Solutions to Exercise Sheet 6

Solution 6.1. *Examples of algebraic integers.*

(1) $\frac{1}{2}(1+\sqrt{5})$ is an algebraic integer because it is a root of the polynomial x^2-x-1. For $3+i$, we let $x=3+i$, rewrite it as $x-3=i$ and square both sides to get $x^2-6x+9=-1$, hence $3+i$ is the root of the polynomial $x^2-6x+10$.

For $\sqrt{2}+\sqrt[3]{3}$, we let $x=\sqrt{2}+\sqrt[3]{3}$, rewrite it as $x-\sqrt{2}=\sqrt[3]{3}$, take the third powers to get $x^3-3\sqrt{2}x^2+6x-2\sqrt{2}=3$. We rewrite it as $x^3+6x-3=(3x^2+2)\sqrt{2}$ and square both sides to get $(x^3+6x-3)^2=2(3x^2+2)^2$. Then we conclude that $\sqrt{2}+\sqrt[3]{3}$ is the root of the polynomial $(x^3+6x-3)^2-2(3x^2+2)^2=x^6-6x^4-6x^3+12x^2-36x+1$. Notice that all coefficients are integers, and the leading term x^6 has coefficient 1. This shows $\sqrt{2}+\sqrt[3]{3}$ is an algebraic integer.

(2) $\frac{1}{2}$ is an algebraic number because it is the root of $2x-1$. We show it is not an algebraic integer by contradiction. Assume it is the root of a monic polynomial

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-2}x^2+a_{n-1}x+a_n.$$

By substitution $x=\frac{1}{2}$ we have

$$\frac{1}{2^n}+\frac{a_1}{2^{n-1}}+\frac{a_2}{2^{n-2}}+\cdots+\frac{a_{n-2}}{2^2}+\frac{a_{n-1}}{2}+a_n=0.$$

Now we multiply 2^n on both sides to clear the denominators and obtain

$$1+2a_1+2^2a_2+\cdots+2^{n-2}a_{n-2}+2^{n-1}a_{n-1}+2^na_n=0.$$

The left-hand side is an odd number. Contradiction. Therefore $\frac{1}{2}$ is not an algebraic integer.

(3) Since α is an algebraic integer, it is a root of a polynomial $f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+a_3x^{n-3}+\cdots+a_{n-1}x+a_n\in\mathbb{Z}[x]$. We consider the polynomial $g(x)=x^n-a_1x^{n-1}+a_2x^{n-2}-a_3x^{n-3}+\cdots+(-1)^{n-1}a_{n-1}x+(-1)^na_n$, which is a monic polynomial with integer coefficients. We claim that $-\alpha$ is a root of $g(x)$. Indeed, we have

$$\begin{aligned}g(-\alpha)&=(-\alpha)^n-a_1(-\alpha)^{n-1}+a_2(-\alpha)^{n-2}-a_3(-\alpha)^{n-3}+\cdots\\&\qquad\cdots+(-1)^{n-1}a_{n-1}(-\alpha)+(-1)^na_n\\&=(-1)^n(\alpha^n+a_1\alpha^{n-1}+a_2\alpha^{n-2}+a_3\alpha^{n-3}+\cdots+a_{n-1}\alpha+a_n)\\&=0.\end{aligned}$$

Hence $-\alpha$ is an algebraic integer.

The following is another proof. I would like to thank people who provided this much better proof in their submitted solutions.

Since both α and -1 are algebraic integers, and the product of two algebraic integers is still an algebraic integer, we immediately know $-\alpha$ is an algebraic integer.

Solution 6.2. *Examples of traces and norms.*

(1) We have $L_\alpha(1) = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, $L_\alpha(\sqrt[3]{2}) = 2c + a\sqrt[3]{2} + b\sqrt[3]{4}$, $L_\alpha(\sqrt[3]{4}) = 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4}$. We write the coefficients as column vectors and get the matrix

$$M = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}.$$

Therefore we have $T(\alpha) = \operatorname{tr}(M) = 3a$ and $N(\alpha) = \det(M) = a^3 + 2b^3 + 4c^3 - 6abc$.

(2) We have $L_\zeta(1) = \zeta$, $L_\zeta(\zeta) = \zeta^2$, $L_\zeta(\zeta^2) = \zeta^3$, $L_\zeta(\zeta^3) = \zeta^4 = -\zeta^3 - \zeta^2 - \zeta - 1$. Hence the matrix is

$$M = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Therefore we have $T(\zeta) = \operatorname{tr}(M) = -1$ and $N(\zeta) = \det(M) = 1$.

Solution 6.3. *Elementary properties of the trace and norm.*

(1) For any $\gamma \in K$, $L_{\alpha+\beta}(\gamma) = (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma = L_\alpha(\gamma) + L_\beta(\gamma)$. Hence the linear transformation $L_{\alpha+\beta}$ is the sum of the two linear transformations L_α and L_β. Under any fixed basis, if the matrices for L_α and L_β are A and B respectively, then their sum $L_{\alpha+\beta}$ corresponds to the matrix $A + B$. Since we have $\operatorname{tr}(A + B) = \operatorname{tr}(A) + \operatorname{tr}(B)$, we get $T(\alpha + \beta) = T(\alpha) + T(\beta)$.

For any $\gamma \in K$, $L_{\alpha\beta}(\gamma) = (\alpha\beta)\gamma = \alpha(\beta\gamma) = L_\alpha(L_\beta(\gamma))$. Hence the linear transformation $L_{\alpha\beta}$ is the composition of the two linear transformations L_α and L_β. Under any fixed basis, if the matrices for L_α and L_β are A and B respectively, then their composition $L_{\alpha\beta}$ corresponds to the matrix AB. Since we have $\det(AB) = \det(A)\det(B)$, we get $N(\alpha\beta) = N(\alpha)N(\beta)$.

(2) For any $\gamma \in K$, $L_{a\alpha}(\gamma) = (a\alpha)\gamma = a(\alpha\gamma) = aL_\alpha(\gamma)$. Hence the linear transformation $L_{a\alpha}$ is the linear transformation $a \cdot L_\alpha$. Under any fixed basis, if the matrices for L_α is A, then the matrix corresponds to $L_{a\alpha}$ is aA. Since we have $\operatorname{tr}(aA) = a\operatorname{tr}(A)$, we get $T(a\alpha) = aT(\alpha)$. Similarly, since we have $\det(aA) = a^n \det(A)$ as A is an $n \times n$ matrix, we get $N(a\alpha) = a^n N(\alpha)$.

(3) For any $\gamma \in K$, $L_1(\gamma) = \gamma$. Hence the linear transformation L_1 is the identity map. Under any basis, its matrix is the $n \times n$ identity matrix I_n. Therefore $T(1) = \operatorname{tr}(I_n) = n$ and $N(1) = \det(I_n) = 1$.

(4) If $\alpha = 0$, then L_α is the zero linear transformation, hence $N(0) = 0$. Now we prove the other direction. We assume that $N(\alpha) = 0$ for some $\alpha \in K$. Under a fixed basis, we assume the matrix for L_α is A. Then $\det(A) = 0$, which means that A has a non-trivial null space. In other words, there is a non-zero vector $\mathbf{v}$ such that $A\mathbf{v} = 0$. But $\mathbf{v}$ is the vector form of some non-zero element $\gamma \in K$. Hence we have $L_\alpha(\gamma) = 0$. In other words, $\alpha\gamma = 0$. Since $\gamma \neq 0$, we must have $\alpha = 0$.

Solution 6.4. *Traces and norms of algebraic integers.*

(1) We first check S is a spanning set. For any $x \in K$, since $\{\beta_j \mid 0 \leqslant j \leqslant n-1\}$ is a spanning set for K over $\mathbb{Q}(\alpha)$, there exist $a_j \in \mathbb{Q}(\alpha)$ for $0 \leqslant j \leqslant n-1$ such that

$$x = \sum_{j=0}^{n-1} a_j \beta_j.$$

Since $\{\alpha^i \mid 0 \leqslant i \leqslant m-1\}$ is a spanning set for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, for every j there exists $b_{ij} \in \mathbb{Q}$ for $0 \leqslant i \leqslant m-1$ such that

$$a_j = \sum_{i=0}^{m-1} b_{ij}\alpha^i.$$

Therefore we have

$$x = \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} b_{ij}\alpha^i \beta_j,$$

which implies that S is a spanning set for K over $\mathbb{Q}$.

(2) We then check elements in S are independent over $\mathbb{Q}$. Assume we have

$$\sum_{j=0}^{n-1} \sum_{i=0}^{m-1} b_{ij}\alpha^i \beta_j = 0$$

for some $b_{ij} \in \mathbb{Q}$. We can group the terms as

$$\sum_{j=0}^{n-1} \left(\sum_{i=0}^{m-1} b_{ij}\alpha^i \right) \beta_j = 0.$$

Since $\sum_{i=0}^{m-1} b_{ij}\alpha^i \in \mathbb{Q}(\alpha)$ for each j, and $\{\beta_j\}$ are independent over $\mathbb{Q}(\alpha)$, we conclude that

$$\sum_{i=0}^{m-1} b_{ij}\alpha^i = 0$$

for each j. Moreover by the linear independence of $\{\alpha^i\}$, we conclude that

$$b_{ij} = 0$$

for every pair (i, j), which implies that elements in S are independent over $\mathbb{Q}$.

(3) Now we compute the matrix of L_α under the basis S for K over $\mathbb{Q}$. We assume that α is a root of a monic irreducible polynomial $g(x) \in \mathbb{Z}[x]$ of degree m, and we write

$$g(x) = x^m + c_1 x^{m-1} + \cdots + c_{m-1}x + c_m$$

where $c_1, \cdots, c_l \in \mathbb{Z}$. For every pair of (i, j), we have

$$L_\alpha(\alpha^i \beta_j) = \begin{cases} \alpha^{i+1}\beta_j & \text{if } 0 \leqslant i \leqslant l-2 \\ \alpha^l \beta_j = -c_1\alpha^{l-1}\beta_j - \cdots - c_{l-1}\alpha\beta_j - c_n\beta_j & \text{if } i = l-1. \end{cases}$$

We observe that all coefficients are integers, hence the matrix M associated to the linear transformation L_α under the basis S is a matrix with integer entries. It follows that $T(\alpha)$ and $N(\alpha)$, as the trace and determinant of M, are also integers.

More precisely, the matrix M can be written in the following block diagonal form

$$M = \begin{pmatrix} D & & & \\ & D & & \\ & & \ddots & \\ & & & D \end{pmatrix},$$

where each block along the diagonal is given by

$$D = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -c_m \\ 1 & 0 & 0 & \cdots & 0 & -c_{m-1} \\ 0 & 1 & 0 & \cdots & 0 & -c_{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -c_2 \\ 0 & 0 & 0 & \cdots & 1 & -c_1 \end{pmatrix}.$$

Hence $T(\alpha) = \mathrm{tr}(M) = -nc_1 \in \mathbb{Z}$ and $N(\alpha) = \det(M) = ((-1)^m c_m)^n \in \mathbb{Z}$.