Algebraic Number Theory - Assignment 4

Matteo Durante, 2303760, Leiden University

10th October 2018

Exercise 4

We see that $f = x^3 - x^2 - 6x - 12$ is the polynomial defining the desired number ring extension of $\mathbb{Z}$, as β is a root and it is irreducible in $\mathbb{Z}[x]$ because it doesn't have any root in $\mathbb{Z}$ (we only have to check the divisors in $\mathbb{Z}$ of the constant term). Its derivative is $f' = 3x^2 - 2x - 6$.

Seeing that the discriminant of f is $\Delta(f) = \frac{(-1)^{3(3-1)/2}R(f,f')}{1} = -4332 = -2^2 \cdot 3 \cdot 19^2$, it has multiple roots only modulo $2, 3$ and 19, hence it is regular above all other primes.

Now, we see that $f(13) = 0 \mod 19$, hence, noticing that $(x-13)^3 = x^3 - 39x^2 + 507x - 2197 = x^3 - x^2 - 6x - 12 \mod 19$, and therefore $\mathfrak{p}_1 = (19, \beta - 13)$, $e_1 = 3$, we look at the division of f by $x - 13$ in $\mathbb{Z}[x]$. There, we get $f = (x^2 + 12x + 150)(x - 13) + 1938$ and, since $1938 = 2 \cdot 3 \cdot 17 \cdot 19$, the only prime ideal above 19 is regular.

The analysis of the primes above 3 has already been carried out in the notes, hence we will move on to the ones above 2.

Seeing that $f = x^3 + x^2 = x^2(x + 1) \mod 2$, we can already say that these primes are exactly $\mathfrak{p}_1 = (2, \beta)$ and $\mathfrak{p}_2(2, 1 + \beta)$. Furthermore, since $e_2 = 1$, the second one is necessarily regular. On the other hand, $e_1 = 2$ and since $f = x(x^2 - x - 6) - 12$ we get that $r_1 = -12 = -2^2 \cdot 3$, hence $\mathfrak{p}_1$ is singular.

Now, we see that $\frac{1}{2}(\beta^2 - \beta - 6) = -(1 + \alpha) \in r(\mathfrak{p})$ by [1, cor. 3.2], thus, since $\mathbb{Z}[\beta] \subset r(\mathfrak{p})$, $\mathbb{Z}[\alpha, \beta] = \tilde{R} \subset r(\mathfrak{p})$.

This proves that $\mathfrak{p}_1$ is an integral $\tilde{R}$-ideal. Now, since all non-zero ideals in this ring are invertible because it is a Dedekind Domain, we get that $\mathfrak{p}_1$ is an invertible $\tilde{R}$-ideal and hence proper, which concludes the proof (indeed, $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha, \beta)$ and anyway the multiplier ring is invariant under field extension).

Exercise 8

Given that $B_\mathfrak{p} \subset Q(B)$, it is a number ring.

Let $\mathfrak{q}$ be a non-zero prime in B. Then, being A a subring of B, $\mathfrak{q} \cap A$ is a non-zero prime of A.

Indeed, it is trivially an ideal and it is proper because $1 \notin \mathfrak{q} \cap A \subset \mathfrak{q}$. Furthermore, there is a prime element $q \in \mathfrak{q} \cap \mathbb{Z} \subset \mathfrak{q} \cap A$. If the ideal was not prime, then there would be $a, b \in A \setminus \mathfrak{q} \subset B \setminus \mathfrak{q}$ s.t. $ab \in \mathfrak{q} \cap A \subset \mathfrak{q}$, which is absurd.

Now, the primes in $B_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}B$ are those which correspond to the ones in B disjoint from $A \setminus \mathfrak{p}$. Let $\mathfrak{q} \subset B$ be a non-zero prime. Since the intersection with A is a non-zero prime, either $\mathfrak{q} \cap A = \mathfrak{p}$ or $\mathfrak{q} \cap (A \setminus \mathfrak{p}) \neq \emptyset$. Indeed, we can't have $\mathfrak{q} \cap A \subsetneq \mathfrak{p}$ or $\supsetneq \mathfrak{p}$ because we are in a domain with Krull dimension 1. In the former case, $\mathfrak{q}$ corresponds to a prime in $B_\mathfrak{p}$, while in the latter it becomes the whole ring in $B_\mathfrak{p}$.

Since a prime ideal $\mathfrak{q}$ corresponding to a non-zero prime in $B_{\mathfrak{p}}$ must contain $\mathfrak{p}$, it contains a prime $p \in \mathfrak{p}$. Given that there are finitely many primes in B with this property (this follows from the fact that (p) has finite index in B), $B_{\mathfrak{p}}$ has finitely many prime ideals and hence finitely many maximal ones.

References

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