

Algebraic Number Theory — Solutions to problem set 1

Problem 1. Show that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean with respect to the norm map $N(a + b\sqrt{-2}) = a^2 + 2b^2$ ($a, b \in \mathbb{Z}$). Show that the only solutions $X, Y \in \mathbb{Z}$ of the equation $X^2 + 2 = Y^3$ are $X = \pm 5$ and $Y = 3$.

Solution. Let $R := \mathbb{Z}[\sqrt{-2}]$. Note that R is a domain, because it is a subring of \mathbb{C} . Also note that $N(x) = x \cdot \bar{x}$; in particular the norm is multiplicative, and because $N(x) \in \mathbb{Z}$ for all $x \in R$ it follows that $N(y) \leq N(xy)$ for all nonzero $x, y \in R$.

Let $x, y \in R$ with $y \neq 0$. We want to find $q, r \in R$ with $x = qy + r$ and either $r = 0$ or $N(r) < N(y)$. Write $x/y = c + d\sqrt{-2}$ in $\mathbb{Q}[\sqrt{-2}]$. Then choose c' and d' in \mathbb{Z} such that $|c - c'| \leq 1/2$ and $|d - d'| \leq 1/2$. Set $q := c' + d'\sqrt{-2}$ and

$$r := x - qy = (c + d\sqrt{-2})y - (c' + d'\sqrt{-2})y = \left((c - c') + (d - d')\sqrt{-2} \right) \cdot y.$$

Since the norm is multiplicative we find:

$$N(r) = \left((c - c')^2 + 2(d - d')^2 \right) \cdot N(y) \leq (1/4 + 2 \cdot 1/4) \cdot N(y) < N(y),$$

which is what we want.

The second part of the exercise closely follows the method discussed in Chapter 1 of the Lecture Notes. Suppose we have $X, Y \in \mathbb{Z}$ with $X^2 + 2 = Y^3$. Let $\xi := X + \sqrt{-2}$ and $\bar{\xi} = X - \sqrt{-2}$. Then $\xi, \bar{\xi} \in R$, and of course $\xi\bar{\xi} = X^2 + 2 = Y^3$. By what was proven above, R is Euclidean; in particular it is a unique factorization domain. We claim that the elements ξ and $\bar{\xi}$ are relatively prime. To see this, first note that X has to be odd, for if X is even then $X^2 + 2 \equiv 2 \pmod{4}$, whereas Y^3 is 0, 1 or 3 modulo 4. Hence the ideal generated by ξ and $\bar{\xi}$ contains $(\xi - \bar{\xi})^2 = -8$ but also $\xi\bar{\xi} = X^2 + 2$, which is an odd integer. So indeed, $\gcd(\xi, \bar{\xi}) = 1$. As R is a UFD, the conclusion is that ξ and $\bar{\xi}$ are both cubes in R , possibly up to a unit. In other words, there is an element $\eta \in R$ and a unit $u \in R^*$ with $\eta^3 = u\xi$.

The units are easily found: if $u \in R^*$ then there is a $v \in R$ with $uv = 1$, so $N(u)N(v) = 1$. But $N(u)$ and $N(v)$ are positive integers, so $N(u) = 1$. From this we readily conclude that ± 1 are the only units in R . Possibly after replacing η by $-\eta$ we may therefore assume that $\eta^3 = \xi$.

If $\eta = m + n\sqrt{-2}$ then

$$\eta^3 = m^3 + 3m^2n\sqrt{-2} - 6mn^2 - 2n^3\sqrt{-2} = (m^3 - 6mn^2) + (3m^2n - 2n^3)\sqrt{-2},$$

and this has to be equal to $\xi = X + \sqrt{-2}$. In particular, $1 = 3m^2n - 2n^3 = n(3m^2 - 2n^2)$, so either $n = 1$ and $3m^2 - 2n^2 = 1$, or $n = -1$ and $3m^2 - 2n^2 = -1$. The second possibility gives $3m^2 = 1$, which has no solutions with integral m . The first possibility gives $n = 1$ and $m = \pm 1$, corresponding to the given solutions $X = m^3 - 6mn^2 = \pm 5$ and $Y = 3$.

Problem 2. Let $\zeta_5 \in \mathbb{C}$ be a primitive 5-th root of unity. Let

$$F := \mathbb{Q}(\zeta_5, \sqrt[4]{5}).$$

- (i) Show that $[F : \mathbb{Q}] = 8$. [*Hint:* Use that $\mathbb{Q}(\zeta_5)$ has a unique quadratic subfield; write that subfield as $\mathbb{Q}(\sqrt{d})$ for some squarefree integer d .]
- (ii) Find a primitive element of F .
- (iii) Determine r_1 and r_2 .
- (iv) Let $\mu_F \subset F^*$ be the subgroup of roots of unity, i.e.,

$$\mu_F = \{x \in F^* \mid \text{there exists an integer } m > 0 \text{ with } x^m = 1\}.$$

Determine $w_F := \#(\mu_F)$, and show that $\mu_F \cong \mathbb{Z}/w_F\mathbb{Z}$ as groups.

Solution. (i) Write $\zeta := \zeta_5$. Let $K = \mathbb{Q}(\zeta + \zeta^4)$. We have $(\zeta + \zeta^4)^2 = \zeta^2 + 2 + \zeta^3$, and since $1 + \zeta + \dots + \zeta^4 = 0$ we find that the minimum polynomial of $\zeta + \zeta^4$ is $T^2 + T - 1$. So K is a quadratic subfield of $\mathbb{Q}(\zeta_5)$. (In fact, $K = \mathbb{Q}(\zeta_5) \cap \mathbb{R}$.) Now $T^2 + T - 1 = (T + \frac{1}{2})^2 - \frac{5}{4}$, and from this we conclude that $K = \mathbb{Q}(\sqrt{5})$. In particular, F has degree at most 2 over its subfield $\mathbb{Q}(\zeta_5)$, which has degree $\varphi(5) = 4$ over \mathbb{Q} . But also it is clear that $F \neq \mathbb{Q}(\zeta_5)$, for F has a real embedding and $\mathbb{Q}(\zeta_5)$ has not. So $[F : \mathbb{Q}(\zeta_5)] = 2$ and $[F : \mathbb{Q}] = 2 \cdot 4 = 8$.

(ii) The complex zeroes of the minimum polynomial of $\zeta = \zeta_5$ over \mathbb{Q} are the elements $\alpha_j = \zeta^j$ for $j = 1, \dots, 4$. The complex zeroes of the minimum polynomial of $\sqrt[4]{5}$ over \mathbb{Q} are the elements $\beta_k = i^{k-1} \cdot \sqrt[4]{5}$ for $k = 1, \dots, 4$. The proof of Thm. 2.2 shows that if $\lambda \in \mathbb{Q}$ is not equal to $(\alpha_j - \alpha_1)/(\beta_1 - \beta_k)$ for any $j \in \{1, \dots, 4\}$ and $k \in \{2, 3, 4\}$ then $\theta := \alpha_1 + \lambda\beta_1$ is a primitive element. Now it is clear that $|\alpha_j - \alpha_1| < 2$ and $|\beta_1 - \beta_k| > 1/2$ for all $j \in \{1, \dots, 4\}$ and $k \in \{2, 3, 4\}$, so $\lambda = 4$ does the job and $\zeta_5 + 4\sqrt[4]{5}$ is an example of a primitive element.

Another possibility is to remark that $\gamma = \zeta \cdot \sqrt[4]{5}$ is a primitive element. Indeed, it is clear that $\mathbb{Q}(\gamma) \subseteq F$. On the other hand,

$$\zeta = 5 \cdot \gamma^{-4} \quad \text{and} \quad \sqrt[4]{5} = (1/5) \cdot \gamma^5,$$

so also $F \subset \mathbb{Q}(\gamma)$.

(iii) Suppose we had a real embedding $j: F \rightarrow \mathbb{R}$. Then $x = j(\zeta)$ was a real number with $x \neq 1$ and $x^5 = 1$. Such elements x do not exist. Hence $r_1 = 0$ and $r_2 = 4$.

(iv) We first remark that μ_F is finite. Indeed, if μ_F contains an element x of order m then we get an embedding $\mathbb{Q}(\zeta_m) \hookrightarrow F$ (with $\zeta_m \mapsto x$), which implies that $\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ divides $[F : \mathbb{Q}] = 8$. But there are only finitely many natural numbers m such that $\varphi(m) | 8$ and for each such m there are only finitely many m th roots of unity. Hence μ_F is finite.

Now we know from Algebra that every finite subgroup of F^* is cyclic. Hence $\mu_F \cong \mathbb{Z}/w_F\mathbb{Z}$. On the other hand, we already know that F contains a primitive 10-th root of unity (namely $-\zeta_5$), so $10 | w_F$.

Next we remark that the only integers n such that $\varphi(10n)$ divides 8 are the integers $n \in \{1, 2, 3\}$. Moreover, if $w_F = 20$ or $w_F = 30$ then $\varphi(w_F) = 8$ so $F = \mathbb{Q}(\zeta_{20})$, resp. $F = \mathbb{Q}(\zeta_{30})$. We claim that this is not the case. There are various ways to see this. Perhaps the simplest way to see this is to use a little Galois theory: the fields $K = \mathbb{Q}(\zeta_{20})$ and $L = \mathbb{Q}(\zeta_{30})$ are Galois extensions of \mathbb{Q} with abelian Galois group. In particular, every subfield of K and of L is again Galois over \mathbb{Q} . But the subfield $\mathbb{Q}(\sqrt[4]{5}) \subset F$ is evidently not Galois over \mathbb{Q} , so F is not $\mathbb{Q}(\zeta_{20})$ or $\mathbb{Q}(\zeta_{30})$.

But also without Galois theory, we can see that F is not one of the fields $\mathbb{Q}(\zeta_{20})$ or $\mathbb{Q}(\zeta_{30})$. We view F as a subfield of \mathbb{C} with $\zeta_5 = e^{2\pi i/5}$. Note that

$$1, \sqrt[4]{5}, \sqrt{5}, (\sqrt[4]{5})^3, \zeta_5, \zeta_5 \cdot \sqrt[4]{5}, \zeta_5 \cdot \sqrt{5}, \zeta_5 \cdot (\sqrt[4]{5})^3$$

is a \mathbb{Q} -basis for F . As the first four elements in this list are real, it follows that for every $x \in F$ the imaginary part $\text{Im}(x)$ lies in $\mathbb{Q} \cdot \text{Im}(\zeta_5)$. On the other hand, we have already seen in (i) that

$$2 \cdot \text{Re}(\zeta_5) = \zeta_5 + \bar{\zeta}_5 = \zeta_5 + \zeta_5^4 = -\frac{1}{2} + \frac{1}{2}\sqrt{5}.$$

(It is clear that $\text{Re}(\zeta_5) > 0$.) So $\text{Im}(\zeta_5)$ satisfies

$$\text{Im}(\zeta_5)^2 = 1 - \left(-\frac{1}{4} + \frac{1}{4}\sqrt{5}\right)^2 = \frac{5}{8} + \frac{1}{8}\sqrt{5}.$$

If $F = \mathbb{Q}(\zeta_{20})$ then $i \in F$ so $1 \in \mathbb{Q} \cdot \text{Im}(\zeta_5)$; this means that $\text{Im}(\zeta_5) \in \mathbb{Q}$, and we get a contradiction. If $F = \mathbb{Q}(\zeta_{30})$ then $\zeta_3 \in F$ so $\frac{1}{2}\sqrt{3} \in \mathbb{Q} \cdot \text{Im}(\zeta_5)$, so $\text{Im}(\zeta_5) \in \mathbb{Q} \cdot \sqrt{3}$, and we again get a contradiction.

Problem 3. Let

$$f := T^3 - 3T + 9 \in \mathbb{Q}[T]$$

and define $F := \mathbb{Q}[T]/(f)$. Write $\alpha \in F$ for the class of T modulo (f) . You may use without proof that f is irreducible in $\mathbb{Q}[T]$, so that F is a field with $[F : \mathbb{Q}] = 3$.

- (i) Compute $\text{Disc}(f)$. [If you want to do this using resultants, you may use the formulas in Exercise (3.K) of the lecture notes without proof.]
- (ii) Show that $1, \alpha, \alpha^2$ is *not* an integral basis for O_F .
- (iii) Give an integral basis and compute Δ_F .

Solution. (i) Prop. 3.2 gives that $\text{Disc}(f) = -N(3\alpha^2 - 3)$. We first compute the matrix M_{α^2} of multiplication by α^2 with respect to the basis $\{1, \alpha, \alpha^2\}$. We have $\alpha^2 \cdot 1 = \alpha^2$. Next, $\alpha^2 \cdot \alpha = \alpha^3 = -9 + 3\alpha$ and $\alpha^2 \cdot \alpha^2 = -9\alpha + 3\alpha^2$. So

$$M_{\alpha^2} = \begin{pmatrix} 0 & -9 & 0 \\ 0 & 3 & -9 \\ 1 & 0 & 3 \end{pmatrix}.$$

This gives

$$\text{Disc}(f) = -\det \begin{pmatrix} -3 & -27 & 0 \\ 0 & 6 & -27 \\ 3 & 0 & 6 \end{pmatrix} = 3 \cdot 36 - 3 \cdot 27^2 = -27 \cdot (81 - 4) = -27 \cdot 7 \cdot 11.$$

(ii) and (iii). The only integer $m > 1$ with $m^2 | \text{Disc}(f)$ is $m = 3$. So we look for linear combinations $y = a_0 + a_1\beta + a_2\beta^2$ such that $y/3$ is integral.

Intermezzo: how do you recognize whether y/m is integral, if the minimum polynomial of $y \in F$ is known and m is a non-zero integer? The answer is quite simple: suppose

$$f = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$$

is the minimum polynomial of y over \mathbb{Q} . Then the minimum polynomial of y/m is

$$T^n + \frac{a_{n-1}}{m}T^{n-1} + \frac{a_{n-2}}{m^2}T^{n-2} + \cdots + \frac{a_1}{m^{n-1}}T + \frac{a_0}{m^n},$$

and therefore: y/m is integral if and only if a_i is divisible by m^{n-i} for each $i \in \{0, 1, \dots, n-1\}$.

The minimum polynomial of α^2 is the characteristic polynomial of the above matrix M_{α^2} , which is $T(T-3)^2 - 81 = T^3 - 6T^2 + 9T - 81$. We find that $\alpha^2/3$ is integral. Hence $1, \alpha, \alpha^2$ is not an integral basis. Using Prop. 3.4 we find that

$$\Delta(1, \alpha, \alpha^2/3) = (1/9) \cdot \Delta(1, \alpha, \alpha^2) = -3 \cdot 7 \cdot 11,$$

and since this is a square free integer, $1, \alpha, \alpha^2/3$ is an integral basis and $\Delta_F = -231$.