Autumn Semester 2019

Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

Solutions to Exercise Sheet 2

Exercise 2.1. Let $A = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$ and $K = \mathbb{Q}(\sqrt{-3})$. Show that the integral closure of A in K is $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-3}}{2})$.

Solution. Since A is clearly integral over $\mathbb{Z}$, by transitivity we get that A^K is also integral over $\mathbb{Z}$, and hence equal to $\mathbb{Z}^K$. On the other hand, if $b \neq 0$, then the minimal polynomial of $a + b\sqrt{-3} \in K$ is $x^2 - 2ax + (a^2 + 3b^2)$. Thus $a + b\sqrt{-3} \in \mathbb{Z}^K$ iff $2a, a^2 + 3b^2 \in \mathbb{Z}$. From $2a \in \mathbb{Z}$ we get that a is half-integral, and from $a^2 + 3b^2 \in \mathbb{Z}$ we get that if $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$, and if $a \in 1/2 + \mathbb{Z}$, then $b \in 1/2 + \mathbb{Z}$. Therefore, $A^K = \mathbb{Z}^K = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-3}}{2})$.

Exercise 2.2. Show that the following numbers are algebraic integers:

(a) $\alpha = \frac{\sqrt{3}+\sqrt{7}}{2}$;

(b) $\beta = \frac{\alpha^2-\alpha}{2}$, where α is a root of $x^3 + x - 6$. (To find a polynomial equation that β satisfies, write down the matrix of multiplication by β in $\mathbb{Q}(\alpha)$.)

Solution. (a) We calculate $4\alpha^2 = 3 + 2\sqrt{21} + 7 = 10 + 2\sqrt{21}$, and thus $(4\alpha^2 - 10)^2 = 84$. Expanding the last expression we get $16\alpha^4 - 80\alpha^2 + 16 = 0$, from which after dividing by 16 we get $\alpha^4 - 5\alpha^2 + 1 = 0$. Therefore, α is an algebraic integer.

(b) In the basis $1, \alpha, \alpha^2$ the operator M_β of multiplication by β looks as follows:

$$\begin{aligned} \beta \cdot 1 &= 0 \cdot 1 - \tfrac{1}{2} \cdot \alpha + \tfrac{1}{2} \cdot \alpha^2 , \\ \beta \cdot \alpha &= 3 \cdot 1 - \tfrac{1}{2} \cdot \alpha - \tfrac{1}{2} \cdot \alpha^2 , \\ \beta \cdot \alpha^2 &= -3 \cdot 1 + \tfrac{7}{2} \cdot \alpha - \tfrac{1}{2} \cdot \alpha^2 . \end{aligned}$$

From this we find that the characteristic polynomial of M_β is

$$\begin{aligned} \det \begin{pmatrix} x & -3 & 3 \\ \frac{1}{2} & x + \frac{1}{2} & -\frac{7}{2} \\ -\frac{1}{2} & \frac{1}{2} & x + \frac{1}{2} \end{pmatrix} &= x(x + \tfrac{1}{2})^2 + \tfrac{3}{4} - \tfrac{21}{4} + \tfrac{3}{2}(x + \tfrac{1}{2}) + \tfrac{3}{2}(x + \tfrac{1}{2}) + \tfrac{7}{4}(x) \\ &= x^3 + x^2 + \tfrac{1}{4}x - \tfrac{9}{2} + 3(x + \tfrac{1}{2}) + \tfrac{7}{4}x = x^3 + x^2 + 5x - 3 . \end{aligned}$$

Hence, by using Cayley-Hamilton theorem, we see that M_β, and hence β as well, satisfies $\beta^3 + \beta^2 + 5\beta - 3 = 0$, and thus it is an algebraic integer.

Exercise 2.3. Let p be a prime, and let ζ_p be a primitive p-th root of unity. Show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$ as follows. Let $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$.

(a) Using the Galois action show that if α is an algebraic integer, then $pa_j \in \mathbb{Z}$;

(b) Show that $\frac{p}{(1-\zeta_p)^l}$ is an algebraic integer for $0 \le l \le (p-1)$;

(c) Show that α can be written as

$$\alpha \;=\; \frac{m_0 + m_1(1-\zeta_p) + \cdots + m_{p-2}(1-\zeta_p)^{p-2}}{p}\,,$$

where $m_i \in \mathbb{Z}$, and, assuming that some m_j is not divisible by p, obtain a contradiction using part (b).

Solution. (a) The conjugates of α are given by α_j, $j = 1, \ldots, p-1$, where

$$\alpha_j = a_0 + a_1\zeta_p^j + \cdots + a_{p-2}\zeta_p^{j(p-2)}$$

(some of α_j might coincide, but it does not matter). If α is integral over $\mathbb{Z}$, then so are all of its conjugates, and hence $\alpha_1 + \cdots + \alpha_{p-1} = pa_0 - s \in \mathbb{Z}$, where $s = a_0 + \cdots + a_{p-2}$. Here we have used the fact that $\sum_{j=1}^{p-1}\zeta_p^{jk} = -1$ for k not divisible by p. Repeating this argument for $\alpha\zeta_p^j$, $j = 1, \ldots, p-1$, which are also algebraic integers, we get that $pa_{p-j} - s \in \mathbb{Z}$ (here $a_{p-1} = 0$). From this we conclude that if α is integral over $\mathbb{Z}$, then $pa_j \in \mathbb{Z}$, $j = 0, \ldots, p-2$.

(b) It is enough to show that $\frac{p}{(1-\zeta_p)^l} \in \mathbb{Z}[\zeta_p]$. Observe that

$$(1-\zeta_p)(1-\zeta_p^2)\ldots(1-\zeta_p^{p-1}) = p\,, \qquad (\star)$$

since $(x-\zeta_p)(x-\zeta_p^2)\ldots(x-\zeta_p^{p-1}) = \frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$. Therefore,

$$\frac{p}{(1-\zeta_p)^l} \;=\; \prod_{j=1}^{l}\frac{1-\zeta_p^j}{1-\zeta_p}\prod_{j=l+1}^{p-1}(1-\zeta_p^j) \;=\; \prod_{j=1}^{l}(1+\cdots+\zeta_p^{j-1})\prod_{j=l+1}^{p-1}(1-\zeta_p^j) \in \mathbb{Z}[\zeta_p]\,,$$

as claimed.

(c) By part (a) $pa_i \in \mathbb{Z}$, so that $\alpha = \frac{n_0+n_1\zeta_p+\cdots+n_{p-2}\zeta_p^{p-2}}{p}$ for some integers n_i. Using $\zeta_p = 1-(1-\zeta_p)$ and expanding the resulting expression using binomial theorem we get

$$\alpha \;=\; \frac{m_0 + m_1(1-\zeta_p) + \cdots + m_{p-2}(1-\zeta_p)^{p-2}}{p}$$

for some $m_i \in \mathbb{Z}$. Suppose that not all m_i are divisible by p. Since changing any m_i by a multiple of p does not matter for the integrality of α, we may assume that

$$\alpha \;=\; \frac{m_k(1-\zeta_p)^k + \cdots + m_{p-2}(1-\zeta_p)^{p-2}}{p}\,,$$

where $0 \le k \le (p-2)$ and m_k is not divisible by p. From this we see that

$$\frac{m_k}{(1-\zeta_p)} \;=\; \frac{p}{(1-\zeta_p)^{k+1}}\alpha - m_{k+1} - \cdots - m_{p-2}(1-\zeta_p)^{p-2-k-1}\,.$$

By part (b) the right-hand side is an algebraic integer, therefore $\frac{m_k}{1-\zeta_p}$ is also an algebraic integer. Taking the product over all conjugates (using $(\star)$) we get that $\frac{m_k^{p-1}}{p}$ is an algebraic integer, hence a usual integer, which contradicts the choice of m_k. Therefore, all m_j have to be divisible by p, and hence $\alpha \in \mathbb{Z}[\zeta_p]$.

Exercise 2.4 (Gauss sums). Let p be an odd prime, and let ζ_p be a primitive p-th root of unity. For $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ define

$$\tau(a) \;=\; \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x}{p}\right) \zeta_p^{ax}\,,$$

where $(\frac{a}{p})$ is the Legendre symbol.

(a) Show that $\tau(a) = (\frac{a}{p})\tau(1)$;

(b) Show that $\tau(1)^2 = (-1)^{\frac{p-1}{2}} p$;

(c) Let $K/\mathbb{Q}$ be a quadratic extension. Prove that there exists a root of unity ζ such that $K \subseteq \mathbb{Q}(\zeta)$.

Hint: in (c) note that $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$*, and use the result of part (b).*

Solution. (a) Using multiplicativity of $(\frac{x}{p})$ we calculate

$$\left(\frac{a}{p}\right)\tau(a) \;=\; \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{ax}{p}\right) \zeta_p^{ax} \;=\; \sum_{y\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{y}{p}\right) \zeta_p^{y} = \tau(1)\,,$$

since $y = ax$ runs over the same set $(\mathbb{Z}/p\mathbb{Z})^\times$. Since $(\frac{a}{p}) = \pm 1$ we get the claim.

(b) By part (a) we have $\tau(-1) = (\frac{-1}{p})\tau(1) = (-1)^{(p-1)/2}\tau(1)$. Therefore, it is enough to show that $\tau(1)\tau(-1) = p$. For this we calculate

$$\tau(1)\tau(-1) \;=\; \sum_{x,y\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{xy}{p}\right) \zeta_p^{x-y} \;=\; \sum_{x,z\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x^2 z}{p}\right) \zeta_p^{x(1-z)}\,,$$

where in the second equality we have changed the summation variable to $z = y/x$. From the properties of Legendre symbol we have $(\frac{x^2 z}{p}) = (\frac{z}{p})$. Using the fact that $\sum_{j=1}^{p-1} \zeta_p^{jk} = p\delta_{k,0} - 1$ for $k = 0, \dots, p-1$, we rewrite the last sum as

$$\sum_{x,z\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{z}{p}\right) \zeta_p^{x(1-z)} \;=\; p \;-\; \sum_{z\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{z}{p}\right) \;=\; p\,,$$

proving the claim. Here $\sum_{z\in(\mathbb{Z}/p\mathbb{Z})^\times} (\frac{z}{p})$ vanishes since if n is any non-residue, $(\frac{n}{p}) = -1$, then

$$\sum_{z\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{z}{p}\right) \;=\; \sum_{z\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{zn}{p}\right) \;=\; -\sum_{z\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{z}{p}\right)\,.$$

(c) Let $K = \mathbb{Q}(\sqrt{d})$, $d = \pm 2^e p_1 \dots p_k$, where $e \in \{0, 1\}$, and p_i are distinct odd primes. Then clearly

$$K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_k})\,.$$

We have $\sqrt{-1} = \zeta_4$, and $\sqrt{2}$ can be expressed in terms of ζ_8, since

$$(\zeta_8 + \zeta_8^{-1})^2 = \zeta_4 + 2 + \zeta_4^{-1} = 2\,.$$

By part (b), for an odd prime p we have $\pm p = (\tau(1))^2$. Therefore either $\sqrt{p} = \pm\tau(1) \in \mathbb{Q}(\zeta_p)$ or $\sqrt{p} = \pm\sqrt{-1}\tau(1) \in \mathbb{Q}(\zeta_4, \zeta_p)$. Thus we conclude

$$K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_8, \zeta_{p_1}, \dots, \zeta_{p_k}) \subseteq \mathbb{Q}(\zeta_m)\,,$$

where $m = 8p_1 \dots p_k$.