# Solutions to Sheet 5

## Exercise 1

Let $m \in \mathbb{Z} \setminus \{0, \pm 1\}$ be a squarefree integer. Using Eisenstein's criterion, one shows that $X^3 - m \in \mathbb{Q}[X]$ is irreducible. Let $K = \mathbb{Q}[X]/(X^3 - m)$ and write $x$ for the image of $X$ in $K$, so that $x^3 = m$. Let $z = a + bx + cx^2$. We know that $\mathrm{N}_{K/\mathbb{Q}}(z) = a^3 + mb^3 + m^2c^3 + 3mabc$ from (ii) and $3\mathcal{O}_K \subset \mathbb{Z}[x]$ from (iv).

(v) Using (ii) and (iv), show that $\mathcal{O}_K = \mathbb{Z}[x]$ if $3 \nmid m$ and $m \not\equiv \pm 1 \mod 9$.

**Solution.**

(v) Let $z = a + bx + cx^2 \in \mathcal{O}_K$. We already know that $3z \in \mathbb{Z}[x]$, so the only thing that can go wrong is that there are (single) 3's in the denominator's of $a$, $b$ or $c$. We also know that $\mathrm{N}_{K/\mathbb{Q}}(3z) = 3^{[K:\mathbb{Q}]}\,\mathrm{N}_{K/\mathbb{Q}}(z) \in 27\mathbb{Z}$. Write $a' = 3a$, $b' = 3b$ and $c' = 3c$. Now $a', b', c' \in \mathbb{Z}$ and we obtain

$$a'^3 + mb'^3 + m^2c'^3 - 3ma'b'c' \equiv 0 \pmod{27}.$$

One can check that there are no non-trivial solutions (that is, no solutions without each number divisible by 3). Below (and in the github repository) is a snippet of python3 code that does exactly that.

```
# solutions.py

MOD = 27

# Use a,b,c in place of a',b',c'.
def f(a,b,c,m):
    return ( a*a*a + m*b*b*b + m*m*c*c*c - 3*m*a*b*c ) % MOD

solutions_found = False
for a in range(MOD):
    for b in range(MOD):
        for c in range(MOD):
            # skip pairs with everything divisible by 3
            if a % 3 == 0 and b%3 == 0 and c%3 == 0:
                continue

            for m in range(MOD):
                # skip pairs with m == +-1 mod 9
                # or 3|m.
                if (m+1)%9 == 0 or (m-1)%9 == 0 or m%3 == 0:
                    continue

                if f(a,b,c,m) == 0:
                    solutions_found = True
                    print(f"Solution found! (a,b,c,m) = ({a},{b},{c},{m})")

if solutions_found == False:
    print("There are no solutions.")
```

Executing this, we find that there are no solutions.

Alternatively, looking at the equivalence mod 3 gives conditions to $a', b', c'$ (mod 3), and one can deduce that there are only trivial solutions that way.

## Exercise 2

To the right, you do not see the flag of Nepal. The ration of its height to its width is equal to a number $\alpha \in \mathbb{R}$ such that $K \coloneqq \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{59 - 24\sqrt{2}})$.

(iv) Using a computer, one finds that

$$\Delta_{K/\mathbb{Q}}\left(1, \alpha, \sqrt{2}, \sqrt{2}\alpha\right) = 2^{10} \cdot 17 \cdot 137$$

Deduce from this together with (iii) that $2\mathcal{O}_K \subset \mathcal{O}_F[\beta] = \mathcal{O}_F + \beta\mathcal{O}_F$.

(v) Let $\xi = x + y\beta \in \mathcal{O}_K$ with $x, y \in F$. We know from $(iv)$ that $x, y \in \frac{1}{2}\mathcal{O}_F = \frac{1}{2}\mathbb{Z} + \frac{1}{\sqrt{2}}\mathbb{Z}$. Deduce from $\mathrm{N}_{K/F}(\xi) \in \mathcal{O}_F$ that $x^2 - \sqrt{2}xy - y^2 \in \mathcal{O}_F$.

(vi) Using (iv) and (v), show that $\mathcal{O}_K = \mathcal{O}_F[\beta]$.

**Solution.**

(iv) There are quite a few symbols flying around, let's collect them. We have $\alpha = \sqrt{59 - 24\sqrt{2}}$, $\beta = \frac{\alpha - 1}{\sqrt{2}}$, in particular $\mathcal{O}_F[\alpha] \subset \mathcal{O}_F[\beta]$. We defined $F = \mathbb{Q}(\sqrt{2})$, and we know from the lecture that $\mathcal{O}_F = \mathbb{Z}[\sqrt{2}]$. Part (iii) showed that $2\alpha^2\mathcal{O}_K \subset \mathcal{O}_F[\beta]$. We know that

$$\Delta_{K/\mathbb{Q}}(1, \alpha, \sqrt{2}, \sqrt{2}\alpha)\mathcal{O}_K \subset \mathbb{Z} + \alpha\mathbb{Z} + \sqrt{2}\mathbb{Z} + \sqrt{2}\alpha\mathbb{Z} = \mathcal{O}_F + \alpha\mathcal{O}_F \subset \mathcal{O}_F[\beta].$$

Write $M \coloneqq \mathbb{Z} + \alpha\mathbb{Z} + \sqrt{2}\mathbb{Z} + \sqrt{2}\alpha\mathbb{Z}$. Basically by the results about the interplay of linear transformations and the discriminant, we find (this is also in the lecture)

$$\Delta_{K/\mathbb{Q}}(1, \alpha, \sqrt{2}, \sqrt{2}\alpha) = [\mathcal{O}_K : M]^2 \Delta_{K/\mathbb{Q}} = 2^{10} \cdot 17 \cdot 137.$$

From this we find $[\mathcal{O}_K : M] \mid 2^5 = 32$. Let $J \subset \mathcal{O}_F$ be the ideal defined by $\{r \in \mathcal{O}_F \mid \forall x \in \mathcal{O}_K : rx \in \mathcal{O}_F[\beta]\}$. Part (iii) and the above show that $(32, 2\alpha^2) \subset J$. Now we just have to calculate:

$$\begin{aligned}(32, 2\alpha^2) = (32, 2(59 - 24\sqrt{2})) &= (32, 4(59 - 24\sqrt{2}), 2\alpha^2) \\ &= (32, 4 \cdot 59 - 3 \cdot 32\sqrt{2}, 2\alpha^2) = (4, 2(59 - 24\sqrt{2})) = (2)\end{aligned}$$

Hence $2 \subset (J)$ and we are done.

(v) This is just a matter of calculating $\mathrm{N}_{K/F}(x + y\beta)$. First note that $K = F(\alpha)$ is of degree 2, with Galois group generated by the morphism generated by $\alpha \mapsto -\alpha$. We have

$$\sigma(x + y\beta) = x + y\sigma\left(\tfrac{\alpha - 1}{2}\right) = x - y\tfrac{1}{\sqrt{2}} - y\tfrac{\alpha}{\sqrt{2}}$$

and one calculates that

$$\begin{aligned}\mathrm{N}_{K/F}(x + y\beta) = (x - \tfrac{y}{\sqrt{2}})^2 - \tfrac{\alpha^2 y^2}{2} &= x^2 - \sqrt{2}xy + \tfrac{y^2}{2} - \tfrac{(59 - 24\sqrt{2})}{2}y^2 \\ &= \underbrace{x^2 - \sqrt{2}xy - y^2}_{\therefore \in \mathcal{O}_F} - \underbrace{28y^2 + \tfrac{24}{\sqrt{2}}y^2}_{\in \mathcal{O}_F}.\end{aligned}$$

Here we used that $y \in \frac{1}{2}(\mathbb{Z} + \sqrt{2}\mathbb{Z})$, so that $y^2$ has at most a four in its denominator.

(vi) The inclusion $\mathcal{O}_F[\beta] \subset \mathcal{O}_K$ is already known. For the reverse inclusion, take any $\xi = x+y\beta$ as in (v). Now we know that $x^2 - \sqrt{2}xy - y^2 \in \mathcal{O}_F = \mathbb{Z} + \sqrt{2}\mathbb{Z}$. Write $2x = x_1 + \sqrt{2}x_2$ and $2y = y_1 + \sqrt{2}y_2$. The integrality condition yields two equations modulo 4, as we have

$$\mathrm{N}_{K/F}(2\xi) = x_1^2 + 2x_2^2 - 2(x_1y_2 + x_2y_1) - y_1^2 - 2y_2^2 + \sqrt{2}\Big(2x_1x_2 - x_1y_1 - 2x_2y_2 - 2y_1y_2\Big) \in 4(\mathbb{Z} + \sqrt{2}\mathbb{Z}).$$

One can again ask a computer if this has a non-trivial solution, and the computer will say `no`:

```
# solutions2.py

def eq1(x1, x2, y1, y2):
    return (x1*x1 + 2*x2*x2 - 2*(x1*y2 + x2*y1) - y1*y1 - 2*y2*y2) % 4
def eq2(x1, x2, y1, y2):
    return (2*(x1*x2 - y1*y2) - x1*y1 - 2*x2*y2) % 4

solutions_found = False
for x1 in range(4):
    for x2 in range(4):
        for y1 in range(4):
            for y2 in range(4):
                if x1%2 == 0 and x2%2 == 0 and y1%2 == 0 and y2%2 == 0:
                    continue
                if eq1(x1,x2,y1,y2) == 0 and eq2(x1,x2,y1,y2) == 0:
                    solutions_found = True
                    print(f"Solution found! (x1,x2,y1,y2) = ({x1},{x2},{y1},{y2})")

if solutions_found == False:
    print("no")
```

## Exercise 3

Find an integral domain $R$ and a non-zero prime ideal $\mathfrak{P} \subset R$ such that $\mathfrak{P}^{-1} = R$.

**Solution.** First remember what the inverse ideal was. If $I \subset R$ is any ideal, then $I^{-1} = \{r \in \mathrm{Frac}(R) \mid \forall x \in I : rx \in R\}$. From here we can directly see that $\mathfrak{P}$ cannot be a principal Ideal; if $\mathfrak{P} = (p)$ for some $p \in R$, $\mathfrak{P}^{-1}$ would simply be given by $\mathfrak{P}^{-1} = p^{-1}R \neq R$. Similarly, it was part of the lecture that for any prime $\mathfrak{P}$ of a Dedekind domain $R$, $\mathfrak{P}^{-1} \supsetneq R$.[1] So let's consider the simplest non-principal ideal we know: The ideal $(x, y) \subset k[x, y]$ for some field $k$. It is prime (even maximal, why?[2]), and we find that

$$(x, y)^{-1} = \{r \in k(x, y) \mid rx \in k[x, y] \wedge ry \in k[x, y]\} = x^{-1}k[x, y] \cap y^{-1}k[x, y] = k[x, y].$$

Thus, we have found an example.

## Exercise 4

Let $I$ denote the ideal $(2, 1 + \sqrt{-3})$ of the ring $\mathbb{Z}[\sqrt{-3}]$.

[1] Thanks to Prof. Dill for pointing this out!
[2] Because $k[x, y]/(x, y) \cong k$ is a field.

1. Show that $I \neq (2)$.

2. Show that $I^2 = 2I$.

$\mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain.

**Solution.**

1. There are many ways to solve this, but let's look at residual rings, that is, calculate $\mathbb{Z}[\sqrt{-3}]/I$. We have $\mathbb{Z}[\sqrt{-3}] \cong \mathbb{Z}[X]/(X^2 - 3)$, hence

$$\mathbb{Z}[\sqrt{-3}]/I \cong \mathbb{Z}[X]/(X^2 - 3, 2, 1 + X) \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 - 1, X + 1) \cong (\mathbb{Z}/2\mathbb{Z}).$$

Meanwhile, we have

$$\mathbb{Z}[\sqrt{-3}]/(2) \cong (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 - 1) \cong (\mathbb{Z}/2\mathbb{Z})[X]/(1 - X)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}.$$

Here, the last ismorphism is to be taken as an isomorphism of modules. In particular, we find $I \neq (2)$, as the corresponding residue rings are not isomorphic.

2. We have $I^2 = (4, 2+2\sqrt{-3}, -2+2\sqrt{-3})$, which can be seen simply by multiplying generators. But the last generator is the difference between the first two, so we find

$$I^2 = (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) = 2I.$$

Note that this in particular implies that factorization of an ideal into prime factors is not unique: $I$ is prime, and one factorization is given by $I^2 = I \cdot I$. But we have $I \cdot I = (2) \cdot I$, and $(2) \neq I$. Note however that uniqueness is not the only thing that fails, the ideal (2) doesn't even have a decomposition into prime ideals.

Max von Consbruch, email: mvconsbruch@uni-bonn.de. Date: November 14, 2023