Algebraic Number Theory - Assignment 12

Matteo Durante, 2303760, Leiden University

12th December 2018

Exercise: compute the invariants of your "favorite" (and maximally impressive) number field $\mathbb{K}$.

We shall study the invariants of $\mathbb{K} = \mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(f)$, where $f = X^3 - 65$ and $\alpha = \sqrt[3]{65}$. This is an interesting number ring because it is the first one defined by a polynomial of the form $X^3 - a$, $a \in \mathbb{N}$, whose Picard group is not cyclic.

Since f has degree 3 and it has no integer roots, it is irreducible in $\mathbb{Q}[X]$ and $\mathbb{K}$ really is a number field. Since it has discriminant $\Delta(f) = -114075 < 0$, it has one real root and two complex, hence $\mathbb{K}$ has one real and two complex embeddings. We fix the real one and hence the real representation(s) of our ring(s).

We shall start looking for its ring of integers by considering $R = \mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(f)$, an order of rank 3 and with $\Delta(R) = \Delta(f) = -114075 = -3^3 \cdot 5^2 \cdot 13^2$.

However, by [1, ex. 3.15], R is a Dedekind ring and hence $R = \mathcal{O}_{\mathbb{K}}$ (remember that we have already fixed a representation for all of our rings).

We now proceed to compute $\mathrm{Pic}(\mathcal{O}_{\mathbb{K}})$, the distinguishing invariant of our number field.

First of all, remembering that $r = s = 1$, $M_{\mathbb{K}} \approx 95.56$. To compute the Picard group, it is useful to look at the primes factorizing ideals whose norm is smaller than it.

To do this, we construct the following table (notice that the last column comes from the table which follows this one and [1, thm. 7.2], however we include it for compactness):

k	$f(k)$	factor $f(k)$	factor $(k-\alpha)$
-18	-5897	$-1\cdot 5897$	$\mathfrak{p}_{5897}$
-17	-4978	$-1\cdot 2\cdot 19\cdot 131$	$\mathfrak{p}_2\mathfrak{r}_{19}$
-16	-4161	$-1\cdot 3\cdot 19\cdot 73$	$\mathfrak{p}_3\mathfrak{q}_{19}\mathfrak{q}_{73}$
-15	-3440	$-1\cdot 2^4\cdot 5\cdot 43$	$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{q}_{43}$
-14	-2809	$-1\cdot 53^2$	$\mathfrak{p}_{53}^2$
-13	-2262	$-1\cdot 2\cdot 3\cdot 13\cdot 29$	$\mathfrak{p}_3\mathfrak{p}_{13}\mathfrak{p}_{29}$
-12	-1793	$-1\cdot 11\cdot 163$	$\mathfrak{p}_{11}\mathfrak{p}_{163}$
-11	-1396	$-1\cdot 2^2\cdot 349$	$\mathfrak{p}_2^2\mathfrak{p}_{349}$
-10	-1065	$-1\cdot 3\cdot 5\cdot 71$	$\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{71}$
-9	-794	$-1\cdot 2\cdot 397$	$\mathfrak{p}_2\mathfrak{p}_{397}$
-8	-577	$-1\cdot 577$	$\mathfrak{p}_{577}$
-7	-408	$-1\cdot 2^3\cdot 3\cdot 17$	$\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_{17}$
-6	-281	$-1\cdot 281$	$\mathfrak{p}_{281}$
-5	-190	$-1\cdot 2\cdot 5\cdot 19$	$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{19}$
-4	-129	$-1\cdot 3\cdot 43$	$\mathfrak{p}_3\mathfrak{p}_{43}$
-3	-92	$-1\cdot 2^2\cdot 23$	$\mathfrak{p}_2^2\mathfrak{p}_{23}$
-2	-73	$-1\cdot 73$	$\mathfrak{p}_{73}$
-1	-66	$-1\cdot 2\cdot 3\cdot 11$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{11}$
0	-65	$-1\cdot 5\cdot 13$	$\mathfrak{p}_5\mathfrak{p}_{13}$
1	-64	$-1\cdot 2^6$	$\mathfrak{p}_2^6$
2	-57	$-1\cdot 3\cdot 19$	$\mathfrak{p}_3\mathfrak{r}_{19}$
3	-38	$-1\cdot 2\cdot 19$	$\mathfrak{p}_2\mathfrak{q}_{19}$
4	-1	-1	(1)
5	60	$2^2\cdot 3\cdot 5$	$\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_5$
6	151	151	$\mathfrak{p}_{151}$
7	278	$2\cdot 139$	$\mathfrak{p}_2\mathfrak{p}_{139}$
8	447	$3\cdot 149$	$\mathfrak{p}_3\mathfrak{p}_{149}$
9	664	$2^3\cdot 83$	$\mathfrak{p}_2^3\mathfrak{p}_{83}$
10	935	$5\cdot 11\cdot 17$	$\mathfrak{p}_5\mathfrak{p}_{11}\mathfrak{p}_{17}$
11	1266	$2\cdot 3\cdot 211$	$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{211}$
12	1663	1663	$\mathfrak{p}_{1663}$
13	2132	$2^2\cdot 13\cdot 41$	$\mathfrak{p}_2^2\mathfrak{p}_{13}\mathfrak{p}_{41}$
14	2679	$3\cdot 19\cdot 47$	$\mathfrak{p}_3\mathfrak{p}_{19}\mathfrak{p}_{47}$
15	3310	$2\cdot 5\cdot 331$	$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{331}$
16	4031	$29\cdot 139$	$\mathfrak{p}_{29}\mathfrak{p}_{139}$
17	4848	$2^4\cdot 3\cdot 101$	$\mathfrak{p}_2^4\mathfrak{p}_3\mathfrak{p}_{101}$
18	5767	$73\cdot 79$	$\mathfrak{r}_{73}\mathfrak{r}_{79}$

The list $\{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89\}$ contains every prime we are interested in. However, the ones in the list $\{7,31,37,59,61,67,89\}$ are missing, thus we shall only consider $\{2,3,5,11,13,17,19,23,29,41,43,47,53,71,73,79,83\}$.

We have the following factorizations of f modulo these primes, which give us factorizations of the corresponding (p):

2	$(X+1)(X^2+X+1)$	$\mathfrak{p}_2\mathfrak{p}_4$
3	$(X+1)^3$	$\mathfrak{p}_3^3$
5	X^3	$\mathfrak{p}_5^3$
11	$(X+1)(X^2+10X+1)$	$\mathfrak{p}_{11}\mathfrak{p}_{11^2}$
13	X^3	$\mathfrak{p}_{13}^3$
17	$(X+7)(X^2+10X+15)$	$\mathfrak{p}_{17}\mathfrak{p}_{17^2}$
19	$(X+5)(X+16)(X+17)$	$\mathfrak{p}_{19}\mathfrak{q}_{19}\mathfrak{r}_{19}$
23	$(X+3)(X^2+20X+9)$	$\mathfrak{p}_{23}\mathfrak{p}_{23^2}$
29	$(X+13)(X^2+16X+24)$	$\mathfrak{p}_{29}\mathfrak{p}_{29^2}$
41	$(X+28)(X^2+13X+5)$	$\mathfrak{p}_{41}\mathfrak{p}_{41^2}$
43	$(X+4)(X+15)(X+24)$	$\mathfrak{p}_{43}\mathfrak{q}_{43}\mathfrak{r}_{43}$
47	$(X+33)(X^2+14X+8)$	$\mathfrak{p}_{47}\mathfrak{p}_{47^2}$
53	$(X+14)(X^2+39X+37)$	$\mathfrak{p}_{53}\mathfrak{p}_{53^2}$
71	$(X+10)(X^2+61X+29)$	$\mathfrak{p}_{71}\mathfrak{p}_{71^2}$
73	$(X+2)(X+16)(X+55)$	$\mathfrak{p}_{73}\mathfrak{q}_{73}\mathfrak{r}_{73}$
79	$(X+37)(X+60)(X+61)$	$\mathfrak{p}_{79}\mathfrak{q}_{79}\mathfrak{r}_{79}$
83	$(X+74)(X^2+9X+81)$	$\mathfrak{p}_{83}\mathfrak{p}_{83^2}$

Notice that $11^2 > M_{\mathbb{K}}$, thus the only primes relevant to the computation of the Picard group are those of prime norm $p < M_{\mathbb{K}}$. Furthermore, we see that the only primes among these appearing in our previous table are $\mathfrak{p}_2 = (2, 1+\alpha), \mathfrak{p}_3 = (3, 1+\alpha), \mathfrak{p}_5 = (5, \alpha), \mathfrak{p}_{11} = (11, 1+\alpha), \mathfrak{p}_{17} = (17, 7+\alpha), \mathfrak{p}_{19} = (19, 5+\alpha), \mathfrak{q}_{19} = (19, 16+\alpha), \mathfrak{r}_{19} = (19, 17+\alpha), \mathfrak{p}_{23} = (23, 3+\alpha), \mathfrak{p}_{29} = (29, 13+\alpha), \mathfrak{p}_{41} = (41, 28+\alpha), \mathfrak{p}_{43} = (43, 4+\alpha), \mathfrak{q}_{43} = (43, 15+\alpha), \mathfrak{p}_{47} = (47, 33+\alpha), \mathfrak{p}_{53} = (53, 14+\alpha), \mathfrak{p}_{73} = (73, 2+\alpha), \mathfrak{q}_{73} = (73, 16+\alpha), \mathfrak{r}_{73} = (73, 55+\alpha), \mathfrak{r}_{79} = (79, 61+\alpha), \mathfrak{p}_{83} = (83, 74+\alpha)$.

Observe that $\mathfrak{p}_5 = (5-\alpha)\mathfrak{p}_2^{-2}\mathfrak{p}_3^{-1}, \mathfrak{p}_{11} = (1+\alpha)\mathfrak{p}_2^{-1}\mathfrak{p}_3^{-1}, \mathfrak{p}_{17} = (7+\alpha)\mathfrak{p}_2^{-3}\mathfrak{p}_3^{-1}, \mathfrak{p}_{19} = (5+\alpha)\mathfrak{p}_2^{-1}\mathfrak{p}_5^{-1}, \mathfrak{q}_{19} = (3-\alpha)\mathfrak{p}_2^{-1}, \mathfrak{r}_{19} = (2-\alpha)\mathfrak{p}_3^{-1}, \mathfrak{p}_{23} = (3+\alpha)\mathfrak{p}_2^{-2}, \mathfrak{p}_{29} = (13+\alpha)\mathfrak{p}_3^{-1}\mathfrak{p}_{13}^{-1}, \mathfrak{p}_{41} = (13-\alpha)\mathfrak{p}_2^{-2}\mathfrak{p}_{13}^{-1}, \mathfrak{p}_{43} = (4+\alpha)\mathfrak{p}_3^{-1}, \mathfrak{p}_{47} = (14-\alpha)\mathfrak{p}_3^{-1}\mathfrak{p}_{19}^{-1}, \mathfrak{p}_{73} = (2+\alpha), \mathfrak{q}_{73} = (16+\alpha)\mathfrak{p}_3^{-1}\mathfrak{q}_{19}^{-1}, \mathfrak{r}_{73} = (73)\mathfrak{p}_{73}^{-1}\mathfrak{q}_{73}^{-1}$ (to verify this, look at the line indicated by the k in the $(k-\alpha)$ which appears at the right of the equality sign).

We get that we only have to consider the following ones: $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_{53}$.

In what follows we shall use the fact that, being in a Dedekind ring, the norm map is multiplicative.

Hopefully, the generating classes are the ones of $\mathfrak{p}_2$ and $\mathfrak{p}_3$, whose order divides respectively 6 and 3. Furthermore, notice that $\mathfrak{p}_{53}$ has order dividing 2, thus it should lie in $[\mathfrak{p}_2^3]$.

By computing, $\mathfrak{p}_2^3\mathfrak{p}_{53} = (424, 279+\alpha, 175+\alpha^2)$. Since $11 - 3\alpha = 117 \cdot 424 - 178(279+\alpha) + \alpha(175+\alpha^2) \in \mathfrak{p}_2^3\mathfrak{p}_{53}$ has norm $2^3 \cdot 53$, $\mathfrak{p}_2^3\mathfrak{p}_{53} = (11 - 3\alpha)$ and thus we may disregard $\mathfrak{p}_{53}$.

Since in $\mathrm{Pic}(\mathcal{O}_{\mathbb{K}})$ the classes of $\mathfrak{p}_2$ and $\mathfrak{p}_3$ have order dividing 6 and 3 respectively and not having found any relation between the two of them, we may conjecture that the Picard group is isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, where each class is given by $a[\mathfrak{p}_2] + b[\mathfrak{p}_3]$, $0 \leq a < 6, 0 \leq b < 3$.

If we can prove that $\mathfrak{p}_2, \mathfrak{p}_3$ are indeed independent and the orders are $6, 3$, then we will have that $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a subgroup of $\mathrm{Pic}(\mathcal{O}_{\mathbb{K}})$, which will then have order ≥ 18.

We start by showing that $\mathfrak{p}_2^2$ is not principal. Indeed it has norm 4 and, knowing that $N(a + b\alpha + c\alpha^2) = (a + b\alpha_0 + c\alpha_0^2)(a + b\alpha_1 + c\alpha_1^2)(a + b\alpha_2 + c\alpha_2^2) = \ldots = a^3 + 65b^3 + 65^2c^3 - 3 \cdot 65abc$ (it's just a matter of using Vieta's formulas), its generating element would have to satisfy $a^3 \equiv \pm 4 \mod 13$, which is not possible, hence the thesis. Furthermore, we get that $\mathfrak{p}_2$ itself is not principal.

We proceed with $\mathfrak{p}_2^3$. A generating element b would be s.t. $b^2 = u(1-\alpha)$, where u is a unit and hence $u = \pm(4-\alpha)^n$ (look at the discussion concerning units in the following section). Consider a homomorphism $\mathbb{Z}[\alpha] \to \mathbb{F}_{41}$ sending α to 13, a root of f in $\mathbb{F}_{41}$. Then, $b^2 = u(1-\alpha)$ would go to $\pm 9^n \cdot 12 = \pm 3^{2n+1} \cdot 2^2$. However, ± 3 is not a square residue in $\mathbb{F}_{41}$, hence we reach a contradiction.

We prove that $\mathfrak{p}_3$ is not principal, s.t. then $[\mathfrak{p}_3]$ will have order 3. Again, a generating element would have to satisfy $a^3 \equiv \pm 3 \mod 13$, which is not possible and hence the thesis.

We prove that $\mathfrak{p}_2^2\mathfrak{p}_3$ is not principal. If it were, there would be a generating element b s.t. $b^3 = 3u(1-\alpha)$, where $u = \pm(4-\alpha)^n$ is a unit. Consider now the homomorphism $\mathbb{Z}[\alpha] \to \mathbb{F}_{19}$ sending α to -16 (i.e. 3). Then, b^3 is sent to ± 6, which is absurd because it is not a cubic residue modulo 19.

We prove that $\mathfrak{p}_2^4\mathfrak{p}_3$ is not principal. Indeed, if it was, then it would be generated by an element $a + b\alpha + c\alpha^2$ s.t. $a^3 \equiv \pm 2^4 \cdot 3 \equiv \pm 9 \mod 13$. However, ± 9 is not a cubic residue in $\mathbb{F}_{13}$, hence this is not possible.

Now we try to compute $\mathcal{O}_{\mathbb{K}}^*$. By [1, thm. 5.13], since $r > 0$, we have that it is $\cong < -1 > \times < \eta_0 >$, where $\eta_0 > 1$ (remember that we have already fixed an embedding).

By looking at the first table, we see that $\eta = (4-\alpha)^{-1} = 16 + 4\alpha + \alpha^2 > 1$ is a unit because $(4-\alpha) = (1)$.

Since $Reg(\mathcal{O}_{\mathbb{K}}) = \log(\eta_0) \geq \frac{1}{3}\log(\frac{114075-24}{4}) \approx 3.41$ by [1, ex. 5.21] and $\log(\eta) \approx 3.87$, having $\eta = \eta_0^n$ for some $n \in \mathbb{N}_{>0}$, $1 \leq n = \frac{\log(\eta)}{\log(\eta_0)} < 2$, thus $n = 1$ and η is a fundamental unit.

We may now compute the residue at 1 of the Dedekind zeta function of this ring to conclude that what we have previously found is indeed the Picard group.

Remembering that this residue equals $\Pi_p E(p)$ and $E(p)^{-1} = \frac{\Pi_{\mathfrak{p}|p}(1-N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p})^{-1})}{1-p^{-1}}$, we may compute it explicitly for the primes $p < 1000000$ and then get a good approximation of the residue of the Dedekind zeta function.

We know that, given a prime p which doesn't ramify, we have that (p) either factorizes as $\mathfrak{p}_p\mathfrak{q}_p\mathfrak{r}_p$ or $\mathfrak{p}_p\mathfrak{p}_{p^2}$ or is inert, depending on the irreducible factors of $f \mod p$.

In the first case, $E(p)^{-1} = \frac{(1-p^{-1})^3}{1-p^{-1}} = (1-p^{-1})^2$, in the second one $E(p)^{-1} = \frac{(1-p^{-1})(1-(p^2)^{-1})}{1-p^{-1}} = 1 - p^{-2}$ and in the third one $E(p)^{-1} = \frac{1-(p^3)^{-1}}{1-p} = 1 + p^{-1} + p^{-2}$. For the primes which ramify, we have that $E(p) = 1$.

Multiplying them, we get that $\Pi_p E(p) \approx 1.298$. Confronting this with $\frac{2^1(2\pi)^1 \cdot 18 \cdot 3.87}{2 \cdot \sqrt{|-114075|}} \approx 1.296$, we can confirm that the Picard group is indeed the one we have found and conclude.

References

[1] P. Stevenhagen, *Number Rings*, 2017.