Student Seminar Solutions Week 8

1. We first compute the class number of $F = \mathbb{Q}(\sqrt{15})$. Since the Hilbert class field of F is a Galois extension of F with Galois group isomorphic to $\mathcal{C}_F$ by the Isomorphy Theorem, the degree of the Hilbert class field extension coincides with the class number of F.

   The discriminant of F is $d_{F/\mathbb{Q}} = 60$, by the known results on discriminants of quadratic extensions. Moreover, the degree of the extension over $\mathbb{Q}$ is $n = 2$, and the number of pairs of complex embeddings is $r_2 = 0$. Hence, the Minkowski bound is given by

$$M_F = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_{F/\mathbb{Q}}|} = \sqrt{15} < 4.$$

   Consequently, every ideal class contains an integral ideal of norm at most 3. To determine the class group, it therefore suffices to examine the prime ideals lying above the rational primes 2 and 3.

   Since 2 and 3 divide the discriminant, they ramify in F. Their norms are 4 and 9, respectively, and hence

$$(2) = \mathfrak{p}_2^2 \quad \text{and} \quad (3) = \mathfrak{p}_3^2,$$

   where $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are the unique prime ideals of $\mathcal{O}_F$ lying above 2 and 3, with $N_{F/\mathbb{Q}}(\mathfrak{p}_2) = 2$ and $N_{F/\mathbb{Q}}(\mathfrak{p}_3) = 3$.

   Using computational tools such as SageMath, one finds

$$\mathfrak{p}_2 = (2, 1 + \sqrt{15}) \quad \text{and} \quad \mathfrak{p}_3 = (3, \sqrt{15}).$$

   Both ideals are non-principal. Indeed, suppose that $\mathfrak{p}_2 = (a)$ for some $a \in \mathcal{O}_F = \mathbb{Z}[\sqrt{15}]$. Then

$$N_{F/\mathbb{Q}}(a) \mid N_{F/\mathbb{Q}}(2) = 4 \quad \text{and} \quad N_{F/\mathbb{Q}}(a) \mid N_{F/\mathbb{Q}}(1 + \sqrt{15}) = -14,$$

   so $N_{F/\mathbb{Q}}(a) \in \{\pm 1, \pm 2\}$. Writing $a = b + c\sqrt{15}$, we have

$$N_{F/\mathbb{Q}}(a) = b^2 - 15c^2.$$

   If $N_{F/\mathbb{Q}}(a) = 1$, then a is a unit, which is impossible since $\mathfrak{p}_2$ is proper. Moreover, a brief check shows that -1 and ± 2 are not values of $b^2 - 15c^2$

for integers b, c. Hence, $\mathfrak{p}_2$ is non-principal. A similar argument shows that $\mathfrak{p}_3$ is likewise not principal.

By the Minkowski bound, the ideal class group is generated by the classes of $\mathfrak{p}_2$ and $\mathfrak{p}_3$. We compute their product:

$$\mathfrak{p}_2\mathfrak{p}_3 = (6, 3+3\sqrt{15}, 2\sqrt{15}, \sqrt{15}+15) = (6, 3+\sqrt{15}).$$

This ideal is principal, since

$$-(3-\sqrt{15})(3+\sqrt{15}) = 6.$$

Hence $[\mathfrak{p}_2] = [\mathfrak{p}_3]^{-1}$. Because $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3^2$, we have

$$[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = \big[(0)\big].$$

Thus, $\mathcal{C}_F \cong \mathbb{Z}/2\mathbb{Z}$.

Now consider $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Since it is the compositum of the linearly disjoint fields $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$, its discriminant satisfies

$$d_{K/\mathbb{Q}} = d_{\mathbb{Q}(\sqrt{3})/\mathbb{Q}}^{\left[\mathbb{Q}(\sqrt{5}):\mathbb{Q}\right]} \cdot d_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}^{\left[\mathbb{Q}(\sqrt{3}):\mathbb{Q}\right]} = 12^2 \cdot 5^2 = 60^2.$$

For a tower of field extensions $A \subset B \subset C$, we have

$$d_{C/A} = N_{B/A}(d_{C/B}) \cdot d_{B/A}^{[C:B]}.$$

Applying this to $\mathbb{Q} \subset F \subset K$, we obtain

$$N_{F/\mathbb{Q}}(d_{K/F}) = 1.$$

In particular, the extension $F \subset K$ is unramified. Moreover, $F \subset K$ is abelian, since $\mathbb{Q} \subset K$ is abelian with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Therefore, K is contained in the Hilbert class field of F (by the equivalent characterization of the Hilbert class field).

Since both fields have the same degree, recall that the class number of F is 2, we conclude that they coincide. Hence,

$$K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

is the Hilbert class field of $F = \mathbb{Q}(\sqrt{15})$.

2. Let F be a number field and denote its Hilbert class field by F_1.

   (I) Let F_2 be the Hilbert class field of F_1. We show that F_2/F is Galois. Since extensions of number fields are separable, it suffices to prove normality of F_2/F, i.e. that every F-embedding $\sigma\colon F_2 \hookrightarrow \mathbb{C}$ has image $\sigma(F_2) = F_2$. Let $\sigma\colon F_2 \hookrightarrow \mathbb{C}$ be an F-embedding. Its restriction to F_1 satisfies

$$\sigma|_{F_1} \in \mathrm{Hom}_F(F_1, \mathbb{C}) = \mathrm{Hom}_F(F_1, F_1),$$

because F_1/F is Galois. In particular $\sigma(F_1) = F_1$. Now σ induces an isomorphism

$$\sigma\colon F_2 \xrightarrow{\cong} \sigma(F_2),$$

Since F_2 is the Hilbert class field of F_1, i.e. the maximal unramified abelian extension of F_1, $\sigma(F_2)$ has to be the maximal unramified abelian extension of $\sigma(F_1) = F_1$. By uniqueness of the Hilbert class field of F_1, we must have $\sigma(F_2) = F_2$. Thus, every F-embedding of F_2 into $\mathbb{C}$ is an F-automorphism of F_2, so F_2/F is normal and hence Galois.

(II) Set $A = \mathrm{Gal}(F_2/F_1)$ and $G = \mathrm{Gal}(F_2/F)$. Then $A \trianglelefteq G$ and

$$G/A \cong \mathrm{Gal}(F_1/F).$$

Since F_2 is the Hilbert class field of F_1, it is unramified over F_1 and hence (by multiplicativity of ramification in towers) also unramified over F. Consequently F_1 is the maximal abelian subextension of F contained in F_2, so G/A is the largest abelian quotient of G. Equivalently, A is the commutator subgroup $G' = [G, G]$ of G.

Next consider the extension-of-ideals map $\mathcal{I}_F \to \mathcal{I}_{F_1}$, which is a group homomorphism. Composing with the quotient $\mathcal{I}_{F_1} \to \mathcal{I}_{F_1}/\mathcal{P}_{F_1}$ gives

$$\tilde{\gamma}\colon \mathcal{I}_F \longrightarrow \mathcal{I}_{F_1}/\mathcal{P}_{F_1}.$$

If $(a) \in \mathcal{P}_F$ is principal in F, then $(a)\mathcal{O}_{F_1}$ is principal in F_1, so $\tilde{\gamma}\big((a)\big)$ is trivial. Hence $\tilde{\gamma}$ factors through the quotient by $\mathcal{P}_F$, yielding a homomorphism of ideal class groups

$$\gamma\colon \mathcal{I}_F/\mathcal{P}_F = \mathcal{C}_F \longrightarrow \mathcal{I}_{F_1}/\mathcal{P}_{F_1} = \mathcal{C}_{F_1},$$

given on classes by $\mathfrak{a}\mathcal{P}_F \mapsto (\mathfrak{a}\mathcal{O}_{F_1})\mathcal{P}_{F_1}$.

(III) By the Isomorphy Theorem, we obtain

$$G/G' \cong \mathrm{Gal}(F_1/F) \cong \mathcal{C}_F \quad \text{and} \quad G' = A = \mathrm{Gal}(F_2/F_1) \cong \mathcal{C}_{F_1},$$

since the Hilbert class field of a number field K is, by definition, the class field associated with $\mathcal{P}_{K,\mathcal{O}_K} = \mathcal{P}_K$, the group of principal ideals of K.

We thus have the following commutative diagram:

$$\begin{array}{ccc} \mathcal{C}_F & \xrightarrow{\cong} & G/G' \\ \big\downarrow{\scriptstyle \gamma} & & \big\downarrow{\scriptstyle V} \\ \mathcal{C}_{F_1} & \xrightarrow{\cong} & G'. \end{array}$$

If we can show that the transfer map V is trivial, then by commutativity of the diagram it follows that γ is trivial as well. Triviality of γ means that every ideal of F becomes principal in F_1, i.e. the Principal Ideal Theorem holds for F_1/F.

(IV) Finally, observe that $A = G'$ is abelian. Hence its commutator subgroup $(G')'$ is trivial. The hypothesis of the given group-theoretic theorem therefore applies and implies that the transfer map

$$V\colon G/G' \longrightarrow A$$

is trivial. By commutativity of the diagram this yields $\gamma = 0$, so every ideal of $\mathcal{O}_F$ becomes principal in $\mathcal{O}_{F_1}$. This is precisely the Principal Ideal Theorem.

3. Let $\|\cdot\|$ be an absolute value on a number field F. We want to show that there exists a positive real number λ such that $\|\cdot\|^\lambda$ satisfies the triangle inequality.

First, note that by multiplicativity we have $\|1\| = 1$, and by definition $\|0\| = 0$. Suppose that $c = 1$. Then, whenever $\|x\| \leq 1$, we have

$$\|1 + x\| \leq 1.$$

Let $y, z \in F$. We claim that $\|\cdot\|$ already satisfies the triangle inequality. If either y or z is zero, the inequality is trivially verified. Hence, suppose that y and z are both nonzero, and without loss of generality assume that $\|y\| \leq \|z\|$. Set $u = \frac{y}{z}$. By multiplicativity of the absolute value, we obtain

$$\|u\| = \frac{\|y\|}{\|z\|} \leq 1.$$

By assumption, this implies that $\|1 + u\| \leq 1$. Therefore,

$$\|y + z\| = \|z\| \cdot \|1 + u\| \leq \|z\| \leq \|y\| + \|z\|.$$

Hence $\|\cdot\|$ satisfies the triangle inequality. Moreover, we have seen that $\|\cdot\|$ is non-Archimedean.

Suppose now that $c > 1$. Note that by setting $\lambda = \log_c(2)$, we obtain

$$\|1 + x\|^\lambda \leq c^\lambda = 2$$

whenever $\|x\| \leq 1$. We will show that $|\cdot| \coloneqq \|\cdot\|^\lambda$ satisfies the triangle inequality.

Let $x_1, x_2 \in F$. If $0 \neq |x_1| \geq |x_2|$, then

$$|x_1 + x_2| = |x_1| \cdot |x_1^{-1} x_2 + 1| \leq 2|x_1|.$$

Hence,

$$|x_1 + x_2| \leq 2 \max\big\{|x_1|, |x_2|\big\}.$$

We now derive an inequality for general finite sums of elements. We will show by induction that the absolute value of a sum of 2^r elements is bounded by 2^r times the maximal absolute value of the summands.

The case $r = 1$ was established above. Assume the statement holds for $r - 1$. Then,

$$\begin{aligned}\left|\sum_{k=1}^{2^r} x_k\right| &\leq 2\max\left\{\left|\sum_{k=1}^{2^{r-1}} x_k\right|, \left|\sum_{k=2^{r-1}+1}^{2^r} x_k\right|\right\} \\ &\leq 2\max\left\{2^{r-1}\max_{1\leq k\leq 2^{r-1}}\big\{|x_k|\big\}, 2^{r-1}\max_{2^{r-1}+1\leq k\leq 2^r}\big\{|x_k|\big\}\right\} \\ &= 2^r\max\big\{|x_1|,\ldots,|x_{2^r}|\big\},\end{aligned}$$

where $x_1, \ldots, x_{2^r} \in F$.

Next, consider a general $n > 1$. Let $r \in \mathbb{N}$ be such that $2^{r-1} < n \leq 2^r$. We can extend any sum over n elements to a sum over 2^r elements by adding $2^r - n$ zeros. Hence,

$$\left|\sum_{k=1}^{n} x_k\right| \leq 2^r\max\big\{|x_1|,\ldots,|x_n|\big\} \leq 2n\max\big\{|x_1|,\ldots,|x_n|\big\}, \tag{1}$$

for any $x_1, \ldots, x_n \in F$.

In particular, this implies that

$$|n| = |\underbrace{1+\ldots+1}_{n \text{ times}}| \leq 2n\cdot|1| \leq 2n \tag{2}$$

for all $n \in \mathbb{N}$.

Now let $y, z \in F$ and $n \in \mathbb{Z}$. We compute:

$$\begin{aligned}|y+z|^n = \big|(y+z)^n\big| &= \left|\sum_{k=0}^{n}\binom{n}{k}y^k z^{n-k}\right| \\ &\leq 2(n+1)\max_{k=0,\ldots,n}\left|\binom{n}{k}y^k z^{n-k}\right| && \text{by (1)} \\ &\leq 2(n+1)\max_{k=0,\ldots,n} 2\binom{n}{k}|y|^k|z|^{n-k} && \text{by (2)} \\ &\leq 4(n+1)\big(|y|+|z|\big)^n.\end{aligned}$$

In the last inequality, we used the trivial observation that a sum of non-negative terms is at least as large as its maximal summand.

Taking the n-th root of both sides and noting that the function $x \mapsto \sqrt[n]{x}$ is increasing on $[0, +\infty)$, we obtain

$$|y+z| \leq \sqrt[n]{4(n+1)}\,\big(|y|+|z|\big).$$

Since this inequality holds for all $n \in \mathbb{Z}$, we can pass to the limit as $n \to +\infty$. Because

$$\lim_{n\to+\infty}\sqrt[n]{4(n+1)} = 1,$$

we conclude that

$$|y+z| \leq |y| + |z|.$$

As $y, z \in F$ were arbitrary, it follows that $|\cdot| = \|\cdot\|^\lambda$ satisfies the triangle inequality.

4. Let $F = \mathbb{Q}(i)$ and $x = 2 - i$. We recall that $\mathcal{O}_F = \mathbb{Z}[i]$, which is a PID (indeed, it is even a Euclidean domain). For any element $a + bi \in \mathcal{O}_F$, the norm is given by

$$N_{F/\mathbb{Q}}(a + bi) = a^2 + b^2,$$

and the norm of a principal ideal generated by such an element coincides with this value. Hence, the norm of x is

$$N_{F/\mathbb{Q}}(x) = 2^2 + (-1)^2 = 5.$$

Since 5 is a rational prime, it follows that x is irreducible, and therefore prime, in $\mathcal{O}_F$. Recall that the $\mathfrak{p}$-adic absolute value of x differs from 1 if and only if $\mathfrak{p}$ appears in the factorization of $(x) = x\mathcal{O}_F$. In particular, the only finite prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ for which $\|x\|_\mathfrak{p} \neq 1$ is the ideal $\mathfrak{p} = (x)$. We compute

$$\|x\|_{(x)} = N\big((x)^{-\operatorname{ord}_{(x)}(x)}\big) = N\big((x)\big)^{-1} = 5^{-1}.$$

Since $\mathbb{Q}(i)$ is an imaginary quadratic field, it possesses a single infinite place, corresponding to the complex embedding

$$\sigma \colon \mathbb{Q}(i) \hookrightarrow \mathbb{C}, \quad a + bi \mapsto a + bi.$$

For this embedding, the corresponding absolute value is

$$\|x\|_\sigma = |\sigma(x)|_\mathbb{C}^2 = |2 - i|^2 = 5.$$

There are no real infinite places of F.

Therefore, only two places $v \in V_F$ satisfy $\|x\|_v \neq 1$, namely the finite place corresponding to (x) and the infinite complex place σ. We may now verify the product formula:

$$\prod_{v \in V_F} \|x\|_v = \|x\|_{(x)} \cdot \|x\|_\sigma = 5^{-1} \cdot 5 = 1.$$

Hence, the product formula holds for $x = 2 - i$ in $F = \mathbb{Q}(i)$.

5. Let G be a topological group and H be a subgroup of G

   (a) For all $g \in G$ the map induced by left multiplication with g is a homeomorphism. In particular, since H is open, every left coset of H in G is open. The union of all left cosets different from H is therefore an open set, so its complement H is closed. Thus an open subgroup is closed.

(b) Conversely, if H is a closed subgroup then each left coset gH is closed. If $[G : H] < \infty$ then there are only finitely many left cosets. The union of finitely many closed sets is closed, so the complement (which is H) is open. Thus a closed subgroup of finite index is open.

(c) If H is open, then every left coset gH is open. By choosing one representative from each coset, we obtain a disjoint open cover of G. If G is compact, every open cover has a finite subcover. Since the cosets in the cover are pairwise disjoint, the open cover can be finite only if there are finitely many cosets. Therefore, $[G : H]$ is finite.