Application of the Kronecker bound in the ideal class group calculation

Kevin Alves Vasconcellos

July, 2021

Abstract

The purpose of this note is to show how the Kronecker bound can be used to calculate the ideal class group of a Dedekind domain. It will be calculated the ideal class group of $\mathbb{Z}[\sqrt{-5}]$, which is the integral closure of $\mathbb{Z}$ in the Galois extension $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$.

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

Proposition 1. *Let K be a number field. Then there exists a constant $\chi > 0$ 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 [2]. □

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

Theorem 2. *Let K be a number field. The ideal classes of $\mathcal{O}_K$ satisfies the following two 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 [2]. □

Using the Theorem 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 $\mathbb{Z}[\sqrt{-5}]$.

Theorem 3 (Dedekind-Kummer Theorem)**.** *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 L. 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 $g_1(X), \ldots, g_n(X) \in R[X]$ 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 $\bar{\cdot}$ denotes reduction modulo $\mathfrak{p}$, and let $\mathfrak{Q}_i = (\mathfrak{p}, g_i(\alpha))$ be the S-ideal generated by $\mathfrak{p}$ 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 [3]. □

Proposition 4. *Let $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ be the integral closure of the number field $\mathbb{Q}(\sqrt{-5})$. Using the Kronecker bound, prove that the ideal class group of $\mathbb{Z}[\sqrt{-5}]$ is*

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

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

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

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

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

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 2, we conclude that the group $\mathrm{CL}(\mathbb{Z}[\sqrt{-5}])$ is generated by prime ideals $\mathfrak{P}$ such that $N(\mathfrak{P}) \leq 10$. Let $\mathfrak{P}$ be a prime ideal of $\mathbb{Z}[\sqrt{-5}]$ such that $N(\mathfrak{P}) \leq 10$ and $(p) = \mathfrak{P} \cap \mathbb{Z}$. 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 values 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 $\mathrm{CL}(\mathbb{Z}[\sqrt{-5}])$, 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 $\overline{q}_1(X) = X$, by Dedekind-Kummer Theorem, we conclude that

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

- $7\mathbb{Z}[\sqrt{-5}]$: 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 $\mathrm{CL}(\mathbb{Z}[\sqrt{-5}])$, 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 2, $\mathrm{CL}(\mathbb{Z}[\sqrt{-5}])$ 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 $\mathrm{CL}(\mathbb{Z}[\sqrt{-5})] = \langle[\mathfrak{P}_2]\rangle$. Since $[\mathfrak{P}_2]^2 = [1]$ and $[\mathfrak{P}_2] \neq [1]$, because $\mathfrak{P}_2$ is not fractional principal ideal (see Remark 5), we conclude that $\mathrm{CL}(\mathbb{Z}[\sqrt{-5}])$ is isomorphic to the cyclic group of order 2, that is

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

In particular, $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain, because $\mathrm{CL}(\mathbb{Z}[\sqrt{-5}])$ is not the trivial group. Moreover, since $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, we also conclude that $\mathbb{Z}[\sqrt{-5}]$ is not an unique factorization domain. □

Remark 5. $\mathfrak{P} = (2, 1+\sqrt{-5})$ *is not a principal fractional ideal of* $\mathbb{Z}[\sqrt{-5}]$. *Indeed, Suppose that*

$$(2, 1+\sqrt{-5}) = \alpha\mathbb{Z}[\sqrt{-5}]$$

for some $\alpha \in \mathbb{Q}(\sqrt{-5})^\times$. *In particular, we would have that* $\alpha \in \mathbb{Z}[\sqrt{-5}]$, *that is,* $\alpha = a + b\sqrt{-5}$, *with* $a, b \in \mathbb{Z}$. *Since the norm function of field extension* $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ *is given by the mapping*

$$N : \mathbb{Q}(\sqrt{-5}) \longrightarrow \mathbb{Q}$$
$$a + b\sqrt{-5} \longmapsto a^2 + 5b^2,$$

we conclude that there would be $m, m' \in \mathbb{Z}[\sqrt{-5}]$ *such that*

$$4 = N(2) = N(\alpha m) = N(\alpha)N(m)$$
$$6 = N(1+\sqrt{-5}) = N(\alpha m') = N(\alpha)N(m').$$

Thus necessarily we have that $N(\alpha) = 2$. *However there is no* $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ *such that* $N(a+\sqrt{-5}) = 2$, *because the equation* $a^2 + 5b^2 = 2$ *has no diophantine solution.*

Remark 6. *Since* $\mathrm{CL}(\mathbb{Z}[\sqrt{-5}])$ *has order* 2, *given an ideal* $\mathfrak{A}$ *of* $\mathbb{Z}[\sqrt{-5}]$, *we have that* $[\mathfrak{A}]^2 = [1]$, *thus either* $\mathfrak{A}$, *or* $\mathfrak{A}^2$ *is principal ideal of* $\mathbb{Z}[\sqrt{-5}]$.

References

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

[2] CONRAD, K. Ideal Classes and the Kronecker bound. Lecture note.

[3] SUTHERLAND, A. Ideal norms and the Dedekind-Kummer theorem, 2015. Lecture Note.