Ludwig-Maximilians-Universität München
Fakultät für Mathematik, Informatik und Statistik
Mathematisches Institut

Bachelor's thesis

Computation of (S, T)-units

Matthias Christoph Bernhard Paulsen

February 2017

Advisor: Prof. Dr. Werner Bley

Recent conjectures in algebraic number theory like the Rubin Stark conjecture rely on (S,T)-units, which are a subgroup of the S-units of an algebraic number field. In this thesis, a practical algorithm for the computation of (S,T)-units will be developed and an implementation in the computational algebra system Magma will be given. Furthermore, the connection to the (S,T)-class group will be revealed and will be used to verify the results of the algorithm.

Contents

1 Introduction **5**

2 From units to S-units **8**
2.1 Unit and class group computation 8
2.2 Definition of S-units 11
2.3 Computation of S-units 12
2.4 The S-class group 13

3 From S-units to (S,T)-units **15**
3.1 Idea and Definition 15
3.2 Computation of (S,T)-units 16
3.3 Implementation within Magma 18
3.4 The (S,T)-class group 20
3.5 Computation of the (S,T)-class group 22
3.6 Heuristic verification 23

4 Examples **25**

List of symbols **28**

Source code of STClassGroup **30**

Bibliography **33**

1 Introduction

Throughout this thesis, we fix an algebraic number field K. We denote by $\mathcal{O}_K$ its ring of integers and by $\mathcal{O}_K^\times$ the group of units in $\mathcal{O}_K$. In general, $\mathcal{O}_K$ is not a unique factorization domain. This motivates the passage from integers to ideals. Let P_K be the set of prime ideals[1] in $\mathcal{O}_K$. Because $\mathcal{O}_K$ is a Dedekind domain, every ideal $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$ has a unique decomposition

$$\mathfrak{a} = \prod_{\mathfrak{p} \in P_K} \mathfrak{p}^{e_\mathfrak{p}} , \quad e_\mathfrak{p} \in \mathbb{N}_0$$

with $e_\mathfrak{p} = 0$ for almost all $\mathfrak{p} \in P_K$. In this sense, ideals and prime ideals generalize the usual integers and prime numbers naturally.

Ideals (except the zero ideal) are just a special case of *fractional ideals*, i. e. finitely generated non-zero $\mathcal{O}_K$-submodules of K. The set I_K of fractional ideals in K forms a group, where the inverse of $\mathfrak{a} \in I_K$ is given by

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \lhd \mathcal{O}_K\} .$$

Every fractional ideal $\mathfrak{a} \in I_K$ has a unique decomposition

$$\mathfrak{a} = \prod_{\mathfrak{p} \in P_K} \mathfrak{p}^{e_\mathfrak{p}} , \quad e_\mathfrak{p} \in \mathbb{Z}$$

with $e_\mathfrak{p} = 0$ for almost all $\mathfrak{p} \in P_K$. Therefore, I_K can be considered as the free abelian group over P_K.

Each prime ideal $\mathfrak{p} \in P_K$ defines a discrete valuation $v_\mathfrak{p} \colon K^\times \to \mathbb{Z}$ where $v_\mathfrak{p}(\alpha) = e_\mathfrak{p}$ is the exponent of $\mathfrak{p}$ in the prime decomposition of $\alpha\mathcal{O}_K$. For convenience, let $v_\mathfrak{p}(0) = \infty$. It follows that

$$\begin{aligned} \mathcal{O}_K &= \{\alpha \in K \mid v_\mathfrak{p}(\alpha) \geq 0,\ \mathfrak{p} \in P_K\} \\ \mathcal{O}_K^\times &= \{\alpha \in K \mid v_\mathfrak{p}(\alpha) = 0,\ \mathfrak{p} \in P_K\} . \end{aligned}$$

As usual, we define the norm of an ideal $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$ via $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$. The multiplication by an element $\alpha \in K$ constitutes a $\mathbb{Q}$-linear map $K \to K$, the determinant of which is called the norm $N_{K|\mathbb{Q}}(\alpha)$. For an algebraic integer, the element norm coincides with the norm of the corresponding principal ideal, i. e. $N_{K|\mathbb{Q}}(a) = N(a\mathcal{O}_K)$ for all $0 \neq a \in \mathcal{O}_K$.

[1] In this context, the zero ideal is not considered as a prime ideal. So in fact, P_K is the set of maximal ideals in $\mathcal{O}_K$.

If ν denotes the degree of the extension $K \mid \mathbb{Q}$, K possesses ν distinct embeddings into $\mathbb{C}$. These split into r real embeddings $\sigma_1, \ldots, \sigma_r$ and t pairs of (proper) complex embeddings $\tau_1, \overline{\tau_1}, \ldots, \tau_t, \overline{\tau_t}$, where $\nu = r + 2t$. These embeddings give rise to $r + t$ archimedian valuations on K via $|\alpha|_i := |\sigma_i(\alpha)|$ for $i \in \{1, \ldots, r\}$ and $|\alpha|_{r+i} := |\tau_i(\alpha)|^2$ for $i \in \{1, \ldots, t\}$.

While the unit group $\mathcal{O}_K^\times$ is the kernel of the transition

$$\begin{aligned} K^\times &\to I_K \\ \alpha &\mapsto \alpha\mathcal{O}_K \end{aligned}$$

from non-zero field elements to fractional ideals, the class group $\mathrm{Cl}_K := I_K/H_K$ is defined as its cokernel, where

$$H_K := \{\alpha\mathcal{O}_K \mid \alpha \in K^\times\} \leq I_K$$

is the subgroup of principal fractional ideals. Then we have the exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \to I_K \to \mathrm{Cl}_K \to 1\ .$$

Therefore, the determination of $\mathcal{O}_K^\times$ and Cl_K are of special interest.

One of the main results in classical algebraic number theory is that the class group Cl_K is always finite. Its cardinality $h_K := |\mathrm{Cl}_K|$ is called the *class number* of K. One could say that h_K measures the "failure" of $\mathcal{O}_K$ being a principal ideal domain. In particular, $h_K = 1$ is equivalent to $\mathcal{O}_K$ being a principal ideal domain.

Another main result is the Dirichlet unit theorem, which states that the unit group $\mathcal{O}_K^\times$ has finite rank, namely $r + t - 1$. The torsion part of $\mathcal{O}_K^\times$ consists exactly of the roots of unity inside K and is therefore finite cyclic. In other words, there exist so called *fundamental units* $\varepsilon_1, \ldots, \varepsilon_{r+t} \in \mathcal{O}_K^\times$ such that

$$\mathcal{O}_K^\times = \varepsilon_1^{\mathbb{Z}/w_K\mathbb{Z}} \times \varepsilon_2^{\mathbb{Z}} \times \cdots \times \varepsilon_{r+t}^{\mathbb{Z}}$$

where ε_1 is a primitive w_K-th root of unity. This means that every unit $\varepsilon \in \mathcal{O}_K^\times$ has a unique representation $\varepsilon = \varepsilon_1^{f_1} \cdots \varepsilon_{r+t}^{f_{r+t}}$ with $f_1, \ldots, f_{r+t} \in \mathbb{Z}$ and $0 \leq f_1 < w_K$. It turns out that the determination of ε_1 and w_K is rather straightforward. On the other hand, the efficient computation of the fundamental units $\varepsilon_2, \ldots, \varepsilon_{r+t}$ requires a lot harder work and is still subject to current research. In Section 2.1, a brief overview will be given on how to attempt this problem, together with an approach for the computation of Cl_K.

Associated to K is its Dedekind zeta function

$$\zeta_K(s) := \sum_{0 \neq \mathfrak{a} \lhd \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p} \in P_K} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

that generalizes the Riemann zeta function obtained for $K = \mathbb{Q}$. It can be shown [Neu92] that the defining series of $\zeta_K(s)$ converges absolutely and uniformely on $\mathrm{Re}(s) \geq 1 + \delta$

for all $\delta > 0$, and that ζ_K has an analytic continuation on $\mathbb{C} \setminus \{1\}$. By the analytic class number formula, the residuum of $\zeta_K(s)$ at $s = 1$ equals

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r+t}\pi^t h_K R_K}{w_K |d_K|^{1/2}} \ ,$$

where R_K is the regulator of K and d_K is its discriminant. This is a surprising and beautiful connection between analytic properties of the holomorphic function ζ_K and algebraic invariants of the number field K.

Because the constants w_K and d_K can be computed rather easily, the analytic class number formula discloses information about the product $h_K R_K$. While the class number h_K is strongly related to the class group Cl_K, the regulator R_K is connected to the unit group $\mathcal{O}_K^\times$. Hence, the knowledge of $h_K R_K$ comes in handy when computing Cl_K and $\mathcal{O}_K^\times$ simultaneously.

Given a finite set $S \subset P_K$ of prime ideals in $\mathcal{O}_K$, we can generalize integers and units to S-integers and S-units in the following way:

$$\mathcal{O}_{K,S} := \{\alpha \in K \mid v_\mathfrak{p}(\alpha) \geq 0, \ \mathfrak{p} \in P_K \setminus S\}$$
$$\mathcal{O}_{K,S}^\times := \{\alpha \in K \mid v_\mathfrak{p}(\alpha) = 0, \ \mathfrak{p} \in P_K \setminus S\}$$

Then $\mathcal{O}_{K,S}$ is the localization of $\mathcal{O}_K$ by a suitable multiplicative set, as we will see later in Section 2.2.

The (S,T)-units $\mathcal{O}_{K,S,T}^\times$ are a subgroup of $\mathcal{O}_{K,S}^\times$ depending on a further finite set $T \subset P_K$ of prime ideals which is disjoint from S. They play an important role in the Rubin Stark conjecture [Rub96] that was formulated by Karl Rubin in 1996. The precise definition of $\mathcal{O}_{K,S,T}^\times$ will be given in Section 3.1. As far as the author knows, the computation of (S,T)-units is not yet available in computational algebra systems like Magma or Pari. Therefore, this thesis aims to develop and implement an algorithm for the calculation of $\mathcal{O}_{K,S,T}^\times$, which will be done in the Sections 3.2 and 3.3.

2 From units to S-units

In this chapter, we will first recall a known algorithm for combined computation of the unit and class group. After that we will introduce S-units and describe how to find them. We will also elaborate on the S-class group.

2.1 Unit and class group computation

The algorithmic computation of the unit group $\mathcal{O}_K^\times$ and the class group Cl_K are two of the most challenging tasks in computational number theory. In this section, we describe an algorithm presented in the book of Henri Cohen [Coh96, Section 6.5] that computes $\mathcal{O}_K^\times$ and Cl_K simultaneously. It generalizes an idea of Johannes Buchmann regarding real quadratic fields.

The basic idea when computing the class group Cl_K is that every ideal $\mathfrak{a} \lhd \mathcal{O}_K$ contains an element $a \in \mathfrak{a}$ such that $N_{K|\mathbb{Q}}(a) \leq M \cdot N(\mathfrak{a})$, where

$$M := \frac{\nu!}{\nu^\nu} \left(\frac{4}{\pi}\right)^t \sqrt{|d_K|}$$

denotes the Minkowski bound [PZ85]. It follows that every ideal class in Cl_K can be represented by an ideal $\mathfrak{a} \lhd \mathcal{O}_K$ with $N(\mathfrak{a}) \leq M$. Because any prime ideal dividing $\mathfrak{a}$ must also have norm at most M, Cl_K is generated by the classes of all prime ideals $\mathfrak{p} \in P_K$ with $N(\mathfrak{p}) \leq M$. Since they divide prime numbers $p \leq M$, there are only finitely many $\mathfrak{p}$ with this property, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. This list of prime ideals can be generated efficiently.

Now we are endowed with a surjective homomorphism

$$\begin{aligned} \mathbb{Z}^k &\to \mathrm{Cl}_K \\ (e_1, \ldots, e_k) &\mapsto [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}] \,. \end{aligned}$$

We have solved the problem of computing Cl_K if we are able to determine the kernel Λ of this map, giving rise to the exact sequence

$$0 \to \Lambda \to \mathbb{Z}^k \to \mathrm{Cl}_K \to 0 \,.$$

Then we would get $\mathrm{Cl}_K \cong \mathbb{Z}^k/\Lambda$ and could use standard algorithms for computing quotients of abelian groups to obtain integers $h_1, \ldots, h_d \geq 2$ such that $\mathrm{Cl}_K \cong \bigoplus_{j=1}^d \mathbb{Z}/h_j\mathbb{Z}$.

For every $\alpha \in K^\times$ that factors over $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ into $\alpha\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ we obtain the relation $[\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_k]^{e_k} = [\mathcal{O}_K]$ inside Cl_K, so $(e_1, \ldots, e_k) \in \Lambda$. The idea is to collect as many such relations as possible and to store the integer vectors $(e_1, \ldots, e_k)$ as columns of a so called *relation matrix* Y consisting of k rows. The image of Y is guaranteed to be a subgroup of Λ and we need to add more and more relations until $\operatorname{Im} Y$ equals Λ.

The reader may ask how the preceeding thoughts are useful for the computation of fundamental units. To this end, note that for every integral combination of the columns of Y that results in the zero vector, the product of the corresponding field elements from whom the relations originated constitutes a unit of $\mathcal{O}_K$, because its valuation at all primes is identically zero. Therefore, the kernel of Y always corresponds to a subgroup of $\mathcal{O}_K^\times$ and we need to add more and more relations until $\operatorname{Ker} Y$ equals $\mathcal{O}_K^\times$.

To summarize, the kernel of the relation matrix Y is an approximation of $\mathcal{O}_K^\times$, while the cokernel of Y is an approximation of Cl_K. As an indicator of how accurate these approximations are, we can consider the "preliminary" regulator $\tilde{R}_K$ which is simply the regulator of the subgroup of $\mathcal{O}_K^\times$ corresponding to $\operatorname{Ker} Y$, together with the "preliminary" class number $\tilde{h}_k$ which is the index of $\operatorname{Im} Y$ inside $\mathbb{Z}^k$. Then it holds $\tilde{h}_K \geq h_K$ and $\tilde{R}_K \geq R_K$.

Of course, we do not yet know the actual values of h_K and R_K. But we can get a good approximation of their product by using the analytic class number formula mentioned in the introduction. We are able to approach $h_K R_K$ in terms of the Euler product

$$h_K R_K = \frac{w_K |d_K|^{1/2}}{2^{r+t}\pi^t} \prod_{p \text{ prime}} \frac{1 - 1/p}{\prod_{\mathfrak{p}|p}(1 - 1/N(\mathfrak{p}))}$$

by cutting off the outer product over all prime numbers at a reasonable bound. Therefore, the analytic class number formula serves as a stop criterion for our method of repeatedly appending new relations to Y.

We have left open the question of how to collect more and more relations, i. e. how to find elements which factor over $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. In fact, there are many possibilities to accomplish this. For example, we could search for elements with a small norm that factors over $N(\mathfrak{p}_1), \ldots, N(\mathfrak{p}_k)$. However, the main tool used by Cohen is different from that: Its algorithm just computes random products $\mathfrak{a} := \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$ (to be more precisely, he uses a smaller factor basis than $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ for this step) and uses advanced techniques like LLL reduction afterwards to find an $\alpha \in K^\times$ such that $\alpha^{-1}\mathfrak{a}$ is *reduced* in a certain sense, thus hoping that $\alpha^{-1}\mathfrak{a}$ factors again over $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ which would lead to a factorization of α into $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and, hence, to a relation.

The set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ is called the *factor basis*. If one assumes the generalized Riemann hypothesis holds true, the Minkowski bound M can be replaced by an even smaller value, for example by the Bach bound $12(\log |d_K|)^2$. Thus our factor basis can be taken considerably smaller. This will make the algorithm much faster, since less relations are required. We could even choose a factor basis which is "too small" on behalf of better

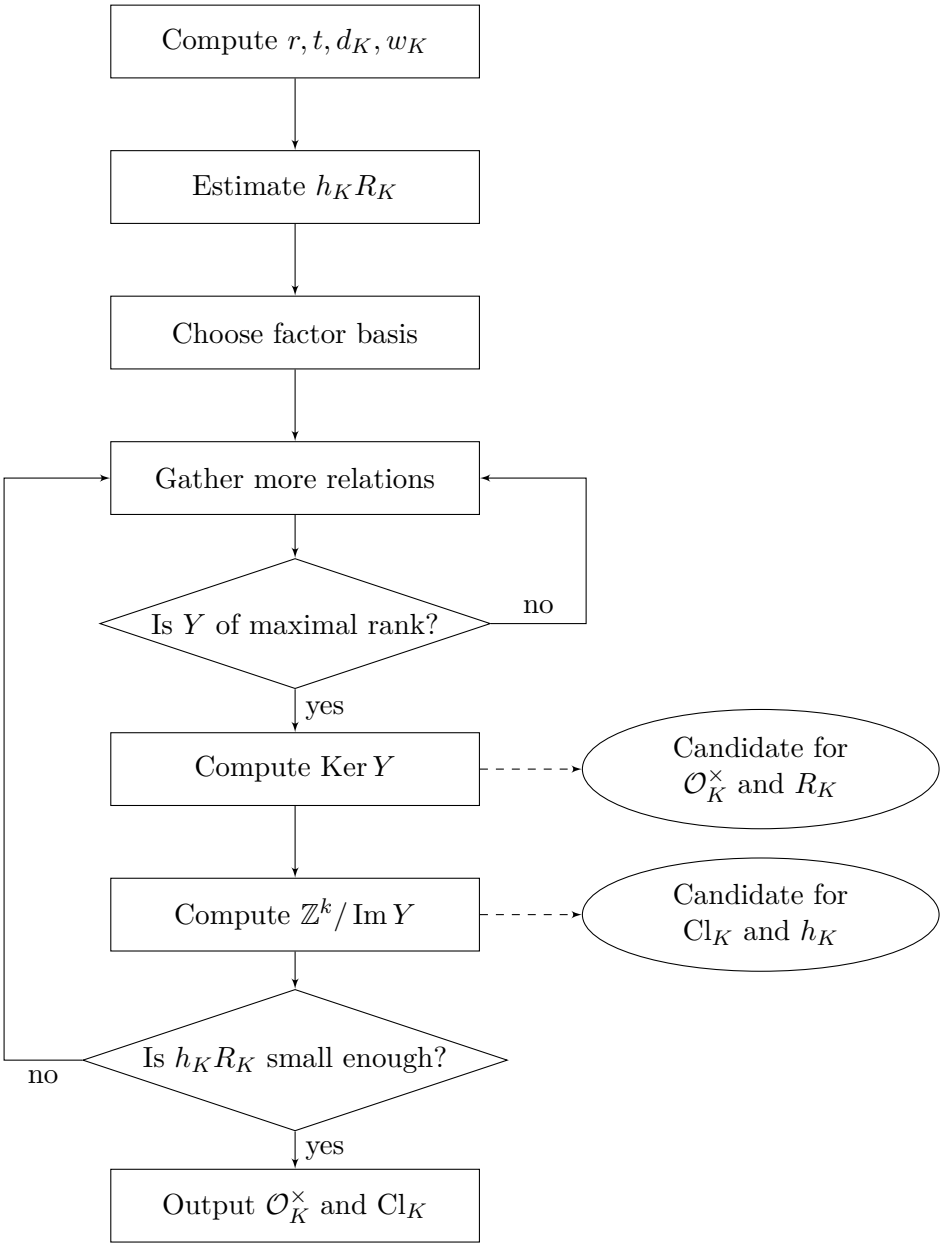

Figure 2.1: The essential steps of a combined algorithm for $\mathcal{O}_K^\times$ and Cl_K

performance, but at the risk of obtaining wrong results. On the other hand, one has to keep in mind that a too small factor basis makes the occurrence of elements which decompose over the factor basis more unlikely. We conclude that the right tuning of our factor basis size is crucial for the running time of the algorithm.

To sum up everything, our algorithm works essentially as follows (see also the flow chart shown in Figure 2.1). First we compute the constants r, t (see [Coh96, Algorithm 4.1.11]), the discriminant d_K (see [Coh96, Algorithm 6.1.8]) as well as the number w_K of roots of unity (see [Coh96, Algorithm 4.9.9]). Then we consult the analytic class number formula to get an estimation of the actual value of the product $h_K R_K$. We also choose an adequate factor basis $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Now we can start collecting relations until Y has a reasonable amount of columns. In particular, Y should have maximal rank, because we know that Cl_K is finite. By computing $\operatorname{Ker} Y$ and $\mathbb{Z}^k / \operatorname{Im} Y$, we obtain candidates for $\mathcal{O}_K^\times$ and Cl_K, respectively, and calculate the preliminary regulator and class number $\tilde{R}_K$ and $\tilde{h}_K$. After that we need to check if $\tilde{h}_K \tilde{R}_K$ is already small enough. If not, we must go back and go on collecting more relations. In case $\tilde{h}_K \tilde{R}_K$ is close to our previously computed approximation, we succeeded and can transform the candidates for $\mathcal{O}_K^\times$ and Cl_K in a canonical form to output them.

It is hard to predict the asymptotical running time of this algorithm, because the generation of new relations is highly randomized. Although Buchmann's algorithm for real quadratic fields is believed to be sub-exponential, Cohen does not claim this also holds for its generalization. In practice, however, this algorithm is very fast compared to other methods.

2.2 Definition of S-units

Before we introduce S-units, we first have to define S-integers.

Definition 2.1. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ be a finite set of prime ideals in $\mathcal{O}_K$. The *S-integers* of K are defined as

$$\mathcal{O}_{K,S} := \{\alpha \in K \mid v_\mathfrak{p}(\alpha) \geq 0,\ \mathfrak{p} \in P_K \setminus S\} .$$

Clearly, $\mathcal{O}_{K,\emptyset} = \mathcal{O}_K$.

If we compare $\mathcal{O}_{K,S}$ to $\mathcal{O}_K$, we simply discard the requirement that $v_\mathfrak{p}(\alpha) \geq 0$ for all $\mathfrak{p} \in S$. Roughly spoken, $\mathcal{O}_{K,S}$ arises from "inverting" the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Formally, $\mathcal{O}_{K,S}$ is the localization of $\mathcal{O}_K$ by an appropriate multiplicative set.

Proposition 2.2. *Let $(\mathfrak{p}_1 \cdots \mathfrak{p}_s)^{h_K} = \omega \mathcal{O}_K$ for some $\omega \in \mathcal{O}_K$. Then $\mathcal{O}_{K,S}$ is the localization of $\mathcal{O}_K$ by the multiplicative set $\{\omega^k \mid k \in \mathbb{N}_0\}$.*

Proof. Since $v_\mathfrak{p}(\omega) = 0$ for all $\mathfrak{p} \in P_K \setminus S$, it is clear that $\omega^{-k}\mathcal{O}_K \subset \mathcal{O}_{K,S}$ for all $k \in \mathbb{N}_0$. On the other hand, for any $\alpha \in \mathcal{O}_{K,S}$ we can take $k > \max\{-v_\mathfrak{p}(\alpha) \mid \mathfrak{p} \in S\}$ to obtain $v_\mathfrak{p}(\alpha\omega^k) \geq 0$ for $\mathfrak{p} \in S$ as well as for $\mathfrak{p} \in P_K \setminus S$. Therefore, we conclude $\alpha \in \omega^{-k}\mathcal{O}_K$. □

Basic localization theory tells us that $\mathcal{O}_{K,S}$ is a Dedekind domain again. Futhermore, there is a canonical bijection between prime ideals of $\mathcal{O}_K$ which do not contain ω and the prime ideals of $\mathcal{O}_{K,S}$. The former ones are precisely $P_K \setminus S$. Therefore, the group $I_{K,S}$ of $\mathcal{O}_{K,S}$-fractional ideals in K is basically the free abelian subgroup of I_K generated by $P_K \setminus S$.

Now we study the group of invertible elements in $\mathcal{O}_{K,S}$.

Definition 2.3. The units of the ring $\mathcal{O}_{K,S}$ are called the *S-units* of K and are denoted by $\mathcal{O}_{K,S}^\times$, i. e.

$$\mathcal{O}_{K,S}^\times := \{\alpha \in K \mid v_\mathfrak{p}(\alpha) = 0,\ \mathfrak{p} \in P_K \setminus S\} .$$

As a consequence, every $\alpha \in \mathcal{O}_{K,S}^\times$ admits a factorization

$$\alpha\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} .$$

Like before, $\mathcal{O}_{K,S}^\times$ differs from $\mathcal{O}_K^\times$ only by discarding the requirement $v_\mathfrak{p}(\alpha) = 0$ for all $\mathfrak{p} \in S$. If $\mathcal{O}_K$ would be a principal ideal domain, say $\mathfrak{p}_i = p_i\mathcal{O}_K$ for $i \in \{1, \ldots, s\}$, we could simply write $\mathcal{O}_{K,S}^\times = p_1^\mathbb{Z} \times \cdots \times p_s^\mathbb{Z} \times \mathcal{O}_K^\times$. But in a general setting, the map $\mathcal{O}_{K,S}^\times \to \mathbb{Z}^s, \alpha \mapsto (v_\mathfrak{p}(\alpha))_{\mathfrak{p}\in S}$ is not surjective. Hence, the determination of $\mathcal{O}_{K,S}^\times$ is a little bit harder and depends on the class group, as we will see in the next section.

2.3 Computation of S-units

We can inductively obtain a set of generators for $\mathcal{O}_{K,S}^\times$ from a set of generators for $\mathcal{O}_{K,S\setminus\{\mathfrak{p}_s\}}^\times$ by adding a single generator, provided that we know the class group Cl_K. The idea of studying the transition from $S \setminus \{\mathfrak{p}_s\}$ to S was taken from John Tate's influential book [Tat84] about the Stark conjectures.

Proposition 2.4. *There exists a $\gamma \in K^\times$ with*

$$\mathcal{O}_{K,S}^\times = \gamma^\mathbb{Z} \times \mathcal{O}_{K,S\setminus\{\mathfrak{p}_s\}}^\times .$$

Proof. Denote by $[\mathfrak{p}_i]$ the class of $\mathfrak{p}_i$ in Cl_K for all $i \in \{1, \ldots, s\}$. Let $m \in \mathbb{N}$ be minimal with $[\mathfrak{p}_s]^m \in \langle[\mathfrak{p}_1], \ldots, [\mathfrak{p}_{s-1}]\rangle$. Such an m exists because Cl_K is finite. It follows that $\mathfrak{p}_s^m = \gamma\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{s-1}^{e_{s-1}}$ for some $\gamma \in K^\times$ and $e_1, \ldots, e_{s-1} \in \mathbb{Z}$. Then

$$v_\mathfrak{p}(\gamma) = \begin{cases} -e_i & \text{if } \mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-1}\} \\ m & \text{if } \mathfrak{p} = \mathfrak{p}_s \\ 0 & \text{if } \mathfrak{p} \in P_K \setminus S . \end{cases}$$

Therefore, we have $\gamma \in \mathcal{O}_{K,S}^\times$ and $\gamma \notin \mathcal{O}_{K,S\setminus\{\mathfrak{p}_s\}}^\times$.

It remains to prove that every S-unit is a product of an $(S \setminus \{\mathfrak{p}_s\})$-unit and a power of γ. Let $\alpha \in \mathcal{O}_{K,S}^\times$. Since $v_\mathfrak{p}(\alpha) = 0$ for all $\mathfrak{p} \notin S$, $\alpha\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$ with $e_i = v_{\mathfrak{p}_i}(\alpha) \in \mathbb{Z}$ for $i \in \{1, \ldots, s\}$. It follows that $[\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_s]^{e_s}$ is trivial in Cl_K and thus $[\mathfrak{p}_s]^{e_s} \in \langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_{s-1}] \rangle$. Because m was chosen minimal, we have $e_s = k \cdot m$ for some $k \in \mathbb{Z}$. We obtain $\alpha = \gamma^k \cdot \alpha\gamma^{-k}$ with $\alpha\gamma^{-k} \in \mathcal{O}_{K,S\setminus\{\mathfrak{p}_s\}}^\times$, since $v_{\mathfrak{p}_s}(\alpha\gamma^{-k}) = e_s - k \cdot m = 0$. □

The proposition shows that a system of fundamental units for $\mathcal{O}_{K,S}^\times$ can be chosen to consist of a system of fundamental units for $\mathcal{O}_K^\times$ together with $|S|$ additional free generators. In particular, $\mathrm{Rank}(\mathcal{O}_{K,S}^\times) = |S| + \mathrm{Rank}(\mathcal{O}_K^\times) < \infty$.

The proof of Proposition 2.4 already discloses a constructive method to compute these additional generators step by step. In practice, however, more efficient algorithms are used, which are able to compute a system of fundamental units for $\mathcal{O}_{K,S}^\times$ all at once. One of them is described in [Coh00, Section 7.4.2]. Its further advantage is that the new generators are still in $\mathcal{O}_K$ and have comparatively small coefficients.

Example 2.5. Let $K = \mathbb{Q}(\sqrt{42})$ and $S = \{\mathfrak{p}\}$ with $\mathfrak{p} = (11, 3 + \sqrt{42})$. Obviously, -1 is the only non-trivial root of unity contained in $\mathcal{O}_K$ due to $K \subset \mathbb{R}$. Thus, by the Dirichlet unit theorem $\mathcal{O}_K^\times = \varepsilon_1^{\mathbb{Z}/2\mathbb{Z}} \times \varepsilon_2^\mathbb{Z}$ with $\varepsilon_1 = -1$ and some fundamental unit ε_2. It can be easily seen that $\varepsilon_2 = 13 + 2\sqrt{42}$ is a possible choice. Following the proof of Proposition 2.4, we need to find the order of $\mathfrak{p}$ in Cl_K. It turns out that $\mathfrak{p}^2$ is already principal, namely generated by $\varepsilon_3 = 17 + 2\sqrt{42}$, and we conclude $\mathcal{O}_{K,S}^\times = \varepsilon_1^{\mathbb{Z}/2\mathbb{Z}} \times \varepsilon_2^\mathbb{Z} \times \varepsilon_3^\mathbb{Z}$.

2.4 The S-class group

The S-class group defined in this section is related to S-units and will be useful when we introduce and compute the (S,T)-class group.

Definition 2.6. The *S-class group* $\mathrm{Cl}_{K,S}$ of K is defined as the class group of the Dedekind domain $\mathcal{O}_{K,S}$, i. e.

$$\mathrm{Cl}_{K,S} := \frac{I_{K,S}}{H_{K,S}}$$

where $I_{K,S}$ is the group of fractional ideals in $\mathcal{O}_{K,S}$ and $H_{K,S}$ is the subgroup of principal fractional ideals in $\mathcal{O}_{K,S}$.

The following proposition summarizes the roles of $\mathcal{O}_{K,S}^\times$ and $\mathrm{Cl}_{K,S}$ in a compact way.

Proposition 2.7. *The sequence*

$$1 \longrightarrow \mathcal{O}_K^\times \hookrightarrow \mathcal{O}_{K,S}^\times \xrightarrow{v} \mathbb{Z}^s \xrightarrow{\lambda} \mathrm{Cl}_K \xrightarrow{\kappa} \mathrm{Cl}_{K,S} \longrightarrow 1$$

is exact, where $v(\alpha) := (v_\mathfrak{p}(\alpha))_{\mathfrak{p}\in S}$, $\lambda(e_1, \ldots, e_s) := [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}]$ and κ is the homomorphism arising from $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{K,S}$ by passage to the quotient.

Proof. By definition of $\mathcal{O}_K^\times$ and $\mathcal{O}_{K,S}^\times$, it is obvious that $\mathcal{O}_K^\times = \operatorname{Ker} v$, so we have proven exactness at $\mathcal{O}_K^\times$ and $\mathcal{O}_{K,S}^\times$.

Let $(e_1, \dots, e_s) \in \operatorname{Im} v$, so there is an $\alpha \in \mathcal{O}_{K,S}^\times$ with $v_{\mathfrak{p}_i}(\alpha) = e_i$ for $i \in \{1, \dots, s\}$. Because $v_\mathfrak{p}(\alpha) = 0$ for $\mathfrak{p} \notin S$, we have $\alpha\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$. Therefore, $[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}]$ is trivial in Cl_K, which means $(e_1, \dots, e_s) \in \operatorname{Ker} \lambda$. On the other hand, if $(e_1, \dots, e_s) \in \operatorname{Ker} \lambda$, then $[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}]$ is trivial in Cl_K. Hence, there exists an $\alpha \in K^\times$ such that $\alpha\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$. But this implies $\alpha \in \mathcal{O}_{K,S}^\times$ and $v_{\mathfrak{p}_i}(\alpha) = e_i$ for $i \in \{1, \dots, s\}$. It follows that $(e_1, \dots, e_s) \in \operatorname{Im} v$.

Let $[\mathfrak{a}] \in \operatorname{Im} \lambda$, so there exists $(e_1, \dots, e_s) \in \mathbb{Z}^s$ such that $[\mathfrak{a}] = [\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}]$. Because $\mathfrak{p}\mathcal{O}_{K,S} = \mathcal{O}_{K,S}$ for all $\mathfrak{p} \in S$, $\kappa(\mathfrak{a}) = [\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_s]^{e_s}$ is trivial in $\mathrm{Cl}_{K,S}$. Conversely, assume that $[\mathfrak{a}] \in \operatorname{Ker} \kappa$. Then $\mathfrak{a}\mathcal{O}_{K,S} = \alpha\mathcal{O}_{K,S}$ for an $\alpha \in K^\times$. Hence the prime decomposition of $\alpha^{-1}\mathfrak{a}$ contains only prime ideals from S. Therefore, $[\mathfrak{a}] = [\alpha^{-1}\mathfrak{a}] \in \operatorname{Im} \lambda$.

Finally, we prove the surjectivity of κ. Note that $I_{K,S}$ is generated by the prime ideals in $\mathcal{O}_{K,S}$. In Section 2.2, we mentioned the natural correspondence between $P_K \setminus S$ and the prime ideals in $\mathcal{O}_{K,S}$, which means that every prime ideal in $\mathcal{O}_{K,S}$ is of the form $\mathfrak{p}\mathcal{O}_{K,S}$ for some $\mathfrak{p} \in P_K \setminus S$. It follows that the ideal classes $\kappa([\mathfrak{p}])$ where $\mathfrak{p} \in P_K \setminus S$ generate the whole class group $\mathrm{Cl}_{K,S}$. □

As an immediate consequence of Proposition 2.7 we get

$$\mathrm{Cl}_{K,S} \cong \mathrm{Cl}_K / \langle [\mathfrak{p}_1], \dots, [\mathfrak{p}_s] \rangle \ .$$

In particular, $\mathrm{Cl}_{K,S}$ is again finite and can be constructed easily from Cl_K. Its cardinality $h_{K,S} := |\mathrm{Cl}_{K,S}|$ is called the S-class number.

3 From S-units to (S,T)-units

In this chapter, we will introduce (S,T)-units. We will present an algorithm for computing them, which is the main goal of this thesis. After that we will enlarge on the related (S,T)-class group. By computing the (S,T)-class group we are able to verify the index of the (S,T)-unit group.

3.1 Idea and Definition

In 1996, Karl Rubin [Rub96] published an extension of the Stark conjectures where he studies Artin L-functions with higher order zeros at $s = 0$, arising from an additional set of prime ideals T. This set T results in a broad range of generalizations: From the S-unit group $\mathcal{O}_{K,S}^\times$ towards the (S,T)-unit group $\mathcal{O}_{K,S,T}^\times$, from the S-class group $\mathrm{Cl}_{K,S}$ towards the (S,T)-class group $\mathrm{Cl}_{K,S,T}$, from the S-zeta function $\zeta_{K,S}$ towards the (S,T)-zeta function $\zeta_{K,S,T}$, from the S-class number formula towards the (S,T)-class number formula, and so on. In the following sections, we focus solely on $\mathcal{O}_{K,S,T}^\times$ and $\mathrm{Cl}_{K,S,T}$ and discuss them independently of their relation to the Rubin Stark conjecture.

While the adoption of S-units "removes" certain prime ideals, thus enlarging $\mathcal{O}_K^\times$ to $\mathcal{O}_{K,S}^\times$, the idea behind the additional set T is to "add" certain prime ideals (although they are already there), thus making $\mathcal{O}_{K,S}^\times$ smaller again into $\mathcal{O}_{K,S,T}^\times$. In Section 3.4, we will see that an analogous picture happens to occur on the class groups Cl_K, $\mathrm{Cl}_{K,S}$ and $\mathrm{Cl}_{K,S,T}$.

Contrary to S-units, the (S,T)-units are *not* a unit group of a particular Dedekind domain. Instead they are defined directly as a subgroup of the S-units.

Definition 3.1. Let S and T be finite sets of prime ideals in $\mathcal{O}_K$ with $S \cap T = \emptyset$. The (S,T)-*units* of K are defined as

$$\mathcal{O}_{K,S,T}^\times := \{\alpha \in \mathcal{O}_{K,S}^\times \mid \alpha \equiv 1 \pmod{\mathfrak{q}},\ \mathfrak{q} \in T\}\ .$$

Clearly, $\mathcal{O}_{K,S,\emptyset}^\times = \mathcal{O}_{K,S}^\times$.

Let $\mathfrak{T}$ be the product of the prime ideals in T. Using the Chinese remainder theorem, the above definition can be equivalently rewritten into a single condition:

$$\mathcal{O}_{K,S,T}^\times = \{\alpha \in \mathcal{O}_{K,S}^\times \mid \alpha \equiv 1 \pmod{\mathfrak{T}}\}\ .$$

However, the actual definition turns out to be quite as useful.

3.2 Computation of (S,T)-units

Let $T = \{\mathfrak{q}_1, \dots, \mathfrak{q}_m\}$. By definition, $\mathcal{O}_{K,S,T}^\times$ is the kernel of the map

$$\pi\colon \mathcal{O}_{K,S}^\times \to \prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times$$

where each $\alpha \in \mathcal{O}_{K,S}^\times$ is sent to its projections in $(\mathcal{O}_K/\mathfrak{q})^\times$ for all $\mathfrak{q} \in T$. This is well-defined, because $S \cap T = \emptyset$ implies that $v_\mathfrak{q}(\alpha) = 0$ for all $\mathfrak{q} \in T$.

In Section 2.3, we have seen that

$$\mathcal{O}_{K,S}^\times = \varepsilon_1^{\mathbb{Z}/w_K\mathbb{Z}} \times \varepsilon_2^\mathbb{Z} \times \cdots \times \varepsilon_n^\mathbb{Z}$$

for certain $\varepsilon_1, \dots, \varepsilon_n \in \mathcal{O}_{K,S}^\times$, where $n = r + t + s$. In other words,

$$\begin{aligned} \phi\colon \mathbb{Z}/w_K\mathbb{Z} \oplus \mathbb{Z}^{n-1} &\to \mathcal{O}_{K,S}^\times \\ (x_1, \dots, x_n) &\mapsto \varepsilon_1^{x_1} \cdots \varepsilon_n^{x_n} \end{aligned}$$

is an isomorphism between the additive group $\mathbb{Z}/w_K\mathbb{Z} \oplus \mathbb{Z}^{n-1}$ and the multiplicative group $\mathcal{O}_{K,S}^\times$.

Because $\mathcal{O}_K/\mathfrak{q}_i$ is always a finite field, $(\mathcal{O}_K/\mathfrak{q}_i)^\times$ is a cyclic group of order $c_i := N(\mathfrak{q}_i) - 1$ generated by some $g_i \in (\mathcal{O}_K/\mathfrak{q}_i)^\times$. This implies that

$$\begin{aligned} \psi\colon \bigoplus_{i=1}^m \mathbb{Z}/c_i\mathbb{Z} &\to \prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times \\ (a_1, \dots, a_m) &\mapsto (g_1^{a_1}, \dots, g_m^{a_m}) \end{aligned}$$

is an isomorphism between the additive group $\bigoplus_{i=1}^m \mathbb{Z}/c_i\mathbb{Z}$ and the multiplicative group $\prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times$.

Therefore, the problem of computing $\mathcal{O}_{K,S,T}^\times$ reduces to computing the kernel of the homomorphism

$$A\colon \mathbb{Z}/w_K\mathbb{Z} \oplus \mathbb{Z}^{n-1} \to \bigoplus_{i=1}^m \mathbb{Z}/c_i\mathbb{Z}$$

defined as $A := \psi^{-1} \circ \pi \circ \phi$, as shown in the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathcal{O}_{K,S,T}^\times & \hookrightarrow & \mathcal{O}_{K,S}^\times & \xrightarrow{\pi} & \prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times \\ & & \uparrow{\scriptstyle \phi|_{\operatorname{Ker} A}}\,{\scriptstyle \cong} & & \uparrow{\scriptstyle \phi}\,{\scriptstyle \cong} & & \uparrow{\scriptstyle \psi}\,{\scriptstyle \cong} \\ 0 & \longrightarrow & \operatorname{Ker} A & \hookrightarrow & \mathbb{Z}/w_K\mathbb{Z} \oplus \mathbb{Z}^{n-1} & \xrightarrow{A} & \bigoplus_{i=1}^m \mathbb{Z}/c_i\mathbb{Z} \end{array}$$

In particular, we get $(\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S,T}^\times) = |\operatorname{Im} A| \leq \prod_{i=1}^m c_i < \infty$ and thus $\operatorname{Rank} \mathcal{O}_{K,S,T}^\times = \operatorname{Rank} \mathcal{O}_{K,S}^\times$.

More explicitly, one has to solve the system of linear congruences

$$a_{i1}x_1 + \cdots + a_{in}x_n \equiv 0 \pmod{c_i}\,, \quad i = 1, \ldots, m$$

in integers $x_1, \ldots, x_n$ (to be more precisely, we have $x_1 \in \mathbb{Z}/w_K\mathbb{Z}$), where the coefficient a_{ij} is given by the i-th component of $\psi^{-1}(\pi(\varepsilon_j))$, which is the discrete logarithm of ε_j in $(\mathcal{O}_K/\mathfrak{q}_i)^\times$. This system of linear congruences is equivalent to the system of linear equations

$$a_{i1}x_1 + \cdots + a_{in}x_n + c_i y_i = 0\,, \quad i = 1, \ldots, m$$

over $\mathbb{Z}$ in $n+m$ variables $x_1, \ldots, x_n, y_1, \ldots, y_m$. Hence, it remains to find a $\mathbb{Z}$-basis for the kernel space of the matrix

$$M := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & c_1 & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} & 0 & c_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{n2} & \cdots & a_{mn} & 0 & 0 & \cdots & c_m \end{pmatrix} \in \mathbb{Z}^{m\times(n+m)}\,,$$

for which efficient algorithms are known.

Therefore, we have developed the following algorithm for the (S,T)-unit group.

Algorithm 3.2 (Computation of (S,T)-units)**.** Let $T = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$.

1. [Compute S-units.] Use the algorithm from Section 2.3 to compute fundamental units $\varepsilon_1, \ldots, \varepsilon_n$ of $\mathcal{O}_{K,S}^\times$.
2. [Take discrete logarithms.] For $i = 1, \ldots, m$ and $j = 1, \ldots, n$ set a_{ij} to be the discrete logarithm of ε_j in the residue class field $\mathcal{O}_K/\mathfrak{q}_i$.
3. [Solve linear equations.] Construct a $\mathbb{Z}$-basis of the kernel space of the matrix M defined as above where $c_i := N(\mathfrak{q}_i) - 1$.
4. [Terminate.] For every kernel vector $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ from step 3, output the fundamental unit $\phi(x_1, \ldots, x_n) = \varepsilon_1^{x_1} \cdots \varepsilon_n^{x_n}$ of $\mathcal{O}_{K,S,T}^\times$.

The running time of this algorithm is dominated by the first step where the S-units are computed. Therefore, the computational complexity of finding fundamental (S,T)-units is not bigger than the one of finding fundamental S-units, which in turn is substantially ruled by the unit group computation.

We demonstrate the operation of Algorithm 3.2 on a small example.

Example 3.3. Let $K = \mathbb{Q}(\sqrt{42})$, $S = \{\mathfrak{p}\}$, $T = \{\mathfrak{q}_1, \mathfrak{q}_2\}$ with $\mathfrak{p} = (11, 3 + \sqrt{42})$ (one of the two prime ideals lying above 11 in $\mathcal{O}_K$), $\mathfrak{q}_1 = (5)$ (the unique principal prime ideal lying above 5 in $\mathcal{O}_K$) and $\mathfrak{q}_2 = (7, \sqrt{42})$ (the unique prime ideal lying above 7 in $\mathcal{O}_K$).

1. [Compute S-units.] Example 2.5 resulted in $\mathcal{O}_{K,S}^\times = \varepsilon_1^{\mathbb{Z}/2\mathbb{Z}} \times \varepsilon_2^{\mathbb{Z}} \times \varepsilon_3^{\mathbb{Z}}$ with $\varepsilon_1 = -1$, $\varepsilon_2 = 13 + 2\sqrt{42}$ and $\varepsilon_3 = 17 + 2\sqrt{42}$.

2. [Take discrete logarithms.] The residue class fields are $\mathcal{O}_K/\mathfrak{q}_1 \cong \mathbb{F}_{25} \cong \mathbb{F}_5(\sqrt{2})$ and $\mathcal{O}_K/\mathfrak{q}_2 \cong \mathbb{F}_7$. We choose the generators $g_1 = 3 + \sqrt{2}$ of $\mathbb{F}_5(\sqrt{2})$ and $g_2 = 3$ of $\mathbb{F}_7$ and calculate

$$\begin{aligned} \mathcal{O}_{K,S}^\times &\xrightarrow{\pi} \mathbb{F}_5(\sqrt{2}) \times \mathbb{F}_7 \xrightarrow{\psi^{-1}} \mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \\ \varepsilon_1 &\mapsto (4,6) \mapsto (12,3) \\ \varepsilon_2 &\mapsto (3 + 2\sqrt{2}, 6) \mapsto (4,3) \\ \varepsilon_3 &\mapsto (2 + 2\sqrt{2}, 3) \mapsto (8,1)\ . \end{aligned}$$

3. [Solve linear equations.] To solve the system of linear congruences

$$\begin{aligned} 12x_1 + 4x_2 + 8x_3 &\equiv 0 \pmod{24} \\ 3x_1 + 3x_2 + x_3 &\equiv 0 \pmod{6}\ , \end{aligned}$$

we determine the kernel of the matrix

$$M = \begin{pmatrix} 12 & 4 & 8 & 24 & 0 \\ 3 & 3 & 1 & 0 & 6 \end{pmatrix} \in \mathbb{Z}^{2\times 5}$$

to be

$$\left\langle \begin{pmatrix} 2 \\ 0 \\ 0 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 3 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 6 \\ -2 \\ -1 \end{pmatrix} \right\rangle .$$

4. [Terminate.] Applying ϕ yields $\varepsilon_1^2 = 1$, $\varepsilon_1^{-1}\varepsilon_2^3 = -8749 - 1350\sqrt{42}$ and $\varepsilon_3^6 = 361703161 + 55811340\sqrt{42}$. We can see that the $\mathbb{Z}/2\mathbb{Z}$-torsion was eliminated and $\mathcal{O}_{K,S,T}^\times$ contains no non-trivial roots of unity. This yields the two fundamental units $-\varepsilon_2^3$ and ε_3^6.

Many additional examples can be found in Chapter 4.

3.3 Implementation within Magma

The computational algebra system Magma was chosen to implement Algorithm 3.2. It already provides the routine SUnitGroup to compute the group of S-units. Because abelian groups are represented in Magma as quotients of $\mathbb{Z}^n$, SUnitGroup additionally returns the isomorphism ϕ defined in the previous section viewed as an injection into K,

i. e. the system of fundamental units for $\mathcal{O}_{K,S}^{\times}$ is given by the images under ϕ of the n canonical generators of $\mathbb{Z}/w_K\mathbb{Z} \oplus \mathbb{Z}^{n-1}$.

For convenience, the newly implemented routine STUnitGroup returns apart from the (S,T)-unit group also the S-unit group together with its map into the field. Because the computed (S,T)-unit group is represented in Magma as a subgroup of the S-unit group, this map into K can be applied to elements of the (S,T)-unit group as well.

```
1  intrinsic STUnitGroup(S :: [ RngOrdIdl ], T :: [ RngOrdIdl ]) -> GrpAb, GrpAb, Map
2  {Compute (S,T)-units.}
3          require not (IsEmpty(S) and IsEmpty(T)):
4                  "At least S or T must be non-empty.";
5          require  IsDisjoint (SequenceToSet(S), SequenceToSet(T)):
6                  "S and T must be disjoint.";
7          if  IsEmpty(S) then
8                  O := Order(T[1]);
9                  U, mU := UnitGroup(O);
10         else
11                 U, mU := SUnitGroup(S);
12         end if;
13         m := #T;
14         n := NumberOfGenerators(U);
15         M := ZeroMatrix(IntegerRing(), m, n + m);
16         for  i  := 1 to m do
17                 F, mF := ResidueClassField(T[i ]);
18                 for  j  := 1 to n do
19                         x := mU(U.j);
20                         r := mF(x);
21                         M[i, j] := Log(r);
22                 end for;
23                 M[i, n + i] := #F - 1;
24         end for;
25         K := KernelMatrix(Transpose(M));
26         L := RowSequence(ColumnSubmatrix(K, n));
27         V := sub<U | L>;
28         return V, U, mU;
29 end intrinsic ;
```

Example 3.4. We demonstrate how to do Example 3.3 in Magma. First we need to attach the file where STUnitGroup is implemented.

```
> Attach("STUnitGroup.m");
```

Then we create $K = \mathbb{Q}(\sqrt{42})$ and $\mathcal{O}_K$, as well as the three prime ideals $\mathfrak{p}$, $\mathfrak{q}_1$ and $\mathfrak{q}_2$.

```
> K := QuadraticField(42);
> O := MaximalOrder(K);
> p := Decomposition(O, 11)[1][1];
> q1 := Decomposition(O, 5)[1][1];
> q2 := Decomposition(O, 7)[1][1];
> p;
Prime Ideal of O
Two element generators:
    11
    $.2 + 3
```

Now we are ready to call STUnitGroup and view the results.

```
> V, U, mU := STUnitGroup([p], [q1, q2]);
> U;
Abelian Group isomorphic to Z/2 + Z + Z
Defined on 3 generators
Relations:
    2*U.1 = 0
> V;
Abelian Group isomorphic to Z + Z
Defined on 2 generators in supergroup U:
    V.1 = 3*U.2
    V.2 = 6*U.3 (free)
```

We can use the returned map to explicitly obtain the fundamental (S,T)-units.

```
> mU(V.1), mU(V.2);
-8749/1*O.1 - 1350/1*O.2
361703161/1*O.1 + 55811340/1*O.2
```

Finally, we are interested in the index $(\mathcal{O}_{K,S}^{\times} : \mathcal{O}_{K,S,T}^{\times})$.

```
> Index(U, V);
36
```

3.4 The (S,T)-class group

The (S,T)-class group can be understood as kind of a ray class, as the following definition suggests.

Definition 3.5. The (S,T)-*class group* of K is defined as

$$\mathrm{Cl}_{K,S,T} := \frac{I_{K,S,T}}{H_{K,S,T}}$$

where

$$I_{K,S,T} := \{\mathfrak{a} \in I_{K,S} \mid (\mathfrak{a},\mathfrak{q}) = 1,\ \mathfrak{q} \in T\}$$

is the group of fractional ideals in $\mathcal{O}_{K,S}$ coprime to all prime ideals in T and

$$H_{K,S,T} := \{\alpha\mathcal{O}_{K,S} \mid \alpha \in K^\times,\ \alpha \equiv 1 \pmod{\mathfrak{q}},\ \mathfrak{q} \in T\} \leq I_{K,S,T}$$

is the subgroup of principal fractional ideals in $\mathcal{O}_{K,S}$ that have a generator which is trivial in $(\mathcal{O}_K/\mathfrak{q})^\times$ for all $\mathfrak{q} \in T$.

Now we want to define a homomorphism $f\colon \prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times \to \mathrm{Cl}_{K,S,T}$. By the Chinese remainder theorem, every tuple $(r_1,\dots,r_m) \in \prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times$ has a common representative $\alpha \in K^\times$ satisfying $\alpha \equiv r_i \pmod{\mathfrak{q}_i}$ for every $i \in \{1,\dots,m\}$. In particular, $(\alpha\mathcal{O}_{K,S},\mathfrak{q}) = 0$ for all $\mathfrak{q} \in T$. Let $f(r_1,\dots,r_m) := [\alpha\mathcal{O}_{K,S}]$. This is well-defined, because for any other representative $\alpha' \in K^\times$ it holds $\frac{\alpha}{\alpha'} \equiv 1 \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in T$ and thus $[\alpha\mathcal{O}_{K,S}] = [\alpha'\mathcal{O}_{K,S}]$ in $\mathrm{Cl}_{K,S,T}$.

Proposition 3.6. *The sequence*

$$1 \longrightarrow \mathcal{O}_{K,S,T}^\times \hookrightarrow \mathcal{O}_{K,S}^\times \xrightarrow{\pi} \prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times \xrightarrow{f} \mathrm{Cl}_{K,S,T} \xrightarrow{\rho} \mathrm{Cl}_{K,S} \longrightarrow 1$$

is exact, where f is like above and ρ denotes the canonical homomorphism induced by $I_{K,S,T} \leq I_{K,S}$ and $H_{K,S,T} \leq H_{K,S}$.

Proof. Because $\mathcal{O}_{K,S,T}^\times$ is defined as $\operatorname{Ker}\pi$, it is clear that the sequence is exact at $\mathcal{O}_{K,S,T}^\times$ and $\mathcal{O}_{K,S}^\times$.

We show that $\operatorname{Im}\pi = \operatorname{Ker} f$. Let $(r_1,\dots,r_m) \in \prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times$ with a common representative $\alpha \in K^\times$. Then $(r_1,\dots,r_m) \in \operatorname{Ker} f$ is equivalent to $\alpha\mathcal{O}_{K,S} = \alpha'\mathcal{O}_{K,S}$ for some $\alpha' \in K^\times$ with $\alpha' \equiv 1 \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in T$. This implies that we have $\beta := \frac{\alpha}{\alpha'} \in \mathcal{O}_{K,S}^\times$. Since $r_i \equiv \alpha \equiv \alpha'\beta \equiv \beta \pmod{\mathfrak{q}_i}$, it holds $\pi(\beta) = (r_1,\dots,r_m)$. On the other hand, every $\pi(\beta) \in \operatorname{Im}\pi$ can be represented by $\beta \in \mathcal{O}_{K,S}^\times$ and thus $f(\pi(\beta)) = [\beta\mathcal{O}_{K,S}] = [\mathcal{O}_{K,S}]$ is trivial in $\mathrm{Cl}_{K,S,T}$.

Because $\operatorname{Im} f$ contains only principal ideals, $\operatorname{Im} f \subset \operatorname{Ker}\rho$ is immediate. Now take $[\alpha\mathcal{O}_{K,S}] \in \operatorname{Ker}\rho$. Since $\alpha\mathcal{O}_{K,S} \in I_{K,S,T}$, α projects to an element in $\prod_{i=1}^m (\mathcal{O}_K/\mathfrak{q}_i)^\times$ and $\operatorname{Ker}\rho \subset \operatorname{Im} f$ follows.

Finally, we prove that ρ is surjective, i. e. for every $\mathfrak{a} \in I_{K,S}$ there exists an $\alpha \in K^\times$ such that $\alpha\mathfrak{a} \in I_{K,S,T}$. By the Chinese remainder theorem, we can choose $\alpha \in K^\times$ such that $v_\mathfrak{q}(\alpha) = -v_\mathfrak{q}(\mathfrak{a})$ for all $\mathfrak{q} \in T$. Therefore the prime decomposition of $\alpha\mathfrak{a}$ contains no prime ideals from T and we are done. □

3.5 Computation of the (S,T)-class group

Proposition 3.6 allows us to compute $\mathrm{Cl}_{K,S,T}$, provided that the other parts of the exact sequence are known. We will now give an explicit construction of $\mathrm{Cl}_{K,S,T}$. For simplicity, write $h := h_{K,S}$ and $\Omega := \prod_{i=1}^{m}(\mathcal{O}_K/\mathfrak{q}_i)^\times$.

Proposition 3.7. *Let $\mathfrak{a}_1,\dots,\mathfrak{a}_h$ be a system of representatives for $\mathrm{Cl}_{K,S}$. By multiplication with suitable principal fractional ideals we can assume that $\mathfrak{a}_1,\dots,\mathfrak{a}_h \in I_{K,S,T}$. Let $\alpha_1,\dots,\alpha_\ell \in K^\times$ be such that their projections onto Ω form a system of representatives for the cokernel $\Omega/\operatorname{Im}\pi$. Then $\alpha_i\mathfrak{a}_j$ is a system of representatives for $\mathrm{Cl}_{K,S,T}$, where $(i,j) \in \{1,\dots,\ell\}\times\{1,\dots,h\}$.*

Proof. Let $\mathfrak{a} \in I_{K,S,T}$ be arbitrary. We show that $\mathfrak{a}$ is modulo $H_{K,S,T}$ congruent to one of the $\alpha_i\mathfrak{a}_j$. First of all, because $\mathfrak{a}_1,\dots,\mathfrak{a}_h$ represent $\mathrm{Cl}_{K,S}$, there exists a $j \in \{1,\dots,h\}$ and an $\alpha \in K^\times$ such that $\mathfrak{a} = \alpha\mathfrak{a}_j$. Now we use that the projections of $\alpha_1,\dots,\alpha_\ell$ represent $\Omega/\operatorname{Im}\pi$ to obtain an $i \in \{1,\dots,\ell\}$ and a $\beta \in \mathcal{O}_{K,S}^\times$ such that $\alpha\beta \equiv \alpha_i \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in T$. This implies $\mathfrak{a} = \frac{\alpha}{\alpha_i}\alpha_i\mathfrak{a}_j$, where $\frac{\alpha}{\alpha_i}\mathcal{O}_{K,S} = \frac{\alpha\beta}{\alpha_i}\mathcal{O}_{K,S} \in H_{K,S,T}$ due to $\frac{\alpha\beta}{\alpha_i} \equiv 1 \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in T$.

It remains to show that the $\alpha_i\mathfrak{a}_j$ are pairwise distinct modulo $H_{K,S,T}$. Suppose that $\alpha_i\mathfrak{a}_j \equiv \alpha_{i'}\mathfrak{a}_{j'} \pmod{H_{K,S,T}}$ for $(i,j) \neq (i',j')$. Then $\alpha_i\mathfrak{a}_j = \beta\alpha_{i'}\mathfrak{a}_{j'}$ with $\beta \equiv 1 \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in T$. In particular, $[\mathfrak{a}_j] = [\mathfrak{a}_{j'}]$ in $\mathrm{Cl}_{K,S}$, so $j = j'$. It follows $\frac{\alpha_i}{\beta\alpha_{i'}} \in \mathcal{O}_{K,S}^\times$. Since $\alpha_i \equiv \frac{\alpha_i}{\beta\alpha_{i'}}\alpha_{i'} \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in T$, this means that α_i and $\alpha_{i'}$ are the same in Ω up to $\pi(\frac{\alpha_i}{\beta\alpha_{i'}})$. Hence, $i = i'$. This is a contradiction. □

The proposition shows that $\mathrm{Cl}_{K,S,T}$ is a finite group of order $h_{K,S,T} := |\mathrm{Cl}_{K,S,T}| = \ell\cdot h_{K,S}$ and gives us a system of representatives for $\mathrm{Cl}_{K,S,T}$. To completely understand the group structure of $\mathrm{Cl}_{K,S,T}$, it suffices to examine how multiplication in $\mathrm{Cl}_{K,S,T}$ works in terms of these representatives. Be aware that we cannot conclude that $\mathrm{Cl}_{K,S,T} \cong \Omega/\operatorname{Im}\pi \times \mathrm{Cl}_{K,S}$. However, multiplication of two $[\alpha_i\mathcal{O}_{K,S}]$ inside $\mathrm{Cl}_{K,S,T}$ simply leads to another $[\alpha_i\mathcal{O}_{K,S}]$. But with $[\mathfrak{a}_j]$ we must be more careful.

Since $\mathrm{Cl}_{K,S}$ is a finite abelian group, $\mathrm{Cl}_{K,S} \cong \bigoplus_{j=1}^{d}\mathbb{Z}/h_j\mathbb{Z}$ for integers $h_1,\dots,h_d \geq 2$. Pick $\mathfrak{b}_1,\dots,\mathfrak{b}_d \in I_{K,S,T}$ such that $\mathrm{Cl}_{K,S} = [\mathfrak{b}_1]^{\mathbb{Z}/h_1\mathbb{Z}} \times \cdots \times [\mathfrak{b}_d]^{\mathbb{Z}/h_d\mathbb{Z}}$. For every $j \in \{1,\dots,d\}$, $\mathfrak{b}_j^{h_j}$ is a principal fractional ideal generated by an element $\alpha \in K^\times$. Then we can find an $i \in \{1,\dots,\ell\}$ such that $[\mathfrak{b}_j]^{h_j} = [\alpha\mathcal{O}_{K,S}] = [\alpha_i\mathcal{O}_{K,S}]$ in $\mathrm{Cl}_{K,S,T}$.

It follows that the abelian group $\mathrm{Cl}_{K,S,T}$ admits a presentation where the generators consist of the generators of $\Omega/\operatorname{Im}\pi$ together with the d generators $[\mathfrak{b}_1],\dots,[\mathfrak{b}_d]$, and the relations consist of the relations inside $\Omega/\operatorname{Im}\pi$ together with the relations $[\mathfrak{b}_j]^{h_j} = [\alpha_i\mathcal{O}_{K,S}]$. It is clear that there are no other relations. We can use well known methods for abelian groups to transform this presentation of $\mathrm{Cl}_{K,S,T}$ into a canonical form.

We end up with the following algorithm for computing $\mathrm{Cl}_{K,S,T}$.

Algorithm 3.8 (Computation of the (S,T)-class group)**.** .

1. [Compute S-units.] Use the algorithm from Section 2.3 to compute fundamental units $\varepsilon_1, \ldots, \varepsilon_n$ of $\mathcal{O}_{K,S}^\times$.
2. [Take discrete logarithms.] For $i = 1, \ldots, m$ and $j = 1, \ldots, n$ set a_{ij} to be the discrete logarithm of ε_j in the residue class field $\mathcal{O}_K/\mathfrak{q}_i$.
3. [Construct quotient group.] Use standard methods for abelian groups to compute the cokernel of A, i. e. the structure of $\bigoplus_{i=1}^m \mathbb{Z}/c_i\mathbb{Z}$ modulo the subgroup generated by $(a_{1j}, \ldots, a_{mj})$ for $j = 1, \ldots, n$. This leads to
$$\frac{\bigoplus_{i=1}^m \mathbb{Z}/c_i\mathbb{Z}}{\operatorname{Im} A} \cong \bigoplus_{i=1}^{\mu} \mathbb{Z}/s_i\mathbb{Z}$$
for integers $s_1, \ldots, s_\mu \geq 2$.
4. [Compute S-class group.] Use the algorithm of Section 2.4 to compute $\mathrm{Cl}_{K,S} = [\mathfrak{b}_1]^{\mathbb{Z}/h_1\mathbb{Z}} \times \cdots \times [\mathfrak{b}_d]^{\mathbb{Z}/h_d\mathbb{Z}}$. If necessary, multiply $\mathfrak{b}_1, \ldots, \mathfrak{b}_d$ by principal fractional ideals to make them coprime to T.
5. [Find relations.] For $j = 1, \ldots, d$, choose a generator $\alpha \in K^\times$ for the principal fractional ideal $\mathfrak{b}_j^{h_j}$. First send α to $\bigoplus_{i=1}^m \mathbb{Z}/c_i\mathbb{Z}$ by taking discrete logarithms again, and then map it to $(k_{1j}, \ldots, k_{\mu j}) \in \bigoplus_{i=1}^\mu \mathbb{Z}/s_i\mathbb{Z}$ by quotienting out $\operatorname{Im} A$.
6. [Terminate.] The desired abelian group $\mathrm{Cl}_{K,S,T}$ is given as
$$\mathrm{Cl}_{K,S,T} \cong \frac{(\bigoplus_{i=1}^\mu \mathbb{Z}/s_i\mathbb{Z}) \oplus \mathbb{Z}^d}{\Gamma}$$
where Γ is the subgroup spanned by the relations $(k_{1j}, \ldots, k_{\mu j}, 0, \ldots, -h_j, \ldots, 0)$ for $j = 1, \ldots, d$ where $-h_j$ stands at the $(\mu + j)$-th coordinate.

Algorithm 3.8 was implemented in Magma. Because the implementation details are quite lengthy, the full source code listing was moved to the appendix.

3.6 Heuristic verification

From Proposition 3.6 we obtain a formula for the index
$$(\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S,T}^\times) = \frac{h_{K,S}}{h_{K,S,T}} \prod_{i=1}^m c_i \tag{3.1}$$
with respect to the class numbers $h_{K,S} := |\mathrm{Cl}_{K,S}|$ and $h_{K,S,T} := |\mathrm{Cl}_{K,S,T}|$. We can compute $\mathcal{O}_{K,S,T}^\times$ and $\mathrm{Cl}_{K,S,T}$ as previously explained. By testing on many examples if this formula holds, we get a rough indication that the two described algorithms seem to be correct, or at least fit well together.

If $S = \emptyset$, then $\mathcal{O}_{K,S,T}^{\times}$ equals the ray class group of the ideal $\mathfrak{q}_1 \cdots \mathfrak{q}_m$ inside $\mathcal{O}_K$. Because the computation of ray class groups is already implemented in Magma, we have a further validation possibility of our algorithm for the (S,T)-class group, just by comparing the results of the routines STClassGroup and RayClassGroup.

Chapter 4 lists several examples which were carried out. Both aforementioned tests always succeeded. Therefore, an implementation mistake seems to be very unlikely.

4 Examples

Example 4.1. Consider the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-1997})$. It turns out that $\mathrm{Cl}_K \cong \mathbb{Z}/42\mathbb{Z}$ and $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z}$. We will work with the following three prime ideals.

name	definition	residue class field
$\mathfrak{p}_1$	(7)	$\mathbb{F}_{49}$
$\mathfrak{p}_2$	$(3, 2+\sqrt{-1997})$	$\mathbb{F}_3$
$\mathfrak{p}_3$	$(17, 3+\sqrt{-1997})$	$\mathbb{F}_{17}$

In order to test our algorithms for as many border cases as possible, we examine all valid combinations of S and T such that $S \cap T = \emptyset$ and $S \cup T \subset \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$. Table 4.1 lists the index of the (S,T)-unit group inside the S-unit group for all these combinations. Because none of the prime ideals divide 2, the $\mathbb{Z}/2\mathbb{Z}$-torsion of $\mathcal{O}_{K,S}^\times$ will always be eliminated when passing to $\mathcal{O}_{K,S,T}^\times$ (except for $T = \emptyset$). In the table we can see that the index increases if we enlarge the set T. This is clear because for any prime ideal added to T, a new congruence relation is imposed.

The computed structures of $\mathrm{Cl}_{K,S,T}$ are shown in Table 4.2. To improve readability, $\mathbb{Z}_n$ was written instead of $\mathbb{Z}/n\mathbb{Z}$. In particular, the entries in the first column are the S-class groups. Furhermore, the entries in the first row are ray class groups. It was verified that they agree with the results of the Magma procedure RayClassGroup. It was also checked that the equation (3.1) holds in all cases.

The purpose of the next example is to highlight the handling of roots of unity.

$S \setminus T$	$\emptyset$	$\{\mathfrak{p}_1\}$	$\{\mathfrak{p}_2\}$	$\{\mathfrak{p}_3\}$	$\{\mathfrak{p}_1, \mathfrak{p}_2\}$	$\{\mathfrak{p}_1, \mathfrak{p}_3\}$	$\{\mathfrak{p}_2, \mathfrak{p}_3\}$	$\{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$
$\emptyset$	1	2	2	2	2	2	2	2
$\{\mathfrak{p}_1\}$	1		2	16			32	
$\{\mathfrak{p}_2\}$	1	8		8		8		
$\{\mathfrak{p}_3\}$	1	16	2		32			
$\{\mathfrak{p}_1, \mathfrak{p}_2\}$	1			16				
$\{\mathfrak{p}_1, \mathfrak{p}_3\}$	1		2					
$\{\mathfrak{p}_2, \mathfrak{p}_3\}$	1	16						
$\{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$	1							

Table 4.1: The indices $(\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S,T}^\times)$

$S \setminus T$	$\emptyset$	$\{\mathfrak{p}_1\}$	$\{\mathfrak{p}_2\}$	$\{\mathfrak{p}_3\}$	$\{\mathfrak{p}_1,\mathfrak{p}_2\}$	$\{\mathfrak{p}_1,\mathfrak{p}_3\}$	$\{\mathfrak{p}_2,\mathfrak{p}_3\}$	$\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}$
$\emptyset$	$\mathbb{Z}_{42}$	$\mathbb{Z}_6 \oplus \mathbb{Z}_{168}$	$\mathbb{Z}_{42}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_{168}$	$\mathbb{Z}_6 \oplus \mathbb{Z}_{336}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{336}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_{336}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_{48} \oplus \mathbb{Z}_{336}$
$\{\mathfrak{p}_1\}$	$\mathbb{Z}_{42}$		$\mathbb{Z}_{42}$	$\mathbb{Z}_{42}$			$\mathbb{Z}_{42}$	
$\{\mathfrak{p}_2\}$	0	$\mathbb{Z}_6$		$\mathbb{Z}_2$		$\mathbb{Z}_2 \oplus \mathbb{Z}_{48}$		
$\{\mathfrak{p}_3\}$	$\mathbb{Z}_{14}$	$\mathbb{Z}_{42}$	$\mathbb{Z}_{14}$		$\mathbb{Z}_{42}$			
$\{\mathfrak{p}_1,\mathfrak{p}_2\}$	0			0				
$\{\mathfrak{p}_1,\mathfrak{p}_3\}$	$\mathbb{Z}_{14}$		$\mathbb{Z}_{14}$					
$\{\mathfrak{p}_2,\mathfrak{p}_3\}$	0	$\mathbb{Z}_3$						
$\{\mathfrak{p}_1,\mathfrak{p}_2,\mathfrak{p}_3\}$	0							

Table 4.2: The (S,T)-class groups

Example 4.2. Consider the cyclotomic field $K = \mathbb{Q}(\zeta_{30})$, where ζ_{30} is a primitive 30-th root of unity, i. e. a zero of the 30-th cyclotomic polynomial

$$\phi_{30}(X) = X^8 + X^7 - X^5 - X^4 - X^3 + X + 1 \,.$$

We have $\mathcal{O}_K^\times \cong \mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}^3$. By definition of $\mathcal{O}_{K,S,T}^\times$, if k is the least common multiple of the orders of ζ_{30} inside the residue class fields $\mathcal{O}_K/\mathfrak{q}$, $\mathfrak{q} \in T$, then exactly the powers of ζ_{30}^k will survive in $\mathcal{O}_{K,S,T}^\times$, so the torsion part of $\mathcal{O}_{K,S,T}^\times$ will be cyclic of order $\frac{30}{k}$. It turns out that $1-\zeta_{30}$, $1-\zeta_{30}^2$, $1-\zeta_{30}^3$ and $1-\zeta_{30}^5$ are units, so there is no residue class field where the order of ζ_{30} equals 1, 2, 3 or 5, respectively. However, $1-\zeta_{30}^6$, $1-\zeta_{30}^{10}$ and $1-\zeta_{30}^{15} = 2$ have prime factors $\mathfrak{q}_1$, $\mathfrak{q}_2$ and $\mathfrak{q}_3$, respectively. Now our algorithm for (S,T)-units computes the following results.

$$\begin{aligned}
\mathcal{O}_{K,\emptyset,\{\mathfrak{q}_1\}}^\times &\cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}^3 & (\mathcal{O}_K^\times : \mathcal{O}_{K,\emptyset,\{\mathfrak{q}_1\}}^\times) &= 24 \\
\mathcal{O}_{K,\emptyset,\{\mathfrak{q}_2\}}^\times &\cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}^3 & (\mathcal{O}_K^\times : \mathcal{O}_{K,\emptyset,\{\mathfrak{q}_2\}}^\times) &= 80 \\
\mathcal{O}_{K,\emptyset,\{\mathfrak{q}_3\}}^\times &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^3 & (\mathcal{O}_K^\times : \mathcal{O}_{K,\emptyset,\{\mathfrak{q}_3\}}^\times) &= 15
\end{aligned}$$

In this case, the residue class fields are $\mathbb{F}_{25}$, $\mathbb{F}_{81}$ and $\mathbb{F}_{16}$. Observe that the torsion parts behave as expected. Of course, we could also have taken a non-empty set S, but this would not change the torsion parts that this example should demonstrate.

The (S,T)-class group algorithm outputs that $\mathrm{Cl}_{K,\emptyset,\{\mathfrak{q}_i\}}$ is trivial for all $i \in \{1,2,3\}$. Hence, by equation (3.1) it should hold

$$(\mathcal{O}_K^\times : \mathcal{O}_{K,\emptyset,\{\mathfrak{q}_i\}}^\times) = N(\mathfrak{q}_i) - 1$$

which matches the computed indices from above.

Finally, we give an example where we test the limits of our implementation by using large sets for S and T.

Example 4.3. Consider the number field $K = \mathbb{Q}(\sqrt[5]{31})$. In contrast to the previous two examples, this is not a Galois extension. It turns out that $\mathrm{Cl}_K \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and $\mathcal{O}_K^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^2$. We take all prime divisors of the first 50 prime numbers and obtain 107 prime ideals. From this set we randomly pick two disjoint subsets S and T, each of cardinality 50.

The (S,T)-unit group algorithm terminates after a few seconds and returns a subgroup of index $(\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S,T}^\times) \approx 10^{200}$. Note that the discrete logarithm matrix has the size 50×53. If we supply an empty set for S, we obtain $(\mathcal{O}_K^\times : \mathcal{O}_{K,\emptyset,T}^\times) \approx 10^{100}$.

The computation of $\mathrm{Cl}_{K,S,T}$ takes a bit longer, but $\mathrm{Cl}_{K,S,T}$ usually ends up to be trivial. However, $\mathrm{Cl}_{K,\emptyset,T}$ is highly non-trivial. This is clear, because (3.1) implies that

$$h_{K,\emptyset,T} = 25 \cdot \frac{(\mathcal{O}_{K,S}^\times : \mathcal{O}_{K,S,T}^\times)}{(\mathcal{O}_K^\times : \mathcal{O}_{K,\emptyset,T}^\times)} \approx 10^{100}$$

if $h_{K,S,T} = h_{K,S} = 1$. It was checked that RayClassGroup returned exactly the same huge group. Also the precise equality in (3.1) was verified.

List of symbols

$\mathbb{N}$	positive integers
$\mathbb{N}_0$	non-negative integers
$\mathbb{Z}$	integers
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
$\mathbb{F}_q$	finite field with q elements
$\lvert X\rvert$	cardinality of set
$\lhd$	ideal relation
$\leq$	subgroup relation
$\mathrm{Re}(s)$	real part
$[\mathfrak{a}]$	equivalence class
$\langle \ldots \rangle$	generated subgroup
$\oplus$	direct sum
$\times$	direct product
Rank	rank of abelian group
Ker	kernel
Im	image
K	algebraic number field
$K^\times$	invertible (i. e. non-zero) field elements
$\mathcal{O}_K$	integer ring
$\mathcal{O}_K/\mathfrak{p}$	residue class field
$\mathcal{O}_K^\times$	unit group
$\mathcal{O}_{K,S}$	S-integers
$\mathcal{O}_{K,S}^\times$	S-units
$\mathcal{O}_{K,S,T}^\times$	(S,T)-units
ν	degree of extension $K \mid \mathbb{Q}$
r	number of real embeddings
t	number of complex embeddings
R_K	regulator
d_K	discriminant
w_K	number of roots of unity
ε_i	fundamental units
$N(\mathfrak{a})$	ideal norm
$v_\mathfrak{p}$	discrete valuation of $\mathfrak{p}$
ζ_K	Dedekind zeta function

σ_i	real embedding
$\tau_i, \overline{\tau_i}$	pair of (proper) complex embeddings
$\lvert\alpha\rvert_i$	archimedian valuation
S	finite set of prime ideals
T	finite set of prime ideals with $S \cap T = \emptyset$
Cl_K	class group
$\mathrm{Cl}_{K,S}$	S-class group
$\mathrm{Cl}_{K,S,T}$	(S,T)-class group
h_K	class number
$h_{K,S}$	S-class number
$h_{K,S,T}$	(S,T)-class number
P_K	set of non-zero prime ideals
I_K	fractional ideals
H_K	principal fractional ideals
$I_{K,S}$	fractional S-ideals
$H_{K,S}$	principal fractional S-ideals
$I_{K,S,T}$	fractional S-ideals coprime to T
$H_{K,S,T}$	T-ray principal fractional S-ideals

Source code of **STClassGroup**

```
1  intrinsic SClassGroup(S :: [ RngOrdIdl ]) -> GrpAb, Map
2  {Compute the S-class group.}
3          require not IsEmpty(S): "S must be non-empty.";
4          O := Order(S[1]);
5          C, mC := ClassGroup(O);
6          R := [ Inverse(mC)(p) : p in S ];
7          D, mD := quo<C | R>;
8          return D, Inverse(mD) * mC;
9  end intrinsic;
10
11 intrinsic IsSPrincipal(S :: [ RngOrdIdl ], I :: RngOrdFracIdl) -> BoolElt, FldOrdElt
12 {Check if I is principal with respect to S-integers, and return a generator in that case.}
13         if IsEmpty(S) then
14                 return IsPrincipal(I);
15         end if;
16         O := Order(I);
17         C, mC := ClassGroup(O);
18         F := FreeAbelianGroup(#S);
19         f := hom< F -> C | [ Inverse(mC)(p) : p in S ]>;
20         a := Inverse(mC)(I);
21         if a in Image(f) then
22                 I := ElementToSequence(Inverse(f)(a));
23                 I := I / &*[S[j] ^ I[j] : j in [1..#S]];
24                 return IsPrincipal(I);
25         end if;
26         return false;
27 end intrinsic;
28
29 intrinsic STClassGroup(S :: [ RngOrdIdl ], T :: [ RngOrdIdl ]) -> GrpAb, Map
30 {Compute the (S,T)-class group.}
31         require not (IsEmpty(S) and IsEmpty(T)):
32                 "At least S or T must be non-empty.";
33         require IsDisjoint(SequenceToSet(S), SequenceToSet(T)):
34                 "S and T must be disjoint.";
35         if IsEmpty(S) then
36                 O := Order(T[1]);
```

```
37              U, mU := UnitGroup(O);
38              C, mC := ClassGroup(O);
39          else
40              O := Order(S[1]);
41              U, mU := SUnitGroup(S);
42              C, mC := SClassGroup(S);
43          end if;
44          if IsEmpty(T) then
45              return C, mC;
46          end if;
47          P := &*T;
48          n := NumberOfGenerators(U);
49          d := NumberOfGenerators(C);
50          A := quo<O | P>;
51          R, mR := UnitGroup(A);
52          Q, mQ := quo<R | [Inverse(mR)(A ! mU(U.j)) : j in [1..n]]>;
53          q := NumberOfGenerators(Q);
54          D := DirectSum(Q, FreeAbelianGroup(d));
55          rel := [];
56          b := [ FieldOfFractions(O) | ];
57          for i := 1 to d do
58              h := AbelianInvariants(C)[i];
59              b[i] := MakeCoprime(mC(C.i), P);
60              I := (b[i] * mC(C.i)) ^ h;
61              t, g := IsSPrincipal(S, I);
62              if not t then
63                  // Something went completely wrong
64              end if;
65              gq := mQ(Inverse(mR)(A ! g));
66              rel[i] := D ! (ElementToSequence(gq) cat [0 : j in [1..d]]) = h * D.(q+i);
67          end for;
68          Y, mY := quo<D | rel>;
69          idealRepresentative := function(x)
70              x := Inverse(mY)(x);
71              x := ElementToSequence(x);
72              y := Q ! [x[i] : i in [1..q]];
73              y := O ! mR(Inverse(mQ)(y));
74              z := &*[PowerIdeal(FieldOfFractions(O)) | (b[i] * mC(C.i)) ^ x[i+q] : i in [1..d]];
75              return y * z;
76          end function;
77          idealClass := function(I)
78              c := Inverse(mC)(I);
79              c := ElementToSequence(c);
80              z := &*[PowerIdeal(FieldOfFractions(O)) | (b[i] * mC(C.i)) ^ c[i] : i in [1..d]];
```

```
81                  t, g := IsSPrincipal (S, I / z);
82                  if not t then
83                          // Something went completely wrong
84                  end if;
85                  gq := mQ(Inverse(mR)(A ! g));
86                  return mY(D ! (ElementToSequence(gq) cat c));
87          end function;
88          return Y, hom<Y -> PowerIdeal(FieldOfFractions(O)) |
89                  x :-> idealRepresentative(x), I :-> idealClass(I) >;
90  end intrinsic;
```

Bibliography

[Coh96] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Number 138 in Graduate Texts in Mathematics. Springer, 3rd corrected printing edition, 1996.

[Coh00] Henri Cohen. *Advanced Topics in Computational Number Theory*. Number 193 in Graduate Texts in Mathematics. Springer, 2000.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[PZ85] Michael Pohst and Hans Zassenhaus. Über die Berechnung von Klassenzahlen und Klassengruppen algebraischer Zahlkörper. *Journal für die reine und angewandte Mathematik*, 361:50–72, 1985.

[Rub96] Karl Rubin. A Stark conjecture "over $\mathbb{Z}$" for abelian L-functions with multiple zeros. *Ann. Inst. Fourier*, 46:33–62, 1996.

[Tat84] John Tate. *Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$*, volume 47 of *Progress in Mathematics*. Birkhäuser, 1984.

Selbstständigkeitserklärung

Hiermit versichere ich, die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel verfasst zu haben.

München, den 22. Februar 2017