Student seminar solutions Week 7

1. The explicit formula for the strict ray class number modulo $\mathfrak{m}$ is

$$|\mathcal{R}^+_{F,\mathfrak{m}}| = \frac{h_F 2^{r_1} \varphi(\mathfrak{m})}{[\mathcal{U}_F : \mathcal{U}^+_{F,\mathfrak{m}}]} \tag{1}$$

where :

- h_F is the class number
- r_1 is the number of real embeddings
- $\varphi(\mathfrak{m})$ is the cardinal of $\left(\frac{\mathcal{O}_F}{\mathfrak{m}}\right)^\times$
- $\mathcal{U}_F = \mathcal{O}_F^\times$, the units of $\mathcal{O}_F$
- $\mathcal{U}^+_{F,\mathfrak{m}} = \{\varepsilon \in \mathcal{U}_F \mid \varepsilon \gg 0, \varepsilon \equiv 1 \pmod{\mathfrak{m}}\}$

(a) Let $F = \mathbb{Q}(\sqrt{3})$ and $\mathfrak{m} = \mathcal{O}_F$. Compute the ray strict ray class number and deduce what the ray class group $\mathcal{R}^+_{\mathbb{Q}(\sqrt{3}),\mathbb{Z}[\sqrt{3}]}$ is up to isomorphism.

(b) Same question for $F = \mathbb{Q}(i)$, $\mathfrak{m} = \mathcal{O}_F$.

(c) Compare $\mathcal{R}^+_{\mathbb{Q}(i),\mathbb{Z}[i]}$ and $\mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}$. How are they related ?

Solution:

(a) We will simply apply the above formula for the strict ray class number.
In our case, as $F = \mathbb{Q}(\sqrt{3})$, we have that $\mathfrak{m} = \mathcal{O}_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}]$ and $r_1 = 2$. Moreover, as $\mathbb{Z}[\sqrt{3}]$ is a PID, we have that $h_F = 1$ and we observe that $\mathcal{O}_F^\times = \{\pm(2+\sqrt{3})^n : n \in \mathbb{Z}\}$. We can also compute

$$\varphi(\mathcal{O}_F) = \left| \left(\frac{\mathcal{O}_F}{\mathcal{O}_F}\right)^\times \right| = 1.$$

The only part missing to use the formula is the denominator

$$[\mathcal{U}_F : \mathcal{U}^+_{F,\mathfrak{m}}].$$

To compute it, recall Theorem 1.9 of the book Class Field Theory by Nancy Childress:

Theorem 0.1 (Dirichlet Unit Theorem)**.** *Let F be a number field and r_1, r_2 represent the number of real embeddings and the number of conjugate pairs of imaginary embeddings of F respectively. There are units $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in \mathcal{O}_F^\times$ such that*

$$\begin{aligned}\mathcal{O}_F^\times &\cong \mathcal{W}_F \times \langle \varepsilon_1 \rangle \times \cdots \times \langle \varepsilon_{r_1+r_2-1} \rangle \\ &\cong \mathcal{W}_F \times \mathbb{Z}^{r_1+r_2-1},\end{aligned}$$

where $\mathcal{W}_F$ is the group of roots of unity in F. The ε_j are called a fundamental system of units for F.

In our case, since $\mathcal{U}_F = \mathcal{O}_F^\times$, $\mathcal{W}_F = \{\pm 1\}$, $r_1 = 2$ and $r_2 = 0$, we get by Dirichlet Unit Theorem that

$$\mathcal{U}_F \cong \{\pm 1\} \times \mathbb{Z} \cong \{\pm 1\} \times \langle \varepsilon \rangle$$

where ε is a fundamental unit. We observe that in our case, the fundamental units for $\mathbb{Q}(\sqrt{3})$ are $\{\pm(2+\sqrt{3})\}$ as $(2+\sqrt{3})^{-1} = 2-\sqrt{3}$. Let us take $\varepsilon = 2 + \sqrt{3}$. Then we have $\varepsilon >> 0$ and by definition

$$\mathcal{U}_F^\times = \{u \in \mathcal{U}_F : u >> 0, u \equiv 1 \ mod(\mathcal{O}_F)\} = \langle \varepsilon \rangle,$$

hence

$$[\mathcal{U}_F : \mathcal{U}_{F,\mathfrak{m}}^\times] = 2$$

and by the above formula, we conclude that

$$|\mathcal{R}_{F,\mathfrak{m}}^+| = \frac{1 \cdot 2^2 \cdot 1}{2} = 2.$$

Since $\mathcal{R}_{F,\mathfrak{m}}^+$ is the quotient of abelian groups, this is an abelian group. We know that up to isomorphism, there is only one abelian group of order 2, thus

$$\mathcal{R}_{\mathbb{Q}(\sqrt{3}),\mathbb{Z}[\sqrt{3}]}^+ \cong \mathbb{Z}/2\mathbb{Z}$$

.

(b) We have $\mathcal{O}_F = \mathbb{Z}[i]$. Since $\mathbb{Q}(i)$ has no real embeddings and one pair of conjugate embedding, we have $r_1 = 0$ and $r_2 = 1$. As above, $\mathbb{Z}[i]$ is a PID so $h_F = 1$. We again have $\varphi(\mathcal{O}_F) = 1$ and we have

$$\mathcal{U}_F = \mathcal{O}_F^\times = \{\pm 1, \pm i\}.$$

In the definition of $\mathcal{U}_{F,\mathfrak{m}}^+$, we have $u >> 0$, which by definition means that $\sigma(u) > 0$ for all real embeddings, but in our case, as we do not have any real embedding, we get $\mathcal{U}_{F,\mathfrak{m}}^+ = \mathcal{U}_F$ and so $[\mathcal{U}_F : \mathcal{U}_{F,\mathfrak{m}}^+] = 1$. By the above formula for the strict ray class number modulo $\mathfrak{m}$, we get

$$|\mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}^+| = \frac{1 \cdot 2^0 \cdot 1}{1} = 1.$$

Thus $\mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}^+$ is trivial.

(c) By definition,

$$\mathcal{R}^+_{F,\mathfrak{m}} = \frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{P}^+_{F,\mathfrak{m}}} \text{ and } \mathcal{R}_{F,\mathfrak{m}} = \frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{P}_{F,\mathfrak{m}}}.$$

Moreover, $\mathcal{P}^+_{F,\mathfrak{m}}$ is the subgroup of totally positive element of $\mathcal{P}_{F,\mathfrak{m}}$. Since we do not have any real embedding, $\mathcal{P}_{F,\mathfrak{m}} = \mathcal{P}^+_{F,\mathfrak{m}}$ and so

$$\mathcal{R}^+_{\mathbb{Q}(i),\mathbb{Z}[i]} = \mathcal{R}_{\mathbb{Q}(i),\mathbb{Z}[i]}.$$

2. Let F be a number field and let $\mathfrak{n}, \mathfrak{m}$ be (not necessarily distinct) ideals of $\mathcal{O}_F$. Is it possible to find $\mathcal{H}_1 \neq \mathcal{H}_2$ with $\mathcal{P}^+_{F,\mathfrak{n}} \leq \mathcal{H}_1 < \mathcal{I}_F(\mathfrak{n})$ and $\mathcal{P}^+_{F,\mathfrak{m}} \leq \mathcal{H}_2 < \mathcal{I}_F(\mathfrak{m})$ such that they have the same class field over F ?

   Solution:

   Yes, it is possible.
   Let $F = \mathbb{Q}$, $\mathfrak{n} = n\mathbb{Z}$ and $\mathfrak{m} = (2n)\mathbb{Z}$ where n is odd. Let $\mathcal{H}_1 = \mathcal{P}^+_{\mathbb{Q},\mathfrak{n}}$, $\mathcal{H}_2 = \mathcal{P}^+_{\mathbb{Q},\mathfrak{m}}$ and observe that $\mathcal{H}_1 \neq \mathcal{H}_2$. By an example of the Lecture Notes, we know that the class field over $\mathbb{Q}$ of $\mathcal{H}_1$ is $K = \mathbb{Q}(\zeta_n)$ and that the class field over $\mathbb{Q}$ of $\mathcal{H}_2$ is $L = \mathbb{Q}(\zeta_{2n})$. Now, since n is odd, we have that $K = L$ and so we found $\mathcal{H}_1 \neq \mathcal{H}_2$ such that they have the same class field over $\mathbb{Q}$.

3. Let K be the class field of $\mathcal{H}$ over F where $\mathcal{P}^+_{F,\mathfrak{m}} \leq \mathcal{H} < \mathcal{I}_F(\mathfrak{m})$.
   Prove that $[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] = [K : F]$.

   Solution:

   By definition, since K is the class field for $\mathcal{H}$, we have

   $$\{\text{primes } \mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \in \mathcal{H}\} \approx S_{K/F} = \{\text{primes } \mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \text{ splits completely in } K/F\}.$$

   By definition of $\approx$, we have that $\{\text{primes } \mathfrak{p} \in \mathcal{O}_F : \mathfrak{p} \in \mathcal{H}\}$ and $S_{K/F}$ differ by a set with Dirichlet density zero, thus

   $$\delta_F(\{\text{primes } \mathfrak{p} \in \mathcal{H}\} \backslash S_{K/F}) = \lim_{s \to 1^+} \sum_{\mathfrak{p} \in \mathcal{H} \backslash S_{K/F}} \frac{N\mathfrak{p}^{-1}}{\log(\frac{1}{s-1})} = 0.$$

   With this equality, we redo the proof of Theorem 2.4 of the book Class Field Theory by Nancy Childress to get the result.
   Let $m(\chi) = \text{ord}_{s=1}(L_{\mathfrak{m}}(s, \chi))$. For $\chi \neq \chi_0$, we know that $m(\chi) \geq 0$, while $m(\chi_0) = -1$. As in the assumption of Theorem 2.4, we take χ to be trivial on $\mathcal{H}$ and we may view χ as a character of $\frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{H}}$.
   There is some constant a such that

   $$\prod_{\chi \in \widehat{\frac{\mathcal{I}_F(\mathfrak{m})}{\mathcal{H}}}} L_{\mathfrak{m}}(s, \chi) = a(s-1)^{\sum_\chi m(\chi)} + \cdots$$

Taking logs, we get

$$\begin{aligned}\sum_{\chi} \log L_{\mathfrak{m}}(s,\chi) &\sim \left(\sum_{\chi} m(\chi)\right) \log(s-1) \\ &= -\left(\sum_{\chi} m(\chi)\right) \log\left(\frac{1}{s-1}\right).\end{aligned}$$

Now

$$\begin{aligned}\log L_{\mathfrak{m}}(s,\chi) &= \sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{n=1}^{\infty} \frac{\chi(\mathfrak{p})^n}{nN\mathfrak{p}^{ns}} \\ &\sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p}) N\mathfrak{p}^{-s}\end{aligned}$$

and so as in the proof of Proposition 2.3

$$\sum_{\chi} \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p}\in\mathcal{H}} [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] N\mathfrak{p}^{-s}.$$

Hence,

$$\sum_{\mathfrak{p}\in\mathcal{H}} [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] N\mathfrak{p}^{-s} \sim -\left(\sum_{\chi} m(\chi)\right) \log\left(\frac{1}{s-1}\right).$$

We can split the LHS, divide by $\log\left(\frac{1}{s-1}\right)$ and let $s \to 1^+$ to obtain

$$\begin{aligned}-\sum_{\chi} m(\chi) &= \lim_{s\to 1^+} \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \sum_{\mathfrak{p}\in S_{K/F}} N\mathfrak{p}^{-s}}{\log\left(\frac{1}{s-1}\right)} + \lim_{s\to 1^+} \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \sum_{\mathfrak{p}\in\mathcal{H}\setminus S_{K/F}} N\mathfrak{p}^{-s}}{\log\left(\frac{1}{s-1}\right)} \\ &= [\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] \delta_f(S_{K/F}) \\ &= \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}{[K : F]}\end{aligned}$$

as the second term on the right is zero by the equation we got at the start of the exercise.
As $m(\chi) \geq 0$ for all $\chi \neq \chi_0$ and $m(\chi_0) = -1$, we have

$$1 \geq 1 - \sum_{\chi\neq\chi_0} m(\chi) = \frac{[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}]}{[K : F]} > 0.$$

This force $m(\chi) = 0$ for all $\chi \neq \chi_0$ and so $-\sum_{\chi} m(\chi) = 1$. Thus we get

$$[\mathcal{I}_F(\mathfrak{m}) : \mathcal{H}] = [K : F].$$

4. Let F be a number field. If we take $\mathfrak{m} = \mathcal{O}_F$, then the class field of $\mathcal{P}_{F,\mathfrak{m}}$ over F is called the *Hilbert class field*.

   (a) Find the Hilbert class field of $\mathbb{Q}$.

   (b) Find the Hilbert class field of $\mathbb{Q}(i)$.

   Solution:

   (a) As $F = \mathbb{Q}$, we have $\mathcal{O}_F = \mathbb{Z}$. By the Isomorphism Theorem, we know that
   $$\mathrm{Gal}(K/F) \cong \mathcal{I}_F/\mathcal{P}_F = \mathcal{C}_F$$
   where K is the Hilbert class field of F.
   In our case, as $\mathbb{Z}$ is a PID, we have $\mathcal{I}_F = \mathcal{P}_F$, thus $\mathrm{Gal}(K/F)$ is trivial and so $K = F = \mathbb{Q}$.

   (b) As $F = \mathbb{Q}(i)$, $\mathcal{O}_F = \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, $\mathcal{P}_F = \mathcal{I}_F$.
   By the Isomorphism Theorem
   $$\mathrm{Gal}(K/\mathbb{Q}(i)) \cong \{1\},$$
   thus $K = F = \mathbb{Q}(i)$.

5. *(Algebraic bonus !)* Prove that there is an exact sequence
   $$0 \longrightarrow \mathcal{O}_F^\times \hookrightarrow F^{\mathfrak{m}} \longrightarrow \mathcal{I}(\mathfrak{m}) \twoheadrightarrow \mathcal{C}_F \longrightarrow 0$$
   where $F^{\mathfrak{m}} := \{a \in F^\times \mid \langle a \rangle \in \mathcal{I}_F(\mathfrak{m})\}$.

   This is lemma 1.1 on page 148 of the book Class Field Theory*, by J. S. Milne. You can refer to it for a proof !*

   Solution:

   Let S be the set of primes dividing $\mathfrak{m}$ and I^S be the subgroup of $\mathcal{I}_F$ generated by primes not in S. We observe that $\mathcal{I}_F(\mathfrak{m}) = I^S$. Moreover, if we define $i : F^\times \to \mathcal{I}_F$ to be the map sending $a \in F^\times$ to the principal ideal $\langle a \rangle$, we see that $i(F^\times) = \mathcal{P}_F$. With these observations, we can rewrite our exact sequence as
   $$0 \longrightarrow \mathcal{O}_F^\times \hookrightarrow F^{\mathfrak{m}} \longrightarrow I^S \twoheadrightarrow C \longrightarrow 0$$
   where $C = \mathcal{I}_F/i(F^+)$.
   To show that $I^S \to C$ is surjective, we have to show that every ideal class $\mathcal{C}$ of C is represented by an ideal in I^S. Let $\mathfrak{a} \in \mathcal{I}_F$ represents $\mathcal{C}$. By definition of a fractional ideal, we have that there exist a non-zero $\alpha \in F$ such that $\alpha\mathfrak{a} \subseteq \mathcal{O}_F$. Take $\mathfrak{b} = \alpha\mathfrak{a}$ and $\mathfrak{c} = \langle \alpha \rangle$, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ with $\mathfrak{b}$ and $\mathfrak{c}$ integral ideals. Now, let $c \in \mathfrak{c}$. We have
   $$\mathfrak{a} \cdot \langle c \rangle = \mathfrak{b} \cdot \mathfrak{c}^{-1} \cdot \langle c \rangle,$$

but since $c \in \mathfrak{c}$, we have $\langle c \rangle \subseteq \mathfrak{c}$, thus $\mathfrak{c}^{-1}\langle c \rangle$ is an integral ideal. This give us that $\mathfrak{a} \cdot \langle c \rangle$ is a product of integral ideals and so integral itself. Now, since the class of $\mathfrak{a}$ in C only depends on it up to multiplication by a principal ideal, we may suppose that $\mathfrak{a}$ is an integral ideal. Write

$$\mathfrak{a} = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n(\mathfrak{p})} \mathfrak{b},$$

where $\mathfrak{b} \in I^S$. For each $\mathfrak{p} \in S$, choose $\pi_\mathfrak{p} \in \mathfrak{p} \backslash \mathfrak{p}^2$ so that $\mathrm{ord}_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. By the Chinese Remainder Theorem, there exists an $a \in \mathcal{O}_F$ such that

$$a \equiv \pi_\mathfrak{p}^{n(\mathfrak{p})} \bmod \mathfrak{p}^{n(\mathfrak{p})+1}$$

for all $\mathfrak{p} \in S$. These congruences imply that $\mathrm{ord}_\mathfrak{p}(a) = n(\mathfrak{p})$ for all $\mathfrak{p} \in S$, so

$$\langle a \rangle = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n(\mathfrak{p})} \mathfrak{b}'$$

with $\mathfrak{b}' \in I^S$. We get $a^{-1}\mathfrak{a} \in I^S$ and it represents the same class as $\mathfrak{a}$ in C, so $I^S \to C$ is surjective as we wanted.
Let the map $F^\mathfrak{m} \to I^S$ be defined by sending a to $\langle a \rangle$. Now, if $\mathfrak{a} \in I^S$ maps to zero in C, then $\mathfrak{a} = \langle a \rangle$ for some $a \in F^\mathfrak{m}$, and a is uniquely determined up to a unit. Conversely, $a \in F^\mathfrak{m}$ is send to $\langle a \rangle \in \mathcal{P}_F$, thus it is in $\ker(I^S \to C)$.
To conclude, we show that $\ker(F^\mathfrak{m} \to I^S)$ is $\mathcal{O}_F^\times$. We see $\mathcal{O}_F^\times \to F^\mathfrak{m}$ as the inclusion. If $a \in \mathcal{O}_F^\times$, then $\langle a \rangle = \mathcal{O}_F$. Conversely, if $\langle a \rangle = \mathcal{O}_F$, then a has an inverse in $\mathcal{O}_F$, so it is a unit. This prove that $\ker(F^\mathfrak{m} \to I^S) = \mathcal{O}_F^\times$ and prove the exactness of the sequence.