Math 209-16 Homework 7

Due Date: Dec. 29, 2022

P1.(2 pts) If α is an algebraic number in $\mathbb{Q}(\sqrt{m})$ with $m < 0$, prove that $N(\alpha) \geqslant 0$. Show that this is false if $m > 0$.

Proof. When $m < 0$ and $\alpha = a + b\sqrt{m}$, we have $N(\alpha) = a^2 - mb^2 \geqslant 0$. But when $m > 0$, we have, for instance, $N(\sqrt{m}) = -m < 0$. $\square$

P2.(2 pts) Prove that the following assertion is false in $\mathbb{Q}(i)$: if $N(\alpha)$ is a rational integer, then α is an algebraic integer.

Proof. For example, $N(\frac{3}{5} + \frac{4}{5}i) = 1$ is a rational integer, but $\frac{3}{5} + \frac{4}{5}i$ is not an algebraic integer. $\square$

P3.(2 pts) Prove that 3 is a prime in $\mathbb{Q}(i)$, but not a prime in $\mathbb{Q}(\sqrt{6})$.

Proof. If 3 is not a prime in $\mathbb{Q}(i)$, then it is reducible and can be written as $3 = xy$ with $x, y \in \mathbb{Z}[i]$ non-units. Taking norms we obtain $9 = N(x)N(y)$, and so $N(x) = 3$ since non-units in $\mathbb{Q}(i)$ have norm larger than 1. But if we write $x = a + bi$ with $a, b \in \mathbb{Z}$ this would mean $a^2 + b^2 = 3$, which is impossible. Therefore 3 is a prime in $\mathbb{Q}(i)$.

On the other hand, in the ring of integers $\mathbb{Z}[\sqrt{6}]$ of $\mathbb{Q}(\sqrt{6})$, we have $3 = (3 + \sqrt{6})(3 - \sqrt{6})$. And since $N(3 + \sqrt{6}) = N(3 - \sqrt{6}) = 3 \neq \pm 1$, they are not units, so indeed 3 is not a prime in $\mathbb{Q}(\sqrt{6})$. $\square$

P4.(2 pts) Prove that $\mathbb{Q}(\sqrt{-11})$ has the unique factorization property.

Proof. Recall the norm map of the field extension $\mathbb{Q}(\sqrt{-11})/\mathbb{Q}$ is given by $N(\alpha) = a^2 + 11b^2$ for $\alpha = a + b\sqrt{-11}$ and the ring of integers in $\mathbb{Q}(\sqrt{-11})$ is $R := \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$. Elements of R are those $a + b\sqrt{-11}$ with $a, b \in \frac{1}{2}\mathbb{Z}$ and $a + b \in \mathbb{Z}$, therefore their norms are actually rational integers. We claim that the norm map $N : R \to \mathbb{N}$ can serve as an Euclidean function for R. Indeed, for any elements $\alpha = a + b\sqrt{-11}$ and $\beta = c + d\sqrt{-11} \neq 0$ in R, we first write $\alpha = \beta\gamma$ with $\gamma = m + n\sqrt{-11} \in$

$\mathbb{Q}(\sqrt{-11})$. Now $2m$ and $2n$ are rational numbers and we can find integers m_0 and n_0 with the same parity such that $|m_0 - 2m| \leqslant 1$ and $|n_0 - 2n| \leqslant \frac{1}{2}$. Putting $\gamma_0 = \frac{1}{2}(m_0 + n_0\sqrt{-11})$, which is an element in R, we find $\alpha = \beta\gamma_0 + \beta\delta$, where $\delta = \gamma - \gamma_0 = (m - \frac{m_0}{2}) + (n - \frac{n_0}{2})\sqrt{-11}$. By our choice of m_0 and n_0, we see that $N(\delta) \leqslant \frac{1}{4} + \frac{11}{16} < 1$, hence $N(\beta\delta) < N(\beta)$, which concludes the proof of the claim. Being an Euclidean domain, the ring R therefore has the unique factorization property. □

P5.(2 pts) Prove that the primes of $\mathbb{Q}(\sqrt{2})$ are $\sqrt{2}$, all rational primes of the form $8k \pm 3$, and all factors $a + b\sqrt{2}$ of rational primes of the form $8k \pm 1$, and all associates of these primes.

Proof. We know that $\mathbb{Q}(\sqrt{2})$ has the unique factorization property, so this proposition follows immediately from Theorem 9.29 in the textbook, since for odd primes p, we have:

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8 \end{cases}$$

□

P6.(2 pts) Find all solutions of $y^2 + 1 = x^3$ in rational integers.

Proof. A solution gives a factorization $x^3 = (y + i)(y - i)$ in the ring $R = \mathbb{Z}[i]$. Notice that y cannot be odd, since otherwise we would have $x^3 \equiv 2 \pmod 4$ which is impossible. Now in R we have $(y + i, y - i) | (2i) = (1 + i)^2$, and $(1 + i) \nmid (y + i)$ since $2 = N(1 + i) \nmid N(y + i) = (y^2 + 1)$, therefore $(y + i, y - i) = 1$. As R is a unique factorization domain we conclude that $y + i$ and $y - i$ should both be perfect cubes in R. Writing $y + i = (a + bi)^3$ we obtain $a^3 - 3ab^2 = y$ and $3a^2b - b^3 = 1$. It is easy to see the only integer solution is $a = 0$ and $b = -1$, which is to say the only solution of the original equation is $x = 1$, $y = 0$. □