MATH7421 Solutions Week 2

Number Fields, Norms and Traces

1. Note that the set is closed under addition, subtraction and multiplication, since given two elements $x = \frac{p_1(\alpha_1,\alpha_2,...,\alpha_n)}{q_1(\alpha_1,\alpha_2,...,\alpha_n)}$ and $y = \frac{p_2(\alpha_1,\alpha_2,...,\alpha_n)}{q_2(\alpha_1,\alpha_2,...,\alpha_n)}$, we have (suppressing notation):

$$x \pm y = \frac{p_1 q_2 \pm p_2 q_1}{q_1 q_2}$$
$$xy = \frac{p_1 p_2}{q_1 q_2}$$

Note that 0 and 1 are elements of this set. The other commutative ring axioms follow from the fact that the polynomial ring $K[x_1, x_2, ..., x_n]$ is a commutative ring.

To show that this commutative ring is a field, we simply need to show that every non-zero element is invertible. But this is clear, since if $z = \frac{p(\alpha_1,\alpha_2,...,\alpha_n)}{q(\alpha_1,\alpha_2,...,\alpha_n)} \neq 0$ then $p(\alpha_1, \alpha_2, ..., \alpha_n) \neq 0$, and so $z^{-1} = \frac{q(\alpha_1,\alpha_2,...,\alpha_n)}{p(\alpha_1,\alpha_2,...\alpha_n)}$ is well defined.

2. A simple computation shows that multiplying numerator and denominator gives the denominator:

$$\begin{aligned}&(d + e\sqrt[3]{5} + f\sqrt[3]{5}^2)((d^2 - 5ef) + (5f^2 - de)\sqrt[3]{5} + (e^2 - df)\sqrt[3]{5}^2)\\ &= d^2 + 5e^2 + 25f^2 - 15def\end{aligned}$$

which is rational.

3. (a) If $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ and $n \geq 3$ then $K = \mathbb{Q}(\alpha_1, \alpha_2)(\alpha_3, ..., \alpha_n)$. If we have proved the result for the case $n = 2$ then we know that we can write $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\beta_1)$ for some algebraic number β_1. Hence $K = \mathbb{Q}(\beta_1, \alpha_3, ..., \alpha_n)$. We may continue recursively, eventually reducing the number of generators to one.

   (b) We know that $K = \mathbb{Q}(\alpha, \beta)$ contains $\mathbb{Q}$ and α, β. Since K is a field and $c \in K$ it must contain $\alpha + c\beta$, hence contains $\mathbb{Q}(\alpha + c\beta)$.

   (c) Suppose that $m_\beta(\gamma) = f_c(\gamma) = 0$ for some $\gamma \in \mathbb{C}$. Then $\gamma = \beta_i$ for some i and $f_c((\alpha + c\beta) - c\beta_i) = 0$, so that $\alpha + c\beta - c\beta_i = \alpha_j$ for some j. If $(i, j) \neq (1, 1)$ then this equation has solution $c = \frac{\alpha_j - \alpha}{\beta - \beta_i}$. Since K is infinite, we may choose $c \in K$ to not be any of these values, forcing $\gamma = \beta$ (which is clearly a root of both polynomials).

   (d) We know that $g(x)|m_\beta(x)$ and $g(x)|f_c(x)$. However, for our special choice of $c \in K$ these polynomials only have one common root $x = \beta$, so that we must have $g(x)|(x - \beta)$.

Since $\deg(g(x)) \geq 1$ we must have that $g(x) = (x - \beta)$ up to non-zero scaling. As $g(x) \in \mathbb{Q}(\alpha + c\beta)[x]$, we must therefore have that the coefficient $-\beta \in \mathbb{Q}(\alpha + c\beta)$. This shows that $\beta \in \mathbb{Q}(\alpha + c\beta)$ and $\alpha = (\alpha + c\beta) - c\beta \in \mathbb{Q}(\alpha + c\beta)$ (since this is a field). This finishes the proof that $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha + c\beta)$ for some choice of $c \in K$.

4. (a) It is clear that the number $\alpha = \sqrt{7}$ is a root of the polynomial $x^2 - 7 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein's Criterion with $p = 7$. This polynomial must then be the minimal polynomial of α, so we therefore have that:

$$\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} \,|\, a, b \in \mathbb{Q}\}$$

and $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$.

(b) It is clear that the number $\alpha = \sqrt[4]{13}$ is a root of the polynomial $x^4 - 13 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein's Criterion with $p = 13$. This polynomial must then by the minimal polynomial of α, so we therefore have that:

$$\mathbb{Q}(\sqrt[4]{13}) = \{a + b\sqrt[4]{13} + c\sqrt[4]{13}^2 + d\sqrt[4]{13}^3 \,|\, a, b, c, d \in \mathbb{Q}\}$$

and $[\mathbb{Q}(\sqrt[4]{13}) : \mathbb{Q}] = 4$.

(c) Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $(\alpha - \sqrt{2})^2 = 3$, so that $\alpha^2 - 2\alpha\sqrt{2} + 2 = 3$. Rearranging gives $2\alpha\sqrt{2} = \alpha^2 - 1$, so that $(\alpha^2 - 1)^2 = 8\alpha^2$. It follows that $\alpha^4 - 2\alpha^2 + 1 = 8\alpha^2$, so that α is a root of the polynomial $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. We show that this is the minimal polynomial of α by showing that it is irreducible over $\mathbb{Q}$, which can be done using Gauss' Lemma (i.e. show that it doesn't admit a non-trivial factorisation over $\mathbb{Z}$).

First note that the rational root test tells us that if this polynomial has a rational root then it must be $x = \pm 1$. Neither of these values is a root and so there can be no linear factors.

The only other possibility for a non-trivial factorisation over $\mathbb{Z}$ is into two quadratics:

$$x^4 - 10x^2 + 1 = (ax^2 + bx + c)(dx^2 + ex + f).$$

Comparing x^4 coefficients gives $ad = 1$ and we may scale the factorisation by ± 1 so that $a = d = 1$. Comparing x^3 coefficients gives that $e + b = 0$, so that $e = -b$. Comparing constant coefficients gives that $cf = 1$, so that $a = f = \pm 1$.

Our factorisation is now:

$$x^4 - 10x^2 + 1 = (x^2 + bx \pm 1)(x^2 - bx \pm 1).$$

Comparing x^2 coefficients gives $\pm 2 - b^2 = -10$, so that $b^2 = 8$ or $b^2 = 12$. There are no integer solutions to this equation and so such a factorisation must not exists.

We therefore have that:

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \{a + b(\sqrt{2} + \sqrt{3}) + c(\sqrt{2} + \sqrt{3})^2 + d(\sqrt{2} + \sqrt{3})^3 \,|\, a, b, c, d \in \mathbb{Q}\}$$

and $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.

(Challenge: Why didn't we use Eisenstein's Criterion to prove irreducibility? It turns out that it doesn't work for this polynomial...even if you consider all shifts $x + a$ in place of x!)

5. (a) It is clear that $\sqrt{d}$ is a root of the polynomial $x^2 - d \in \mathbb{Q}[x]$, and so it is algebraic. If $d = -1$ then the polynomial $x^2 + 1 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{R}$, hence over $\mathbb{Q}$. If $d \neq 0, \pm 1$ then there exists a prime $q|d$. Since d is square-free we must also have that $q^2 \nmid d$, and so we may use Eisenstein's Criterion with prime q to prove that the polynomial $x^2 - d \in \mathbb{Q}[x]$ is irreducible. It follows that in each case we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

   (b) Suppose that $[K : \mathbb{Q}] = 2$, i.e. that K is a 2-dim vector space over $\mathbb{Q}$. In particular, there must exist $\alpha \in K$ such that $\alpha \notin \mathbb{Q}$. Consider the three elements $1, \alpha, \alpha^2 \in K$. These must be linearly dependent over $\mathbb{Q}$ (since it's a 2-dim vector space!) and so there must exist $a, b, c \in \mathbb{Q}$, not all zero such that $a\alpha^2 + b\alpha + c = 0$.

   If $a = 0$ then we find that $b\alpha + c = 0$. We must have that $b \neq 0$ since otherwise $(a, b, c) = (0, 0, 0)$, and so we find that $\alpha = -\frac{c}{b} \in \mathbb{Q}$. This is a contradiction.

   Hence $a \neq 0$ and α is a root of a quadratic polynomial $ax^2 + bx + c \in \mathbb{Q}[x]$. It follows that $\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ and $K = \mathbb{Q}(\alpha)$.

   Let $d' = \sqrt{b^2 - 4ac}$ and note that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d'})$, since α is in the RHS and $\sqrt{d'}$ is in the LHS (and both fields contain $\mathbb{Q}$ by definition!).

   Finally, by unique factorisation in $\mathbb{Z}$ we can write $d' = \left(\frac{s}{t}\right)^2 d$ for some square-free integer d. It is then clear that $\mathbb{Q}(\sqrt{d'}) = \mathbb{Q}(\frac{s}{t}\sqrt{d}) = \mathbb{Q}(\sqrt{d})$. Note that $d \neq 0, 1$ is forced since $\alpha \notin \mathbb{Q}$.

6. (a) The conjugates of $\sqrt{3}$ are $\pm\sqrt{3}$. It follows that

$$T(2 + 7\sqrt{3}) = (2 + 7\sqrt{3}) + (2 - 7\sqrt{3}) = 4$$

   and

$$N(2 + 7\sqrt{3}) = (2 + 7\sqrt{3})(2 - 7\sqrt{3}) = 4 - 3 \cdot 49 = -143.$$

   (b) The conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}, \zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$, where $\zeta = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$ is a (primitive) cube root of unity. It follows that

$$T(1 + \sqrt[3]{2}) = (1 + \sqrt[3]{2}) + (1 + \zeta\sqrt[3]{2}) + (1 + \zeta^2\sqrt[3]{2}) = 3 + (1 + \zeta + \zeta^2)\sqrt[3]{2} = 3$$

   (since one can check that $1 + \zeta + \zeta^2 = 0$). We also have that

$$N(1+\sqrt[3]{2}) = (1+\sqrt[3]{2})(1+\zeta\sqrt[3]{2})(1+\zeta^2\sqrt[3]{2}) = 1+(1+\zeta+\zeta^2)\sqrt[3]{2}+(\zeta+\zeta^2+\zeta^3)\sqrt[3]{2}^2+2\zeta^3 = 3$$

   (since $1 + \zeta + \zeta^2 = \zeta + \zeta^2 + \zeta^3 = 0$ and $\zeta^3 = 1$).

   (c) The roots of $x^4 - 10x^2 + 1$ are $\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{3} + \sqrt{2}$ and $-\sqrt{2} - \sqrt{3}$. It follows that these are the conjugates of $\sqrt{2} + \sqrt{3}$ and so we have that

$$T(\sqrt{2} + \sqrt{3}) = (\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3}) + (-\sqrt{2} + \sqrt{3}) + (-\sqrt{2} - \sqrt{3}) = 0$$

   and

$$N(\sqrt{2} + \sqrt{3}) = (\sqrt{2} + \sqrt{3})(\sqrt{2} - \sqrt{3})(-\sqrt{2} + \sqrt{3})(-\sqrt{2} - \sqrt{3}) = (2 - 3)(2 - 3) = 1$$

7. Let $\alpha_1, \alpha_2, ..., \alpha_d$ be the conjugates of α. Consider the factorisation of $m_\alpha(x)$:

$$m_\alpha(x) = \prod_{i=1}^{d}(x - \alpha_i).$$

We have that:

$$N(a - b\alpha) = \prod_{i=1}^{d} \sigma_i(a - b\alpha) = \prod_{i=1}^{d}(a - b\sigma_i(\alpha)) = \prod_{i=1}^{d}(a - b\alpha_i) = b^d \prod_{i=1}^{d}\left(\frac{a}{b} - \alpha_i\right) = b^d m_\alpha\left(\frac{a}{b}\right).$$

For $\alpha = \sqrt[3]{2}$ we have that $m_\alpha(x) = x^3 - 2$ and so $N(1 + \sqrt[3]{2}) = (-1)^3 m_\alpha(1)(-1) = (-1)((-1)^3 - 2) = 3$.

8. (a) We know by definition that $\Delta(\beta_1, \beta_2, ..., \beta_d) = \det(M_{\beta_1,\beta_2,...,\beta_d})^2$, where

$$M_{\beta_1,\beta_2,...,\beta_d} = \begin{pmatrix} \sigma_1(\beta_1) & \sigma_1(\beta_2) & \dots & \sigma_1(\beta_d) \\ \sigma_2(\beta_1) & \sigma_2(\beta_2) & \dots & \sigma_2(\beta_d) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_d(\beta_1) & \sigma_d(\beta_2) & \dots & \sigma_d(\beta_d) \end{pmatrix}.$$

By the hint we may write $\Delta(\beta_1, \beta_2, ..., \beta_d) = \det(M^T_{\beta_1,\beta_2,...,\beta_d} M_{\beta_1,\beta_2,...,\beta_d})$. This matrix has (i,j)-entry $\sum_{k=1}^{d} \sigma_k(\beta_i)\sigma_k(\beta_j) = \sum_{k=1}^{d} \sigma_k(\beta_i\beta_j) = T(\beta_i\beta_j) \in \mathbb{Q}$, and so the determinant of this matrix must be rational. Hence $\Delta(\beta_1, \beta_2, ..., \beta_d) \in \mathbb{Q}$.

To show that it is non-zero, note that if $\Delta(\beta_1, \beta_2, ..., \beta_d) = 0$ then the rational matrix

$$M^T_{\beta_1,\beta_2,...,\beta_d} M_{\beta_1,\beta_2,...,\beta_d} = \begin{pmatrix} T(\beta_1^2) & T(\beta_1\beta_2) & ... & T(\beta_1\beta_d) \\ T(\beta_2\beta_1) & T(\beta_2^2) & ... & T(\beta_2\beta_d) \\ \vdots & \vdots & \ddots & \vdots \\ T(\beta_d\beta_1) & T(\beta_d\beta_2) & ... & T(\beta_d^2) \end{pmatrix}$$

has determinant 0, so that it's rows are linearly dependent over $\mathbb{Q}$. Hence, there exists $c_1, c_2, ..., c_d \in \mathbb{Q}$, not all zero, such that:

$$c_1 T(\beta_1\beta_j) + c_2 T(\beta_2\beta_j) + ... + c_d T(\beta_d\beta_j) = 0$$

for each j. However, by linearity this implies that $T((c_1\beta_1 + c_2\beta_2 + ... + c_d\beta_d)\beta_j) = 0$ for each j.

Letting $x = c_1\beta_1 + c_2\beta_2 + ... + c_d\beta_d \in \mathbb{Q}(\alpha)\backslash\{0\}$, we see that $T(x\beta_j) = 0$ for each j. But this implies that $T(xy) = 0$ for every $y \in \mathbb{Q}(\alpha)$ (since the β_j form a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$). However, since $x \neq 0$ we may choose $y = x^{-1} \in \mathbb{Q}(\alpha)$ and find that $T(xx^{-1}) = T(1) = d \neq 0$, which is a contradiction. Hence $\Delta(\beta_1, \beta_2, ..., \beta_d) \neq 0$.

(b) This follows from the fact that the σ_i are field homomorphisms. The (i,j) entry of $M_{\beta'_1,\beta'_2,...,\beta'_d}$ is

$$\sigma_i(\beta'_j) = \sigma_i(\sum_{i=1}^{d} c_{i,j}\beta_j) = \sum_{i=1}^{d} c_{i,j}\sigma_i(\beta_j).$$

This is the (i,j) entry of $CM_{\beta_1,\beta_2,...,\beta_d}$, and so

$$\begin{aligned} \Delta(\beta'_1, \beta'_2, ..., \beta'_d) = \det(M_{\beta'_1,\beta'_2,...,\beta'_d})^2 &= \det(CM_{\beta_1,\beta_2,...,\beta_d})^2 \\ &= \det(C)^2 \det(M_{\beta_1,\beta_2,...,\beta_d})^2 \\ &= \det(C)^2 \Delta(\beta_1, \beta_2, ..., \beta_d). \end{aligned}$$

9. (a) Recall Leibniz's formula for determinants:

$$\det(a_{i,j}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Note that for our matrix:

$$\prod_{i=1}^{n} a_{i,\sigma(i)} = \prod_{i=1}^{n} x_i^{\sigma(i)-1},$$

which is a monomial of total degree $\sum_{i=1}^{n}(\sigma(i)-1) = 0+1+2+...+n-1 = \frac{n(n-1)}{2} = \binom{n}{2}$. Thus $\det(V)$ is a polynomial of degree $\binom{n}{2}$ in $\mathbb{Q}[x_1, x_2, .., x_n]$ (since it is a signed sum of such monomials, and $\pm 1 \in \mathbb{Q}$).

Now note that setting $x_j = x_i$ for any $1 \leq i < j \leq n$ forces two rows of V to be equal, so that $\det(V) = 0$ in this case. It follows that $(x_j - x_i) \,|\, \det(V)$ for each such i, j. Since these linear polynomials are coprime in $\mathbb{Q}[x_1, x_2, ..., x_n]$ we must have that $\prod_{1 \leq i < j \leq n}(x_j - x_i) \,|\, \det(V)$.

However, the product on the LHS also has degree $\binom{n}{2}$ and so we must have that $\det(V) = c\prod_{1 \leq i < j \leq n}(x_j - x_i)$ for some constant $c \in \mathbb{Q}$.

We must have that $c = 1$ since there is only one term in the determinant of the form $x_2 x_3^2 ... x_n^{n-1}$ (i.e. the product of the diagonal entries of V) and this term appears in the product with coefficient c. Thus $\det(V) = \prod_{1 \leq i < j \leq n}(x_j - x_i)$.

(b) We find that:

$$\Delta(1, \gamma, \gamma^2, ..., \gamma^{d-1}) = \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\gamma) & \sigma_1(\gamma^2) & ... & \sigma_1(\gamma^{d-1}) \\ \sigma_2(1) & \sigma_2(\gamma) & \sigma_2(\gamma^2) & ... & \sigma_2(\gamma^{d-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_d(1) & \sigma_d(\gamma) & \sigma_d(\gamma^2) & ... & \sigma_d(\gamma^{d-1}) \end{pmatrix}^2$$

$$= \det \begin{pmatrix} 1 & \sigma_1(\gamma) & \sigma_1(\gamma)^2 & ... & \sigma_1(\gamma)^{d-1} \\ 1 & \sigma_2(\gamma) & \sigma_2(\gamma)^2 & ... & \sigma_2(\gamma)^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_d(\gamma) & \sigma_d(\gamma)^2 & ... & \sigma_d(\gamma)^{d-1} \end{pmatrix}^2$$

This matrix is a Vandermonde matrix, hence by part (a) we have:

$$\Delta(1, \gamma, \gamma^2, ..., \gamma^{d-1}) = \prod_{1 \leq i < j \leq d} (\sigma_j(\gamma) - \sigma_i(\gamma))^2 = (-1)^{\frac{d(d-1)}{2}} \prod_{i \neq j} (\sigma_j(\gamma) - \sigma_i(\gamma)),$$

since we need $\binom{d}{2} = \frac{d(d-1)}{2}$ sign changes to flip the terms in the brackets with $1 \leq j \leq i \leq d$.

Now note that $m_\gamma(x) = \prod_{i=1}^{d}(x - \sigma_i(\gamma))$, since the quantities $\sigma_i(\gamma)$ are the conjugates of γ (which are by definition the roots of $m_\gamma(x)$).

The derivative of $m_\gamma(x)$ is $m'_\gamma(x) = \sum_{t=1}^{d} \prod_{i \neq t}(x - \sigma_i(\gamma))$. It follows that:

$$N(m'_\gamma(\gamma)) = \prod_{j=1}^{d} \sigma_j(m'_\gamma(\gamma)) = \prod_{j=1}^{d} m'_\gamma(\sigma_j(\gamma)) = \prod_{j=1}^{d} \left(\sum_{t=1}^{d} \prod_{i \neq t} (\sigma_j(\gamma) - \sigma_i(\gamma)) \right).$$

Note that each bracket on the RHS consists of a sum of products, with each product omitting the term $(\sigma_j(\gamma) - \sigma_t(\gamma))$. If $j \neq t$ then this product will contain the term $(\sigma_j(\gamma) - \sigma_j(\gamma)) = 0$, so contributes 0 to the bracket. Hence only the case $j = t$ contributes, so that:

$$N(m'_\gamma(\gamma)) = \prod_{j=1}^{d} \left(\prod_{i \neq j} (\sigma_j(\gamma) - \sigma_i(\gamma)) \right) = \prod_{i \neq j} (\sigma_j(\gamma) - \sigma_i(\gamma)),$$

proving the claim.

10. (a) We rationalise the denominator of $\frac{1}{a+b\sqrt{d}}$ as follows:

$$\frac{1}{a+b\sqrt{d}} = \frac{1}{a+b\sqrt{d}} \cdot \frac{a-b\sqrt{d}}{a-b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2},$$

which has rational denominator and is non-zero (since $(a,b) \neq (0,0)$ and $d \neq 0,1$ is square-free.

Notice that all we did was multiply numerator and denominator by the non-trivial conjugate of $a+b\sqrt{d}$, and the denominator becomes the norm $N(a+b\sqrt{d}) = a^2 - db^2$.

(b) We know that $N(\beta) = \prod_{i=1}^{d} \sigma_i(\beta) \in \mathbb{Q}$, and it is non-zero since $\beta \neq 0$ (recall that the σ_i are injective embeddings of K into $\mathbb{C}$ and so if $\sigma_i(\beta) = 0$ for any i then $\beta = 0$.

Order the embeddings so that $\sigma_1(\beta) = \beta$. Letting $\gamma = \prod_{i=2}^{d} \sigma_i(\beta) = \frac{N(\beta)}{\beta} \in \mathbb{Q}(\alpha)$, we see that:

$$\frac{1}{\beta} = \frac{1}{\beta}\frac{\gamma}{\gamma} = \frac{\gamma}{\beta\gamma} = \frac{\gamma}{N(\beta)},$$

which has rational non-zero denominator.