0)$ is trivially a principal ideal. Suppose now that $\mathfrak{A} \neq 0$ and consider the following set

$$\mathcal{F} = \{N(a) \in \mathbb{N} \ ; \quad a \in \mathfrak{A},\ a \neq 0\}.$$

Clearly $\mathcal{F}$ is a nonempty subset of $\mathbb{N}$. By well-ordering principle, $\mathcal{F}$ has a minimum element n. Let $z_0 \in \mathfrak{A}$ such that $N(z_0) = n$. I claim that $\mathfrak{A} = (z_0)$. Indeed, since $z_0 \in \mathfrak{A}$, it is clear that

$$(z_0) \subseteq \mathfrak{A}.$$

On the other hand, given $z \in \mathfrak{A}$. By the division property proved above, there are $q, r \in \mathbb{Z}[i]$ such that $z = z_0 q + r$ with $0 \leq N(r) < N(z_0) = n$. Since $r = z - z_0 q \in \mathfrak{A}$ and the following property holds: Given $w \in \mathbb{Z}[i]$

$$N(w) = 0 \qquad \text{if and only if} \qquad w = 0,$$

we conclude that $r = 0$, thus $z = z_0 q \in (z_0)$ and so

$$\mathfrak{A} \subseteq (z_0).$$

Since $\mathfrak{A}$ is an arbitrary ideal of $\mathbb{Z}[i]$, we conclude that $\mathbb{Z}[i]$ is a Principal Ideal Domain. $\square$

1.9 Cyclotomic Fields

Question 1: Let ε_n denote the primitive n-th root of unity. If m is an odd integer, prove that $\mathbb{Q}(\varepsilon_m) = \mathbb{Q}(\varepsilon_{2m})$ and conclude that 2 ramifies in $\mathbb{Q}(\varepsilon_{2m})$ even though 2 divides $2m$. Show this is the only exception to assertion "p ramifies in $\mathbb{Q}(\varepsilon_n)$ whenever p is a prime dividing n".

Proof: In fact, since $(\epsilon_m)^m = 1$, we have that $(\epsilon_m)^{2m} = 1$, thus $\varepsilon_m \in \mathbb{Q}(\varepsilon_{2m})$ and so

$$\mathbb{Q}(\varepsilon_m) \subseteq \mathbb{Q}(\varepsilon_{2m}).$$

In order to show that $\mathbb{Q}(\varepsilon_m) = \mathbb{Q}(\varepsilon_{2m})$, it is enough to show that $[\mathbb{Q}(\varepsilon_m) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon_m) : \mathbb{Q}]$. Since $\gcd(2,m) = 1$ and the Euler's Totient function is a multiplicative function, we conclude that

$$[\mathbb{Q}(\varepsilon_{2m}) : \mathbb{Q}] = \phi(2m) = \phi(2)\phi(m) = \phi(m) = [\mathbb{Q}(\varepsilon_m) : \mathbb{Q}]$$

and so $\mathbb{Q}(\varepsilon_{2m}) = \mathbb{Q}(\varepsilon_m)$. Since m is an odd integer, we have that 2 does not divide m, so, by Theorem 9.2, we conclude that 2 ramifies in $\mathbb{Q}(\varepsilon_m) = \mathbb{Q}(\varepsilon_{2m})$.

Now suppose that p divides n, then, we have that $n = p^a m$, where $a \geq 1$ and $\gcd(p,m) = 1$. By Theorem 9.2, we have that p has ramification index $\phi(p^a)$. Since $\phi(p^a) > 1$ except when $p = 2$ and $a = 1$, we conclude that the case $p = 2$ is the only exception to the assertion "p ramifies in $\mathbb{Q}(\varepsilon_n)$ whenever p is a prime dividing n". □

1.10 Lattices in Real Vector Spaces

Question 1 [*Second edition*]: The one-dimensional vector space $V = \mathbb{R}$ contains the rank two abelian group $A = \mathbb{Z} + \sqrt{2}\mathbb{Z}$. Prove that this group can not be a lattice.

Proof: In fact, since $1 < \sqrt{2} < 2$, we have that $0 < \sqrt{2} - 1 < 1$. Consider the sequence $a_n = (\sqrt{2} - 1)^n$. Since $0 < \sqrt{2} - 1 < 1$, we have that this sequence is strictly decreasing and $0 < a_n < 1$ for all $n \in \mathbb{N}$. Now, in order to prove that this group is not a Lattice in $\mathbb{R}$, it is enough to show that $a_n \in \mathbb{Z} + \sqrt{2}\mathbb{Z}$ for all $n \in \mathbb{N}$, and thus we will conclude that the sphere $[-1,1]$ contains infinity elements of $\mathbb{Z} + \sqrt{2}\mathbb{Z}$. However, this is easy, because if $n = 2m$, then

$$a_n = (\sqrt{2} - 1)^n = \sum_{k=0}^{n} \binom{2m}{k} (\sqrt{2})^k (-1)^{2m-k} = \sum_{k=0}^{m} \binom{2m}{2k} 2^k (-1)^{2(m-k)} + \left(\sum_{k=0}^{m} \binom{2m}{2k+1} 2^k (-1)^{2(m-k)+1} \right) \sqrt{2} \in \mathbb{Z} + \sqrt{2}\mathbb{Z}.$$

If $n = 2m - 1$, then

$$a_n = (\sqrt{2} - 1)^n = \sum_{k=0}^{n} \binom{2m+1}{k} (\sqrt{2})^k (-1)^{2m-k} = \sum_{k=0}^{m} \binom{2m+1}{2k} 2^k (-1)^{2m-(2k+1)} + \left(\sum_{k=0}^{m} \binom{2m}{2k+1} 2^k (-1)^{2(m-k)+1} \right) \sqrt{2} \in \mathbb{Z} + \sqrt{2}\mathbb{Z}.$$

Thus $a_n \in \mathbb{Z} + \sqrt{2}\mathbb{Z}$ for all $n \in \mathbb{N}$, which implies that $[-1, 1]$ contains infinite elements of $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ and so $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ can not be a lattice. □

Chapter 2

Complete Fields

2.1 Valuations

This section does not contain exercises.

2.2 Completions

Lemma: In $\mathbb{Q}_p$, prove that the element $1/(1-p)$ has representation

$$1+p+p^2+\cdots+p^n+\cdots.$$

Proof: It is enough to show that the partial sums converges $(s_n)_{n\in\mathbb{N}}$ to $1/(1-p)$. Note that, given $n\in\mathbb{N}$, we have that

$$\left|s_n-\frac{1}{1-p}\right|=\left|\frac{(1-p^{n+1})-1}{1-p}\right|=\left|\frac{-p^{n+1}}{1-p}\right|=\left|\frac{1}{1-p}\right|\left(\frac{1}{p^{n+1}}\right)$$

Letting $n\to\infty$, we conclude that $(s_n)_{n\in\mathbb{N}}$ converges to $1/(1-p)$. □

Corollary: In $\mathbb{Q}_p$, prove that the element $1/(1-p^k)$ has representation

$$1+p^k+p^{2k}+\cdots+p^{nk}+\cdots.$$

Proof: Just imitate the proof of the Lemma above. □

Question 1: In $\mathbb{Q}_3$, show that the series

$$1+2\cdot 3+3^2+2\cdot 3^3+\cdots+3^{2n}+2\cdot 3^{2n+1}+\cdots$$

converges to a rational number.

Proof: Note that

$$1+2\cdot 3+3^2+2\cdot 3^3+\cdots+3^{2n}+2\cdot 3^{2n+1}+\cdots=\sum_{k=0}^{\infty}\left(3^2\right)^k+2\cdot(3+3^3+\cdots+3^{2n+1}+\cdots)=$$

$$\sum_{k=0}^{\infty}\left(3^2\right)^k+6\sum_{k=0}^{\infty}\left(3^2\right)^k=\frac{1}{1-3^2}+\frac{6}{1-3^2}=-\frac{1}{8}-\frac{6}{8}=-\frac{7}{8}.$$

Then $1+2\cdot 3+3^2+2\cdot 3^3+\cdots+3^{2n}+2\cdot 3^{2n+1}+\cdots=-7/8\in\mathbb{Q}$. □

Question 2: More generally in $\mathbb{Q}_p$, show that the periodic series

$$\sum_{k=0}^{\infty}a_kp^k$$

with $a_k\in\{0,1,\ldots,p-1\}$ and $a_k=a_{k+m}$ for some $m\in\mathbb{N}$ fixed and all $k\in\mathbb{N}_0$ converges to a rational number.

Proof: Firstly note that we can write the series $\sum_{k=0}^{\infty}a_kp^k$ as the following sum

$$\sum_{k=0}^{\infty}a_kp^k=\sum_{k=0}^{\infty}a_{mk}p^{mk}+\sum_{k=0}^{\infty}a_{mk+1}p^{mk+1}+\cdots\sum_{k=0}^{\infty}a_{mk+(m-1)}p^{mk+(m-1)}.$$

Using the fact that $a_k=a_{k+m}$ for every $k\in\mathbb{N}_0$ and that $a_i=a_{m+i}=a_{2m+i}=\cdots=a_{km+i}=\ldots$ for all $i\in\{0,\ldots,m-1\}$, we have that

$$\sum_{k=0}^{\infty}a_kp^k=a_0\sum_{k=0}^{\infty}p^{mk}+a_1\sum_{k=0}^{\infty}p^{mk+1}+\cdots+a_{m-1}\sum_{k=0}^{\infty}p^{mk+(m-1)}=a_0+a_1p\sum_{k=0}^{\infty}p^{mk}+\cdots a_{m-1}p^{m-1}\sum_{k=0}^{\infty}p^{mk}$$

$$=\left(a_0+a_1p+\ldots+a_{m-1}p^{m-1}\right)\sum_{k=0}^{\infty}(p^m)^k=\frac{a_0+a_1p+\ldots+a_{m-1}p^{m-1}}{1-p^m}\in\mathbb{Q}.$$

Then the periodic series converges to a rational number.

Chapter 3

Application of the Kronecker bound in ideal class group calculation

The Kronecker bounder is a positive real number which appears in the middle of proof of finiteness of class group in number fields. More especifically, it appears in the following proposition.

Proposition 3.1. *Let $\mathcal{K}$ be a number field. Then there exists a constant $\chi > 0$ such that such that in every nonzero ideal $\mathfrak{a} \subseteq \mathcal{O}_K = \sum_{k=1}^{n} \mathbb{Z}e_i$, there is a nonzero $\alpha \in \mathfrak{a}$ such that*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \chi[\mathcal{O}_K : \mathfrak{a}],$$

where the constant χ is

$$\chi = \prod_{\sigma \in \mathrm{Hom}(K,\mathbb{C})} \sum_{i=1}^{n} |\sigma(e_i)|.$$

Proof: Consult the Theorem 2.1 of [**?**]. □

The Kronecker bound can help us to determine the ideal class group of some number fields if we know the following theorem.

Theorem 3.2. *Let $\mathcal{K}$ be a number field. The ideal classes of $\mathcal{K}$ satisfies the two following properties:*

1. *They are represented by ideals with norm at most χ;*
2. *They are generated as a group by prime ideals $\mathfrak{p}$ with $N(\mathfrak{p}) \leq \chi$.*

Proof: Consult the Theorem 2.2 of [**?**] □

Using the Theorem 3.2 and the Dedekind-Kummer Theorem, which we will enunciate in the following, we will use the Kronecker bound to determine the ideal class group of $\mathbb{Q}(\sqrt{-5})$.

Theorem 3.3 (Dedekind-Kummer)**.** *Let R be a Dedekind domain with field of fractions K and L be a finite separable extension of K. Consider S the integral closure of R in S. Assume that $L = K(\alpha)$, $\alpha \in S$, let $f(X) \in R[X]$ be the minimal polynomial of α and assume that $S = R[\alpha]$. Suppose that $g_1(X), \dots, g_n(X) \in R[X]$ are monic polynomials for which*

$$\overline{f}(X) = \prod_{k=1}^{n} \overline{g_k}(X)^{e_k}$$

is a complete factorization of $\overline{f}(X)$ in $(R/\mathfrak{p})[X]$, where $\overline{\cdot}$ denotes reduction modulo $\mathfrak{P}$ and let $\mathfrak{Q}_i = (\mathfrak{P}, g_i(\alpha))$ be the S-ideal generated by $\mathfrak{P}_i$ and $g_i(\alpha)$. Then

$$\mathfrak{P}S = \prod_{k=1}^{n} \mathfrak{Q}_k^{e_k}$$

is the factorization of $\mathfrak{P}S$ in S and the residue degree of $\mathfrak{Q}_i$ is $f_i := \deg(g_i)$.

Proof: Consult the Theorem 6.13 of [**?**] □

Example 3.4. *Using the Kronecker bound, prove that*

$$\mathrm{CL}(\mathbb{Q}(\sqrt{-5})) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right).$$

Proof: Firstly we will determine the field homomorphisms $\sigma : \mathbb{Q}(\sqrt{-5}) \longrightarrow \mathbb{C}$. Note that, given $\sigma \in \mathrm{Hom}(\mathbb{Q}(\sqrt{-5}), \mathbb{C})$, we have that

$$\sigma(\sqrt{-5})^2 = \sigma((\sqrt{-5})^2) = \sigma(-5) = -5.$$

Thus $\sigma(\sqrt{-5}) = \sqrt{5}i$ or $\sigma(\sqrt{-5}) = -\sqrt{5}i$, then we conclude that $\mathrm{Hom}(\mathbb{Q}(\sqrt{-5}), \mathbb{C}) = \{\iota, \sigma\}$, where

$$\begin{aligned} \iota : \mathbb{Q}(\sqrt{-5}) &\longrightarrow \mathbb{C} \\ a + b\sqrt{-5} &\longmapsto a + b\sqrt{-5} \end{aligned} \quad \text{and} \quad \begin{aligned} \sigma : \mathbb{Q}(\sqrt{-5}) &\longrightarrow \mathbb{C} \\ a + b\sqrt{-5} &\longmapsto a - b\sqrt{-5} \end{aligned}$$

Consider now the $\mathbb{Z}$-basis $\{1, \sqrt{-5}\}$ for $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$. Thus the Kronecker bound associated to this $\mathbb{Z}$-basis is

$$\chi = (|\iota(1)| + |\iota(\sqrt{-5})|) \cdot (|\sigma(1)| + |\sigma(\sqrt{-5})|) = (1 + \sqrt{5})^2 \approx 10,4.$$

By Theorem 3.2, we conclude that the group $\mathrm{CL}(\mathbb{Q}(\sqrt{-5}))$ satisfies the following two conditions:

- It is represented by ideals $\mathfrak{A} \subseteq \mathbb{Z}[\sqrt{-5}]$ such that $N(\mathfrak{A}) \leq 10$;

- It is generated by prime ideals $\mathfrak{P}$ such that $N(\mathfrak{P}) \leq 10$.

Let $(p) = \mathfrak{P} \cap \mathbb{Z}$. Since $N(\mathfrak{P}) = p^f \leq 10$, where $f = [\mathbb{Z}[\sqrt{-5}]/\mathfrak{P} : \mathbb{Z}/(p)]$, we conclude that the only possible primes integers for p are $p = 2$, 3, 5 or 7. In particular, since

$$p\mathbb{Z}[\sqrt{-5}] = (\mathfrak{P} \cap \mathbb{Z})\mathbb{Z}[\sqrt{-5}] \subseteq \mathfrak{P},$$

we conclude that $\mathfrak{P}$ divides $2\mathbb{Z}[\sqrt{-5}]$, $3\mathbb{Z}[\sqrt{-5}]$, $5\mathbb{Z}[\sqrt{-5}]$ or $7\mathbb{Z}[\sqrt{-5}]$. Thus, if $\mathfrak{P}$ is one of the generators of $\mathrm{CL}(\mathbb{Q}(\sqrt{-5}))$, then $\mathfrak{P}$ is one of prime factors of $2\mathbb{Z}[\sqrt{-5}]$, $3\mathbb{Z}[\sqrt{-5}]$, $5\mathbb{Z}[\sqrt{-5}]$ or $7\mathbb{Z}[\sqrt{-5}]$. Now we will calculate the decomposition of each of these ideals in product of prime ideals using the Dedekind-Kummer Theorem. Knowing that $f(X) = X^2 + 5$ is the minimal polynomial of $\sqrt{-5}$ over $\mathbb{Q}$, we obtain the following factorizations:

- $2\mathbb{Z}[\sqrt{-5}]$: Note that, in $\mathbb{F}_2$, we have $\overline{f}(X) = X^2+1 = (X+1)(X+1)$. Calling $\overline{q}_1(X) = (X+1)$ and $\overline{q}_2(X) = (X+1)$, by Dedekind-Kummer Theorem, we conclude that

$$2\mathbb{Z}[\sqrt{-5}] = (2, 1+\sqrt{-5})(2, 1+\sqrt{-5}) = (2, 1+\sqrt{-5})^2 := \mathfrak{P}_2^2.$$

- $3\mathbb{Z}[\sqrt{-5}]$: Note that, in $\mathbb{F}_3$, we have $\overline{f}(X) = X^2+2 = (X+1)(X+2)$. Calling $\overline{q}_1(X) = (X+1)$ and $\overline{q}_2(X) = (X+2)$, by Dedekind-Kummer Theorem, we conclude that

$$3\mathbb{Z}[\sqrt{-5}] = (3, 1+\sqrt{-5})(3, 2+\sqrt{-5}) := \mathfrak{P}_3\mathfrak{P}_3'.$$

- $5\mathbb{Z}[\sqrt{-5}]$: Note that, in $\mathbb{F}_5$, we have $\overline{f}(X) = X^2$. Calling $\overline{q}_1(X) = X$ and $\overline{q}_2(X) = X$, by Dedekind-Kummer Theorem, we conclude that

$$5\mathbb{Z}[\sqrt{-5}] = (\sqrt{-5})(\sqrt{-5}) = (\sqrt{-5})^2 := \mathfrak{P}_5^2.$$

- $7\mathbb{Z}[\sqrt{-5}]$: Note that, in $\mathbb{F}_7$, we have $\overline{f}(X) = X^2+5 = (X+3)(X+4)$. Calling $\overline{q}_1(X) = (X+3)$ and $\overline{q}_2(X) = (X+4)$, by Dedekind-Kummer Theorem, we conclude that

$$7\mathbb{Z}[\sqrt{-5}] = (7, 3+\sqrt{-5})(7, 4+\sqrt{-5}) := \mathfrak{P}_7\mathfrak{P}_7'.$$

Since, in $\mathrm{CL}[\mathbb{Q}(\sqrt{-5})]$, principal ideals become trivial, we conclude that

$$[\mathfrak{P}_2]^2 = [1] \qquad [\mathfrak{P}_3\mathfrak{P}_3'] = [1] \qquad [\mathfrak{P}_5] = [1] \qquad [\mathfrak{P}_7\mathfrak{P}_7'] = [1],$$

and then, by Theorem 3.2, $\mathrm{CL}(\mathbb{Q}[\sqrt{-5}])$ is a group generated by $[\mathfrak{P}_1]$, $[\mathfrak{P}_3]$ and $[\mathfrak{P}_7]$. However, observe that

$$\mathfrak{P}_2\mathfrak{P}_3 = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6, 1+\sqrt{-5}, -4+2\sqrt{-5}) = (1+\sqrt{-5})$$

and

$$\mathfrak{P}_2\mathfrak{P}_7 = (2, 1+\sqrt{-5})(7, 3+\sqrt{-5}) = (14, 6+2\sqrt{-5}, 7+7\sqrt{-5}, -2+4\sqrt{-5}) = (3+\sqrt{-5})$$

Thus we conclude that $[\mathfrak{P}_2][\mathfrak{P}_3] = [\mathfrak{P}_2\mathfrak{P}_3] = [1]$ and $[\mathfrak{P}_2][\mathfrak{P}_7] = [\mathfrak{P}_2\mathfrak{P}_7] = [1]$, which allows us to conclude that

$$[\mathfrak{P}_3] = [\mathfrak{P}_2]^{-1} \qquad \text{and} \qquad [\mathfrak{P}_7] = [\mathfrak{P}_2]^{-1}.$$

Thus we conclude that $\mathrm{CL}(\mathbb{Q}(\sqrt{-5})) = \langle[\mathfrak{P}_2]\rangle$. Since $[\mathfrak{P}_2]^2 = [1]$ and $[\mathfrak{P}_2] \neq [1]$, because $\mathfrak{P}_2$ is not principal ideal, we conclude that $\mathrm{CL}(\mathbb{Q}(\sqrt{-5}))$ is isomorphic to the cyclic group of order 2, that is

$$\mathrm{CL}(\mathbb{Q}(\sqrt{-5})) \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right).$$

In particular, $\mathbb{Q}(\sqrt{-5})$ is not a principal ideal domain, because $\mathrm{CL}(\mathbb{Q}(\sqrt{-5}))$ is not the trivial group. □

Chapter 4

Convergence in p-adic number fields

The purpose of these notes is to solve the two first questions of the section 2.2 of the book [1]. These questions are about convergence in the p-adic number fields. However we will do a brief introduction about these fields. As well as $\mathbb{R}$ and $\mathbb{C}$ have a norm, we also can define a norm in an arbitrary field.

Definition 4.1. *Let $\mathbb{K}$ be a field, a function $\|\cdot\| : \mathbb{K} \longrightarrow \mathbb{R}$ is called a norm if it satisfies the four following properties:*

- $\|x\| \geq 0$ *for all* $x \in \mathbb{K}$*;*
- $\|x\| = 0$ *if and only if* $x = 0$*;*
- $\|xy\| = \|x\|\|y\|$ *for all* x, $y \in \mathbb{K}$*;*
- $\|x+y\| \leq \|x\| + \|y\|$ *for all* x, $y \in \mathbb{K}$*.*

For example, the following functions

$$\begin{aligned} \|\cdot\|_\infty : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto |x| \end{aligned} \qquad \text{and} \qquad \begin{aligned} \|\cdot\| : \mathbb{C} &\longrightarrow \mathbb{R} \\ a+bi &\longmapsto \sqrt{a^2+b^2} \end{aligned}$$

are norms in the fields $\mathbb{R}$, $\mathbb{C}$, respectively. Now our goal is study a specific type of norm in $\mathbb{Q}$.

Definition 4.2. *Let p be a prime integer and $n \in \mathbb{Z}$, we define the order of p in n, denoting it by $\mathrm{Ord}_p(n)$, the highest non-negative integer m such that p^m divides n.*

Viewing the order as a function $\mathrm{Ord}_p : \mathbb{Z} \longrightarrow \mathbb{Z}$, since this this function has the following property

$$\mathrm{Ord}_p(n \cdot m) = \mathrm{Ord}_p(n) + \mathrm{Ord}_p(m),$$

we can naturally extend the order function to $\mathbb{Q}$ defining

$$\begin{aligned} \mathrm{Ord}_p : \mathbb{Q} &\longrightarrow \mathbb{Z} \\ m/n &\longmapsto \mathrm{Ord}_p(m) - \mathrm{Ord}_p(n) \end{aligned}$$

It is easy to see that this functions is well defined. With this function in mind, we can define the p-adic norm:

Proposition 4.3 (p-adic norm)**.** *The function*

$$\begin{aligned} \| \cdot \|_p : \mathbb{Q} &\longrightarrow \mathbb{Q} \\ x &\longmapsto \begin{cases} 0 & \text{if } x = 0; \\ \frac{1}{p^{\mathrm{Ord}_p(x)}} & \text{if } x \neq 0. \end{cases} \end{aligned}$$

is a norm in $\mathbb{Q}$

Proof: Consult the Proposition 1.2.1 of [2]. □

Since $(\mathbb{Q}, \| \cdot \|_\infty)$ can be completed as a quotient of ring of Cauchy sequences in $(\mathbb{Q}, \| \cdot \|_\infty)$ by the ideal of convergent sequences in $(\mathbb{Q}, \| \cdot \|_\infty)$ that converges to 0, obtaining a complete field, in this case $(\mathbb{R}, \| \cdot \|_\infty)$, we also can do the same procedure in $(\mathbb{Q}, \| \cdot \|_p)$. The field obtained with this procedure is called the p-adic number field.

Definition 4.4. *Let p be a prime integer. The completion of the metric space $(\mathbb{Q}, \| \cdot \|_p)$ is called the field of p-adic numbers and it is denoted by $\mathbb{Q}_p$.*

Translating the usual definition of convergence to $(\mathbb{Q}, \| \cdot \|_p)$, we can formulate the following definition.

Definition 4.5. *Let p be a prime integer and $\sum_{n=1}^{\infty} a_n$ be a series in $\mathbb{Q}_p$. This series converges to x in $\mathbb{Q}_p$ if the sequence $(s_n)_{n \in \mathbb{N}}$ of partial sums converges in $\mathbb{Q}_p$, that is, if*

$$\lim_{n \to \infty} \|s_n - x\|_p = 0.$$

Now we will go to prove a lemma which will help us to solve the two questions.

Lemma 4.6. *Let p be a prime integer and consider the following series in $\mathbb{Q}_p$*

$$1 + p^k + p^{2k} + \cdots + p^{nk} + \cdots$$

Then this series converges to the rational number

$$\frac{1}{1-p^k}.$$

Proof: It is enough to show that the partial sums converges $(s_n)_{n\in\mathbb{N}}$ to $1/(1-p^k)$. Given $n \in \mathbb{N}$, we have

$$\left\|s_n - \frac{1}{1-p^k}\right\|_p = \left\|\frac{(1-p^{k(n+1)})-1}{1-p^k}\right\|_p = \left\|\frac{-p^{k(n+1)}}{1-p}\right\|_p = \left\|\frac{1}{1-p^k}\right\|_p \cdot \|-p^{k(n+1)}\|_p = \left\|\frac{1}{1-p^k}\right\|_p \|p^{k(n+1)}\|_p = \left\|\frac{1}{1-p^k}\right\|_p \left(\frac{1}{p^{n+1}}\right).$$

Letting $n \to \infty$, we conclude that $(s_n)_{n\in\mathbb{N}}$ converges to $1/(1-p)$. □

Let's get to the questions at hand.

Question 4.7 (Question 1 of section 2.2 of [1]). *In $\mathbb{Q}_3$, show that the series*

$$1 + 2\cdot 3 + 3^2 + 2\cdot 3^3 + \cdots + 3^{2n} + 2\cdot 3^{2n+1} + \cdots$$

converges to a rational number.

Proof: Set $L = 1 + 2\cdot 3 + 3^2 + 2\cdot 3^3 + \cdots + 3^{2n} + 2\cdot 3^{2n+1} + \cdots$. Note that

$$L = \sum_{k=0}^{\infty} \left(3^2\right)^k + 2\cdot \sum_{k=0}^{\infty} \left(3\right)^{2k+1} = \sum_{k=0}^{\infty} \left(3\right)^{2k} + 2\cdot 3 \sum_{k=0}^{\infty} \left(3^2\right)^k = \sum_{k=0}^{\infty} \left(3\right)^{2k} + 2\cdot 3 \sum_{k=0}^{\infty} \left(3^2\right)^k = 7\sum_{k=0}^{\infty} \left(3^2\right)^k = \frac{7}{1-3^2} = -\frac{7}{8}.$$

Thus this series converges to a rational number in $\mathbb{Q}_3$. □

Question 4.8 (Question 2 of section 2.2 of [1]). *More generally in $\mathbb{Q}_p$, show that the periodic series*

$$\sum_{k=0}^{\infty} a_k p^k$$

with $a_k \in \{0, 1, \ldots, p-1\}$ and $a_k = a_{k+m}$ for some $m \in \mathbb{N}$ fixed and all $k \in \mathbb{N}_0$ converges to a rational number.

Proof: Firstly note that the series $\sum_{k=0}^{\infty} a_k p^k$ can be written as

$$\sum_{k=0}^{\infty} a_k p^k = \sum_{k=0}^{\infty} a_{mk} p^{mk} + \sum_{k=0}^{\infty} a_{mk+1} p^{mk+1} + \cdots \sum_{k=0}^{\infty} a_{mk+(m-1)} p^{mk+(m-1)}.$$

Using the fact that $a_k = a_{k+m}$ for every $k \in \mathbb{N}_0$ and that

$$\begin{cases} a_0 = a_{km} & \text{for all } k \in \mathbb{N}_0; \\ a_1 = a_{km+1} & \text{for all } k \in \mathbb{N}_0; \\ \vdots & \vdots \\ a_{m-1} = a_{km+(m-1)} & \text{for all } k \in \mathbb{N}_0. \end{cases}$$

we can write $\sum_{n=0}^{\infty} a_n p^n$ as

$$\sum_{k=0}^{\infty} a_k p^k = a_0 \sum_{k=0}^{\infty} p^{mk} + a_1 \sum_{k=0}^{\infty} p^{mk+1} + \cdots + a_{m-1} \sum_{k=0}^{\infty} p^{mk+(m-1)} =$$

$$a_0 \sum_{k=0}^{\infty} p^{mk} + a_1 p \sum_{k=0}^{\infty} p^{mk} + \cdots a_{m-1} p^{m-1} \sum_{k=0}^{\infty} p^{mk} = (a_0 + a_1 p + \ldots + a_{m-1} p^{m-1}) \sum_{k=0}^{\infty} (p^m)^k =$$

$$\frac{a_0 + a_1 p + \ldots + a_{m-1} p^{m-1}}{1 - p^m}.$$

Thus any periodical series converges to a rational number in $\mathbb{Q}_p$. □

Let p be a prime integer and $\mathbb{Q}_p$ be the completion of $(\mathbb{Q}, \| \cdot \|_p)$. Since $\| \cdot \|_p$ is a non-Archimedean norm, it is classical exercise to show that the subset

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ ; \ \|x\| \leq 1\} \subseteq \mathbb{Q}_p$$

is a discrete valuation domain, whose maximal ideal $\mathfrak{m}$ is exactly its subset $\{x \in \mathbb{Q}_p \ ; \ \|x\| = 1\}$. We call $(\mathbb{Z}_p, \mathfrak{m})$ by the ring of p-adic integers. In the Question 4.8, we had that $\|L\|_p \leq 1$, thus we conclude that $L \in \mathbb{Z}_3$, even though $L \in \mathbb{Q} \setminus \mathbb{Z}$, thus we see $\mathbb{Z}_p$ can contain non-integer numbers.

Bibliography

[1] JANUSZ, Gerald J. Algebraic number fields. American Mathematical Soc., 1996.

[2] KOBLITZ, Neal. p-adic Numbers, p-adic Analysis, and Zeta-Functions. Springer Science Business Media, 2012.