Algebraic Number Theory - Assignment 9

Matteo Durante, 2303760, Leiden University

30th November 2018

Exercise 14

First of all, notice that, given $k \in \mathbb{Z}$, both $X - k$ and $X^2 - (2k+1)X + k(k+1)$ are monic polynomials in $\mathbb{Z}[X]$ with discriminant $= 1$ up to sign, therefore we only have to check the other implication.

Notice that such a polynomial must have distinct roots, for otherwise $\Delta(f) = 0$.

If it is irreducible in $\mathbb{Z}[X]$ and it has a non-integer root α (which therefore does not lie in $\mathbb{Q}$), then it is irreducible in $\mathbb{Q}[X]$ and, since $\mathbb{Q}[X]/(f) \cong \mathbb{Q}(\alpha)$ is a non-trivial finite field extension of $\mathbb{Q}$, we have $\mathbb{Z} \ni |\Delta(f)| \geq |\Delta_{\mathbb{Q}(\alpha)}| \neq 1$, hence the roots of our polynomial must lie in $\mathbb{Z}$.

If it is the product of two (distinct monic) polynomials in $\mathbb{Z}[X]$, $f = f_1 f_2$, then, calling α_i the roots of f and α_{ki} the roots of f_k, we get $\Delta(f) = \Pi_{i<j}(\alpha_i - \alpha_j)^2 = \Pi_{i<j}(\alpha_{1i} - \alpha_{1j})^2 \cdot \Pi_{i<j}(\alpha_{2i} - \alpha_{2j})^2 \cdot \Pi_{i,j}(\alpha_{1i} - \alpha_{2j})^2 = \Delta(f_1)\Delta(f_2)Res(f_1, f_2)^2$.

Since $Res(f_1, f_2) \in \mathbb{Z}$, to have $|\Delta(f)| = 1$ we need $|\Delta(f_1)| = |\Delta(f_2)| = 1$ (they already lie in $\mathbb{Z}$). Iterating the procedure, we get that the absolute values of the discriminants of the irreducible factors have to be $= 1$, hence f only has integer roots.

Continuing, since $\Delta(f) = \Pi_{i<j}(\alpha_i - \alpha_j)^2$ and $\alpha_i \in \mathbb{Z}$, we need $|\alpha_i - \alpha_j| = 1$ for every i, j, where $i \neq j$. This means that it can't have more than two roots.

It follows that either it has only one root, and hence $f = X - k$, or it has only two (consecutive) roots, i.e. $f = (X - k)(X - (k+1)) = X^2 - (2k+1)X + k(k+1)$, for some $k \in \mathbb{Z}$.

Exercise 20

Let A be an integral ring extension of R.

If $x \in R^*$, then $x^{-1} \in R \subset A$, hence $x \in A^*$ and $R^* \subset A^* \cap R$.

We only have to show the opposite inclusion.

Let $x \in A^* \cap R$. Being x^{-1} integral over R, it is the zero of a monic polynomial $f = \sum_{i=0}^{n} r_i X^i \in R[X]$. It follows that $x^{n-1}(\sum_{i=0}^{n} r_i x^{-i}) = (\sum_{i=0}^{n-1} x^{n-(i+1)} r_i) + x^{-1} = 0$, hence $x^{-1} = -\sum_{i=0}^{n-1} x^{n-(i+1)} r_i \in R$ and $x \in R^*$.

We notice that the integrality condition is necessary, for $\mathbb{Q}^* \cap \mathbb{Z} = \mathbb{Z} \setminus \{0\} \neq \mathbb{Z}^*$.

References

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