Solutions 7

Class number, Discriminant bounds, Units

*1. Let $K := \mathbb{Q}(\sqrt{-\ell}\,)$ for a prime $\ell \equiv 3 \bmod (4)$. Thus complex conjugation is the non-trivial Galois automorphism of $K/\mathbb{Q}$.

(a) Show that every fractional ideal $\mathfrak{b}$ with $\bar{\mathfrak{b}} = \mathfrak{b}$ is principal.

(b) Deduce that for every fractional ideal $\mathfrak{a}$ we have $[\bar{\mathfrak{a}}] = [\mathfrak{a}^{-1}]$ in $\mathrm{Cl}(\mathcal{O}_K)$.

(c) Prove that for any $a \in K^\times$ with $\mathrm{Nm}_{K/\mathbb{Q}}(a) = 1$ there exists $b \in K^\times$ with $a = \bar{b}b^{-1}$. (*Hilbert 90. Hint:* Try $b = \bar{a} + 1$.)

(d) Show that any fractional ideal $\mathfrak{a}$ with $\mathfrak{a}^2$ principal is equivalent to a fractional ideal $\mathfrak{b}$ with $\bar{\mathfrak{b}} = \mathfrak{b}$.

(e) Conclude that the class number of $\mathcal{O}_K$ is odd.

Solution: By construction K has discriminant $-\ell$ and the ring of integers $\mathbb{Z}[\sqrt{-\ell}\,]$.

(a) Consider the prime factorization $\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i^{\mu_i}$ with distinct maximal ideals $\mathfrak{p}_i$ and exponents $\mu_i \in \mathbb{Z}$. Then $\bar{\mathfrak{b}} = \prod_{i=1}^r \bar{\mathfrak{p}}_i^{\mu_i}$ is the prime factorization of $\bar{\mathfrak{b}}$. By the uniqueness of the prime factorization it follows that every factor $\bar{\mathfrak{p}}_i^{\mu_i}$ must be equal to $\mathfrak{p}_j^{\mu_j}$ for some j. As any product and any quotient of principal ideals is principal, it suffices to prove (a) whenever $\mathfrak{b} = \mathfrak{p} = \bar{\mathfrak{p}}$ or $\mathfrak{b} = \mathfrak{p} \cdot \bar{\mathfrak{p}}$ for a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$.

Any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies above a rational prime p. If this prime is inert in $\mathcal{O}_K$, we have $\mathfrak{p} = (p) = \bar{\mathfrak{p}}$ and are done. If it is split, we have $\mathfrak{p}\mathfrak{p}' = (p)$ for another maximal ideal $\mathfrak{p}'$. As complex conjugation transitively permutes the primes of $\mathcal{O}_K$ above p, it then follows that $\mathfrak{p}' = \bar{\mathfrak{p}}$; hence $\mathfrak{p}\bar{\mathfrak{p}} = (p)$ is principal. Finally, Example 6.2.6 shows that ℓ is the only rational prime that is ramified in $\mathcal{O}_K$. The only prime $\mathfrak{p}$ above ℓ therefore satisfies $\mathfrak{p}^2 = (\ell)$. But $(\sqrt{-\ell}\,)^2 = (-\ell) = (\ell)$ and unique factorization of ideals shows that then $\mathfrak{p} = (\sqrt{-\ell}\,)$; hence we are done in all cases.

(b) For any fractional ideal $\mathfrak{a}$ the ideal $\mathfrak{b} := \mathfrak{a}\bar{\mathfrak{a}}$ satisfies $\bar{\mathfrak{b}} = \mathfrak{b}$ and is therefore principal by (a). Thus $[\bar{\mathfrak{a}}]$ is the inverse of $[\mathfrak{a}]$ in $\mathrm{Cl}(\mathcal{O}_K)$ and therefore equal to $[\mathfrak{a}^{-1}]$.

(c) By assumption we have $a\bar{a} = \mathrm{Nm}_{K/\mathbb{Q}}(a) = 1$. Thus $b := \bar{a} + 1$ satisfies $ab = a\bar{a} + a = 1 + a = \overline{1 + \bar{a}} = \bar{b}$. Thus we are done except if $b = 0$, that is, if $a = -1$. But in that case $b := \sqrt{-\ell}$ does the job.

(d) That $\mathfrak{a}^2$ is principal means that $[\mathfrak{a}^{-1}] = [\mathfrak{a}]$ in $\mathrm{Cl}(\mathcal{O}_K)$. By (b) we thus have $[\bar{\mathfrak{a}}] = [\mathfrak{a}]$ and therefore $\bar{\mathfrak{a}} = a\mathfrak{a}$ for some element $a \in \mathfrak{a}$. Taking norms this implies that

$$\mathrm{Nm}(\mathfrak{a}) \;=\; \mathrm{Nm}(\bar{\mathfrak{a}}) \;=\; |\,\mathrm{Nm}_{K/\mathbb{Q}}(a)| \cdot \mathrm{Nm}(\mathfrak{a})$$

and therefore $|\,\mathrm{Nm}_{K/\mathbb{Q}}(a)| = 1$. But since K is imaginary quadratic, we have $\mathrm{Nm}_{K/\mathbb{Q}}(a) = a\bar{a} > 0$; so we must have $\mathrm{Nm}_{K/\mathbb{Q}}(a) = 1$. Choose $b \in K^\times$ with $a = \bar{b}b^{-1}$ as in (c). Then $\bar{\mathfrak{a}} = a\mathfrak{a} = \bar{b}b^{-1}\mathfrak{a}$ implies that $\mathfrak{b} := b^{-1}\mathfrak{a} = \bar{\mathfrak{b}}$.

(e) If the class number is even, the group $\mathrm{Cl}(\mathcal{O}_K)$ possesses an element of precise order 2. This is represented by a non-principal fractional ideal $\mathfrak{a}$ for which $\mathfrak{a}^2$ is principal. By (d) this is equivalent to a fractional ideal $\mathfrak{b}$ with $\mathfrak{b} = \bar{\mathfrak{b}}$. But then $\mathfrak{b}$ is principal by (a); hence $\mathfrak{a}$ is principal as well, and we have obtained a contradiction. Thus the class number is odd.

2. Determine all totally real cubic number fields with discriminant ± 4.

   Hint: Use a computer algebra system for the actual computation.

   Solution: Let K be such a field with the three real embeddings $\sigma_1, \sigma_2, \sigma_3$. Then by Theorem 4.2.2 for every $t > \sqrt{|d_K|} = 2$ there exists an element $x \in \mathcal{O}_K \smallsetminus \{0\}$ with $|\sigma_1(x)| < t$ and $|\sigma_2(x)|, |\sigma_3(x)| < 1$. As $\mathrm{Nm}_{K/\mathbb{Q}}(x) \in \mathbb{Z} \smallsetminus \{0\}$ we then have $\prod_{i=1}^3 |\sigma_i(x)| \geqslant 1$ and therefore $|\sigma_1(x)| > 1$. In particular $\sigma_1(x) \neq \sigma_2(x)$ and therefore $x \notin \mathbb{Q}$. As $[K/\mathbb{Q}] = 3$ it follows that $K = \mathbb{Q}(x)$. Thus

$$f(X) \;:=\; X^3 + aX^2 + bX + c \;:=\; \prod_{i=1}^{3}(X - \sigma_i(x))$$

   is the minimal polynomial of x over $\mathbb{Q}$. The conditions on $|\sigma_i(x)|$ now imply that $|a| < 2 + t$ and $|b| < 1 + 2t$ and $|c| < t$. As a, b, c are integers, taking t just a little bit larger than 2 we then have $|a| \leqslant 4$ and $|b| \leqslant 5$ and $|c| \leqslant 2$. Since f must be irreducible, we also have $c \neq 0$. After possibly replacing x by $-x$ we can then make $1 \leqslant c \leqslant 2$.

   It remains to study the $9 \cdot 11 \cdot 2 = 198$ possibilities for a, b, c. For this recall that by Proposition 1.7.4 the discriminant of f is the discriminant of $\mathbb{Z}[x]$ and by Proposition 3.2.1 (b) this is equal to $d_K \cdot [\mathcal{O}_K : \mathbb{Z}[x]]^2 = \pm 4 \cdot [\mathcal{O}_K : \mathbb{Z}[x]]^2$. Thus the discriminant of f must be ± 4 times a non-zero square. On the other hand the discriminant is $\prod_{1 \leqslant i < j \leqslant 3}(\sigma_i(x) - \sigma_j(x))^2$ with all terms real; hence it is > 0. Thus the discriminant of f must be 4 times a non-zero square. Using a computer algebra system we compute the discriminant in all 198 cases and find only one that satisfies this condition, namely the polynomial $X^3 - 2X^2 - X + 2 = (X-2)(X^2-1)$. But that is reducible. Therefore there is no totally real cubic number field with discriminant ± 4.

Aliter: By Theorem 4.4.2 we have

$$\sqrt{|d_K|} \geqslant \frac{27}{6} * \left(\frac{\pi}{4}\right)^{3/2} \approx 3.13 > 2.$$

Therefore there is no cubic number field with discriminant ± 4.

3. Work out an analogue of Proposition 5.4.2 in the case $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

   Solution: In this case $\mathcal{O}_K$ consists of the real numbers of the form $a + b\sqrt{d}$ for all $a, b \in \frac{1}{2}\mathbb{Z}$ with $a \equiv b \bmod (2)$. If such a number is a unit, then so is its galois conjugate $a - b\sqrt{d}$, and so their product $a^2 - b^2 d$ is a unit in $\mathbb{Z}$ and therefore equal to ± 1. Conversely, if $a^2 - b^2 d = \pm 1$, then $a + b\sqrt{d}$ is a unit in $\mathcal{O}_K$ with the inverse $\pm(a - b\sqrt{d})$. Thus

   $$\mathcal{O}_K^\times \;=\; \big\{a + b\sqrt{d} \;\big|\; a, b \in \tfrac{1}{2}\mathbb{Z},\ a \equiv b \bmod (2),\ a^2 - b^2 d = \pm 1\big\}.$$

   Next, any unit $u \in \mathcal{O}_K^\times \setminus \{\pm 1\}$ gives rise to four distinct units $\pm u^{\pm 1}$, one lying in each of the intervals between $-\infty, -1, 0, 1, \infty$. Writing $u = a + b\sqrt{d}$, these are the elements $\pm a \pm b\sqrt{d}$ with all four possibilities of signs, the largest of which being $|a| + |b|\sqrt{d}$. Thus

   $$\mathcal{O}_K^\times \cap \mathbb{R}^{>1} \;=\; \big\{a + b\sqrt{d} \;\big|\; a, b \in \tfrac{1}{2}\mathbb{Z}^{>0},\ a \equiv b \bmod (2),\ a^2 - b^2 d = \pm 1\big\}.$$

   The unique fundamental unit $\varepsilon > 1$ is therefore the element $a + b\sqrt{d} \in \mathcal{O}_K^\times \cap \mathbb{R}^{>1}$ as above with the smallest value for a.

4. Prove without number theory that the equation $a^2 - b^2 d = -1$ has infinitely many solutions $(a, b) \in \mathbb{Z}^2$ for $d = 2$, but none for $d = 3$. Explain the answer with algebraic number theory.

   Solution: *Elementary solution using renaissance arithmetic only:* For $d = 2$ we find the solution $(a, b) = (1, 1)$ by trial and error. Given a solution (a, b) with $a, b > 0$, a direct computation shows that $(a^3 + 6ab^2, 3a^2 b + 2b^2)$ is another solution with strictly larger coefficients. Thus there exist infinitely many solutions. For $d = 3$ the equation implies that $a^2 \equiv 2 \bmod (3)$, which is not solvable in $\mathbb{Z}/3\mathbb{Z}$.

   Explanation: Let $K := \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$. In both cases we have $d \not\equiv 1 \bmod (4)$ and hence $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. A general element has norm $\mathrm{Norm}_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - b^2 d$, so we want to find all elements of norm -1. Any such element is a unit in $\mathcal{O}_K^\times$. From the lecture we know that $\mathcal{O}_K^\times = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$ for a fundamental unit $\varepsilon > 1$. Since $\mathrm{Norm}_{K/\mathbb{Q}}$ is multiplicative and $\mathrm{Norm}_{K/\mathbb{Q}}(-1) = 1$, we deduce that

   $$\big\{a + b\sqrt{d} \in \mathcal{O}_K \;\big|\; a^2 - b^2 d = -1\big\} \;=\; \begin{cases} \{\pm\varepsilon^m \mid m \in \mathbb{Z} \text{ odd}\} & \text{if } \mathrm{Norm}_{K/\mathbb{Q}}(\varepsilon) = -1, \\ \varnothing & \text{if } \mathrm{Norm}_{K/\mathbb{Q}}(\varepsilon) = 1. \end{cases}$$

Moreover, by Proposition 5.4.2 we have $\varepsilon = a + b\sqrt{d}$ for $a, b \in \mathbb{Z}^{>0}$ with $a^2 - b^2 d = \pm 1$ and a minimal, which we can find by trial and error.

For $d = 2$ the element $1 + \sqrt{2}$ is a fundamental unit with $\mathrm{Norm}_{K/\mathbb{Q}}(1 + \sqrt{2}\,) = 1^2 - 1^2 \cdot 2 = -1$; hence we are in the first case.

For $d = 3$ the element $2 + \sqrt{3}$ is a unit with $\mathrm{Norm}_{K/\mathbb{Q}}(2 + \sqrt{3}\,) = 2^2 - 1^2 \cdot 3 = 1$. On the other hand $\mathcal{O}_K$ has discriminant $4d = 12$; hence by Proposition 5.4.5 of the lecture the fundamental unit $\varepsilon > 1$ satisfies $\varepsilon \geqslant \frac{\sqrt{12}+\sqrt{12-4}}{2} = \sqrt{3} + \sqrt{2}$. Since $(\sqrt{3} + \sqrt{2}\,)^2 > 2 + \sqrt{3} > 1$, we cannot have $2 + \sqrt{3} = \varepsilon^k$ with an integer $k > 1$, so $2 + \sqrt{3} = \varepsilon$ is already a fundamental unit. Therefore we are in the second case.

5. (a) For any number field K, a subring $\mathcal{O} \subset \mathcal{O}_K$ of finite index is called an *order in* $\mathcal{O}_K$. For any such order prove that $\mathcal{O}^\times$ is a subgroup of finite index in $\mathcal{O}_K^\times$.

   (b) Consider a squarefree integer $d > 1$ with $d \equiv 1 \bmod (4)$, so that $K := \mathbb{Q}(\sqrt{d}\,)$ has the ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}\,]$. Explain the precise relation between $\mathbb{Z}[\sqrt{d}\,]^\times$ and $\mathcal{O}_K^\times$.

Solution: (a) Any ring homomorphism induces a homomorphism for the groups of units. Thus the embedding $\mathcal{O} \hookrightarrow \mathcal{O}_K$ induces an embedding $\mathcal{O}^\times \hookrightarrow \mathcal{O}_K^\times$ of groups. Next set $m := [\mathcal{O}_K : \mathcal{O}]$. Then $m\mathcal{O}_K \subset \mathcal{O}$, so we have an embedding $\mathcal{O}/m\mathcal{O}_K \hookrightarrow \mathcal{O}_K/m\mathcal{O}_K$ and hence a homomorphism of abelian groups $(\mathcal{O}/m\mathcal{O}_K)^\times \hookrightarrow (\mathcal{O}_K/m\mathcal{O}_K)^\times$. From this we deduce that $\mathcal{O}^\times$ is the kernel of the composite homomorphism

$$\mathcal{O}_K^\times \to (\mathcal{O}_K/m\mathcal{O}_K)^\times \twoheadrightarrow (\mathcal{O}_K/m\mathcal{O}_K)^\times \;\big/\; (\mathcal{O}/m\mathcal{O}_K)^\times.$$

Since the target is a finite group, it follows that $[\mathcal{O}_K^\times : \mathcal{O}^\times]$ is finite.

(b) Here we have $m = 2$, and the minimal polynomial of $\omega := \frac{1+\sqrt{d}}{2}$ over $\mathbb{Z}$ is

$$P(X) \;:=\; (X - \tfrac{1+\sqrt{d}}{2}\,)(X - \tfrac{1-\sqrt{d}}{2}\,) \;=\; X^2 - X + \tfrac{1-d}{4}.$$

Hence $\mathcal{O}_K \cong \mathbb{Z}[X]/(P(X))$.

Assume first that $d \equiv 1 \bmod (8)$. Then $P(X) \equiv X(X-1) \bmod (2)$ and hence $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[X]/(X(X-1)) \cong (\mathbb{F}_2)^2$. Thus $(\mathcal{O}_K/2\mathcal{O}_K)^\times = 1$, which by the construction in (a) implies that $\mathcal{O}^\times = \mathcal{O}_K^\times$.

In the other case we have $d \equiv 5 \bmod (8)$. Then $P(X) \equiv X^2 + X + 1 \bmod (2)$, which is irreducible in $\mathbb{F}_2[X]$. Thus $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[X]/(X^2 + X + 1)$ is a field of order 4, and so $(\mathcal{O}_K/2\mathcal{O}_K)^\times$ is a cyclic group of order 3. From the construction in (a) it follows that $\mathbb{Z}[\sqrt{d}\,]^\times$ is a subgroup of $\mathcal{O}_K^\times$ of index dividing 3.

In either case this shows that $\mathbb{Z}[\sqrt{d}\,]^\times$ is a subgroup of $\mathcal{O}_K^\times$ of index 1 or 3. The case $d \equiv 1 \bmod (8)$ shows that the index 1 actually occurs, and the example of $d = 13$ explained in the lecture course shows that the index 3 also occurs.

6. (a) Determine the ring of integers of $K := \mathbb{Q}(\sqrt{5}, i)$.

   (b) Determine $\mathcal{O}_F^\times$ for the subfield $F := \mathbb{Q}(\sqrt{5})$.

   (c) Find a fundamental unit of $\mathcal{O}_K^\times$.

   (d) Show that $|\mu(K)| = 4$ and write down $\mathcal{O}_K^\times$.

Solution:

(a) Consider the subfields $F := \mathbb{Q}(\sqrt{5})$ and $F' := \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. Since $5 \equiv 1 \mod 4$ and $-1 \not\equiv 1 \mod 4$, their discriminants are $\mathrm{disc}(\mathcal{O}_F) = 5$ and $\mathrm{disc}(\mathcal{O}_{F'}) = -4$ and hence coprime. Furthermore, the fields F and F' are linearly disjoint, since $[FF'/\mathbb{Q}] = [K/\mathbb{Q}] = 4 = [F/\mathbb{Q}] \cdot [F'/\mathbb{Q}]$. Therefore Theorem 1.8.3 implies that $\mathcal{O}_K \cong \mathcal{O}_F \otimes_\mathbb{Z} \mathcal{O}_{F'} \cong \mathbb{Z}[\frac{1+\sqrt{5}}{2}, i]$. In particular a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is $1, \frac{1+\sqrt{5}}{2}, i, i\frac{1+\sqrt{5}}{2}$.

(b) By Proposition 5.4.2, the element $\varepsilon := a + b\sqrt{5} \in \mathcal{O}_F$ with minimal $a, b \in \frac{1}{2}\mathbb{Z}^{>0}$ such that $\mathrm{Norm}_{F/\mathbb{Q}}(\varepsilon) = \pm 1$ is a fundamental unit in $\mathcal{O}_F^\times$. By a direct calculation, we verify that $\varepsilon := \frac{1+\sqrt{5}}{2}$ already has norm -1 and hence is a fundamental unit. It follows that $\mathcal{O}_F^\times = \{\pm 1\} \times \varepsilon^\mathbb{Z}$.

(c) The field K has $(r, s) = (0, 2)$ and hence $\mathcal{O}_K^\times = \mu(K) \times \tilde{\varepsilon}^\mathbb{Z}$ for some fundamental unit $\tilde{\varepsilon} \in \mathcal{O}_K^\times$. In view of (b) it follows that $\zeta\tilde{\varepsilon}^n = \varepsilon^{\pm 1}$ for some $n \geqslant 1$ and $\zeta \in \mu(K)$. After possibly replacing $\tilde{\varepsilon}$ with $\tilde{\varepsilon}^{-1}$ and ζ with ζ^{-1}, we may assume that $\zeta\tilde{\varepsilon}^n = \varepsilon$. Writing $\mathrm{Norm}_{K/F}(\tilde{\varepsilon}) = \pm\varepsilon^k$ with $k \in \mathbb{Z}$, we deduce that

$$\varepsilon^2 = \mathrm{Norm}_{K/F}(\varepsilon) = \mathrm{Norm}_{K/F}(\zeta\tilde{\varepsilon}^n) = \pm \mathrm{Norm}_{K/F}(\tilde{\varepsilon})^n = \pm(\pm\varepsilon^k)^n,$$

which implies that $kn = 2$. Suppose that $n = 2$ and hence $k = 1$. Write $\tilde{\varepsilon} = a + b\frac{1+\sqrt{5}}{2} + ci + di\frac{1+\sqrt{5}}{2}$ with $a, b, c, d \in \mathbb{Z}$. Then

$$\pm\tfrac{1+\sqrt{5}}{2} = \pm\varepsilon = \mathrm{Norm}_{K/F}(\tilde{\varepsilon}) = \tilde{\varepsilon}\bar{\tilde{\varepsilon}} = (a^2+b^2+c^2+d^2)+(2ab+b^2+2cd+d^2)\tfrac{1+\sqrt{5}}{2}.$$

Comparing coefficients implies that $a^2 + b^2 + c^2 + d^2 = 0$ and hence $a = b = c = d = 0$. This contradicts the fact that $\tilde{\varepsilon} \neq 0$. Therefore $n = 1$ and $\tilde{\varepsilon} = \zeta^{-1}\varepsilon$ is also a fundamental unit in $\mathcal{O}_K^\times$. Since the fundamental unit of K is only determined up multiplication with an element of $\mu(K)$ and taking its inverse, we conclude that ε is a fundamental unit in $\mathcal{O}_K^\times$.

(d) Let ζ be a generator of $\mu(K)$ and let n be the order of ζ. Then $[\mathbb{Q}(\zeta)/\mathbb{Q}] = \varphi(n)$, where $\varphi(\cdot)$ denotes the Euler φ-function, and this divides $[K/\mathbb{Q}] = 4$. On the other hand, since $i \in K$, we have $n = 2^k m$ with m odd and $k \geqslant 2$ and hence $\varphi(n) = (2^k - 2^{k-1})\varphi(m) = 2^{k-1}\varphi(m)$. Together this leaves only the possibilities $n = 4$, 8, 12.

If $n = 8$, we have $\zeta = \frac{\pm 1 \pm i}{\sqrt{2}}$ and hence $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta + \bar{\zeta}) \subset K$.

If $n = 12$, we have $\zeta^4 = \frac{-1\pm\sqrt{-3}}{2}$ and hence $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta^4) \subset K$.

But the extension $K/\mathbb{Q}$ is galois with a non-cyclic Galois group of order 4; hence by Galois theory it contains precisely three different quadratic subfields. Since $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(i\sqrt{5}) = \mathbb{Q}(\sqrt{-5})$ are all contained in K and non-isomorphic by the classification of quadratic number fields, these are precisely all quadratic subfields of K. Again by the classification of quadratic number fields, none of them is isomorphic to $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-3})$. Thus the cases $n = 8$, 12 are impossible, leaving only $n = 4$.
In conclusion, we have $|\mu(K)| = 4$ and $\mathcal{O}_K^\times = \{\pm 1, \pm i\} \times (\frac{1+\sqrt{5}}{2})^{\mathbb{Z}}$.