Solutions 4

Lattices, Units

1. Suppose that the equation $y^2 = x^5 - 2$ has a solution with $x, y \in \mathbb{Z}$.

   (a) Write down the ring of integers and the class number of $K := \mathbb{Q}(\sqrt{-2})$.

   (b) Show that y is odd and that the two ideals $(y \pm \sqrt{-2})$ of $\mathcal{O}_K$ are coprime.

   (c) Prove that $y + \sqrt{-2}$ is a 5-th power in $\mathcal{O}_K$.

   (d) Deduce a contradiction, proving that the equation has no integer solution.

Solution: (a) Since $-2 \not\equiv 1 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$ and $\mathrm{disc}(\mathcal{O}_K) = -8$. Furthermore, we have $r = 0$ and $s = 1$. To compute the class number of K, we use Minkowski's bound: Every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ with

$$\mathrm{Nm}(\mathfrak{a}) \leqslant \frac{2}{\pi}\sqrt{8} = 1.8\ldots < 2.$$

Since the only ideal in $\mathcal{O}_K$ with norm 1 is the unit ideal, it follows that the class group is trivial and the class number is 1.

(b) Assume, for contradiction, that y is even. Then $x^5 - 2 = y^2 \equiv 0 \bmod 4$. By checking all cases in $\mathbb{Z}/4\mathbb{Z}$, the equation $x^5 - 2 \equiv 0 \bmod 4$ has no solutions. We obtain a contradiction and hence y is odd.

Next the ideal $(y + \sqrt{-2}) + (y - \sqrt{-2})$ contains the element $2\sqrt{-2}$ and hence its square -8. But it also contains the integer $(y + \sqrt{-2})(y - \sqrt{-2}) = y^2 + 2$, which is odd, because y is odd. Thus it contains 1, and so the ideals $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime.

(c) Since the class number is 1, the ring $\mathcal{O}_K$ is a unique factorization domain. Since $x^5 = (y + \sqrt{-2})(y - \sqrt{-2})$, where the factors are coprime, it follows that $y + \sqrt{-2} = u\alpha^5$ for some $\alpha \in \mathcal{O}_K$ and some unit $u \in \mathcal{O}_K^\times$. But here $\mathcal{O}_K^\times = \{\pm 1\}$ has order 2, so we have $u = u^5$ and hence $y + \sqrt{-2} = u^5\alpha^5 = (u\alpha)^5$.

(d) By (c), we can write $y + \sqrt{-2} = (a + b\sqrt{-2})^5$ for some $a, b \in \mathbb{Z}$. The binomial expansion yields

$$y + \sqrt{-2} = (a + b\sqrt{-2})^5 = \big(a^5 - 20a^3b^2 + 20ab^4\big) + \big(5a^4b - 20a^2b^3 + 4b^5\big)\sqrt{-2}.$$

Comparing coefficients shows that $b(5a^4 - 20a^2b^2 + 4b^4) = 1$. This implies that $b = \pm 1$ and hence $5a^4 - 20a^2 + 4 = b$.

If $b = 1$, we have $5a^4 - 20a^2 + 3 = 0$. Thus a^2 is a rational root of the quadratic polynomial $5X^2 - 20X + 3$. But this polynomial has discriminant $(-20)^2 - 4 \cdot 5 \cdot 3 = 20 \cdot 17$, which is not a square in $\mathbb{Q}$, hence it does not possess any rational root.

If $b = -1$, we have $5a^4 - 20a^2 + 5 = 0$. Dividing by 5, we obtain $a^4 - 4a^2 + 1 = 0$. Thus a^2 is a rational root of the quadratic polynomial $X^2 - 4X + 1$. But this polynomial has discriminant 12, which is not a square in $\mathbb{Q}$, hence it does not possess any rational root.

In either case we have obtained a contradiction, proving that $y^2 = x^5 - 2$ has no solutions in $\mathbb{Z}$.

P.S.: Is there a direct proof that does not use algebraic number theory?

2. (a) A *cone* in a real vector space is a subset that is invariant under multiplication by $\mathbb{R}^{>0}$. Let C be a non-empty open convex cone in a finite dimensional real vector space V. Prove that for any complete lattice $\Gamma \subset V$ there exists a point in $\Gamma \cap C$.

   (b) Let K be a totally real number field, i.e., one with $\Sigma := \mathrm{Hom}(K, \mathbb{C}) = \mathrm{Hom}(K, \mathbb{R})$. Let T be any nonempty proper subset of Σ. Show that there exists a unit $\varepsilon \in \mathcal{O}_K^\times$ such that $\sigma(\varepsilon) > 1$ for all $\sigma \in T$ and $0 < \sigma(\varepsilon) < 1$ for all $\sigma \in \Sigma \smallsetminus T$.

Solution: (a) The definition of convexity implies that a subset C is a convex cone if and only if any linear combination of vectors in C with coefficients in $\mathbb{R}^{\geqslant 0}$ and not all zero again lies in C.

As the given subset C is open and non-empty, its measure is positive. Since any proper linear subspace of V has measure 0, we deduce that $\mathrm{span}(C) = V$. Choose a basis $v_1, \ldots, v_n \in C$ of V. Choose a bounded subset $\Phi \subset V$ with $V = \Gamma + \Phi$. Choose $c > 0$ such that $\Phi \subset \{\sum_{i=1}^n x_i v_i \mid \forall i : |x_i| < c\}$. Write $\sum_{i=1}^n c v_i = \gamma + v$ with $\gamma \in \Gamma$ and $v = \sum_{i=1}^n x_i v_i \in \Phi$. By the above characterization of convex cones we deduce that

$$\gamma \;=\; \sum_{i=1}^n (c - x_i) v_i \;\in\; C,$$

because $c - x_i > 0$ for all i. Thus $\gamma \in \Gamma \cap C$, as desired.

(b) By §5, Theorem 10 of the lecture, the subgroup $\Gamma := l \circ j(\mathcal{O}_K^\times)$ is a complete lattice in the vector space $H := \ker(\mathrm{Tr} : (\mathbb{R}^\Sigma)^+ \to \mathbb{R})$. Here $(\mathbb{R}^\Sigma)^+ = \mathbb{R}^\Sigma$, because K is totally real. Consider the subset

$$C \;:=\; \big\{(x_\sigma)_{\sigma \in \Sigma} \in H \;\big|\; \forall \sigma \in T : x_\sigma > 0 \text{ and } \forall \sigma \notin T : x_\sigma < 0\big\}.$$

As this is defined by homogeneous linear strict inequalities, it is an open cone in H. It also contains the element $(a_\sigma)_\sigma$ with

$$a_\sigma := \begin{cases} |\Sigma \smallsetminus T| & \text{if } \sigma \in T, \\ -|T| & \text{if } \sigma \notin T. \end{cases}$$

Thus C is a non-empty open convex cone. By part (a) it follows that $\Gamma \cap C$ contains the point $(\log(|\sigma(\varepsilon)|))_{\sigma\in\Sigma}$ for some $\varepsilon \in \mathcal{O}_K^\times$. The choice of C means that $|\sigma(\varepsilon)| > 1$ for all $\sigma \in T$ and $0 < |\sigma(\varepsilon)| < 1$ for all $\sigma \in \Sigma \smallsetminus T$. The unit ε^2 then satisfies the required condition.

*3. (a) Let M be a bounded subset of a finite dimensional real vector space V. Construct another bounded subset $N \subset V$ such that for any complete lattice $\Gamma \subset V$ with $V = \Gamma + M$, the subset $\Gamma \cap N$ generates Γ.

(b) Deduce that, in principle, for every number field K one can effectively find generators of $\mathcal{O}_K^\times$.

Solution: See for example [Borewicz-Shafarevic: Zahlentheorie (1966) Kapitel II §5.3]. Alternatively, here is an ad hoc solution for (a):

After replacing M by the convex closure of $M + (-M)$ we may assume that M is convex and centrally symmetric. Let $n := \dim_{\mathbb{R}}(V)$. We claim that then $N := \max\{n, 2\}M$ does the job.

First let Γ' be the subgroup generated by $\Gamma \cap 2M$. For any $\gamma \in \Gamma$ write $\frac{\gamma}{2} = \delta + m$ with $\delta \in \Gamma$ and $m \in M$. Then $2m = \gamma - 2\delta \in \Gamma \cap 2M \subset \Gamma'$; hence $\gamma \in 2\Gamma + \Gamma'$. Since γ was arbitrary, it follows that the composite homomorphism $\Gamma' \hookrightarrow \Gamma \twoheadrightarrow \Gamma/2\Gamma$ is surjective. But Γ is a lattice of rank n, and so Γ' is a sublattice of some rank $n' \leqslant n$. We thus have a surjective homomorphism $\mathbb{Z}^{n'} \cong \Gamma' \twoheadrightarrow \Gamma/2\Gamma \cong (\mathbb{Z}/2\mathbb{Z})^n$, which implies that $n' = n$.

We can therefore choose $\mathbb{R}$-linearly independent elements $\gamma_1, \ldots, \gamma_n \in \Gamma \cap 2M$. With $\Gamma'' := \bigoplus_{i=1}^n \mathbb{Z}\gamma_i$ we then have $V = \bigoplus_{i=1}^n \mathbb{R}\gamma_i = \Gamma'' + \Phi$ for the subset $\Phi := \sum_{i=1}^n [-\frac{1}{2}, \frac{1}{2}]\gamma_i$. Here the fact that $\gamma_i \in 2M$ and the assumption that M is convex and centrally symmetric implies that $[-\frac{1}{2}, \frac{1}{2}]\gamma_i \subset M$. Again by the convexity of M we therefore have $\Phi \subset nM \subset N$, and so $V = \Gamma'' + N$. Finally this implies that $\Gamma = \Gamma'' + (\Gamma \cap N)$. Since Γ'' is already generated by a subset of $\Gamma \cap 2M \subset \Gamma \cap N$, it follows that Γ is generated by $\Gamma \cap N$, as desired.

4. (a) For any number field K, any 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 $\mathcal{O}^\times \hookrightarrow \mathcal{O}_K^\times$ as a subgroup. Next abbreviate $m := [\mathcal{O}_K : \mathcal{O}]$. 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

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

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.

5. Show that the equation $a^2 - b^2d = -1$ 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 $(a^3+6ab^2, 3a^2b+2b^2)$ 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 $d \not\equiv 1 \bmod 4$, hence we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. The norm of a general element is $\mathrm{Nm}_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - b^2d$. Hence, we want to find all elements of norm -1. Any such element is a unit in $\mathcal{O}_K^\times$. By §5 Cor. 14 of the lecture, we have $\mathcal{O}_K^\times = \{\pm1\} \times \varepsilon^{\mathbb{Z}}$ for a fundamental unit $\varepsilon > 1$. Since $\mathrm{Nm}_{K/\mathbb{Q}}$ is multiplicative and $\mathrm{Nm}_{K/\mathbb{Q}}(-1) = 1$, we deduce that

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

Moreover, by §5 Prop. 15 we have $\varepsilon = a + b\sqrt{d}$ for $a, b \in \mathbb{Z}^{>0}$ with $a^2 - b^2d = \pm1$ and a minimal, which we can find by trial and error.

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

For $d = 3$ the element $2+\sqrt{3}$ is a unit with $\mathrm{Nm}_{K/\mathbb{Q}}(2+\sqrt{3}) = 2^2 - 1^2 \cdot 3 = 1$. On the other hand $\mathcal{O}_K$ has discriminant $4d = 12$; hence by §5 Prop.17 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.