MATH7421 Problems Week 2

Number Fields, Norms and Traces

1. Let K be a field. In the notes we defined the extension field $K(\alpha_1, \alpha_2, ..., \alpha_n)$ to be the smallest field containing K and $\alpha_1, \alpha_2, ..., \alpha_n$. We then showed that $K(\alpha_1, \alpha_2, ..., \alpha_n)$ contains the set:
$$\left\{ \frac{p(\alpha_1, \alpha_2, ..., \alpha_n)}{q(\alpha_1, \alpha_2, ..., \alpha_n)} \,\middle|\, \frac{p(x_1, x_2, ..., x_n)}{q(x_1, x_2, ..., x_n)} \in K[x_1, x_2, ..., x_n] \quad \text{and} \quad q(\alpha_1, \alpha_2, ..., \alpha_n) \neq 0 \right\}.$$
Show that this set is a field, so that in fact we have equality.

2. Let $(d, e, f) \neq (0, 0, 0)$ be a triple of rational numbers. We claimed in the notes that we can rationalise the denominator of:
$$\frac{1}{d + e\sqrt[3]{5} + f\sqrt[3]{5}^2}$$
by multiplying numerator and denominator by $(d^2 - 5ef) + (5f^2 - de)\sqrt[3]{5} + (e^2 - df)\sqrt[3]{5}^2$. Show that this claim is true.

3. In the notes, it was promised that every number field is of the form $\mathbb{Q}(\alpha)$ for some algebraic number α. In this exercise we will prove this fact.

   (a) A general number field is of the form $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ for algebraic numbers $\alpha_1, ..., \alpha_n$. Show that it suffices to prove the claim for the case $n = 2$.

   (b) Let $K = \mathbb{Q}(\alpha, \beta)$ with α, β algebraic numbers. Show that $\mathbb{Q}(\alpha + c\beta) \subseteq K$ for every $c \in K$.

   (c) We will now show that there exists $c \in K$ such that $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha + c\beta)$, proving the claim for the case $n = 2$.

   Suppose that the minimal polynomials of α and β factor as follows:
$$m_\alpha(x) = \prod_{i=1}^{n}(x - \alpha_i)$$
$$m_\beta(x) = \prod_{i=1}^{m}(x - \beta_i)$$
   with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. The α_i are distinct and similarly for the β_i (by Exercise 7 of Week 1, irreducible polynomials in $\mathbb{Q}[x]$ cannot have repeated roots).

   For each $c \in K$ consider the polynomial $f_c(x) = m_\alpha((\alpha + c\beta) - cx)$. Show that there exists a value of $c \in K$ such that the polynomials $m_\alpha(x)$ and $f_c(x)$ have at most one common root, which is $x = \beta$.

(d) Let $g(x)$ be the minimal polynomial of β over $\mathbb{Q}(\alpha+c\beta)$. Show that $g(x)=x-\beta$, so that $\beta\in\mathbb{Q}(\alpha+c\beta)$. Hence show that $\mathbb{Q}(\alpha,\beta)\subseteq\mathbb{Q}(\alpha+c\beta)$.

4. Show that each of the following numbers α are algebraic, find their minimal polynomials, give explicit descriptions of the number field $\mathbb{Q}(\alpha)$ and state the values of the degree $[\mathbb{Q}(\alpha):\mathbb{Q}]$:

   (a) $\alpha=\sqrt{7}$

   (b) $\alpha=\sqrt[4]{13}$

   (c) $\alpha=\sqrt{2}+\sqrt{3}$

5. (a) Let $d\neq 0,1$ be a square-free integer. Show that $\sqrt{d}$ is algebraic and that $K=\mathbb{Q}(\sqrt{d})$ is a quadratic number field, i.e. $[K:\mathbb{Q}]=2$.

   (b) Show that every quadratic number field is of the form $K=\mathbb{Q}(\sqrt{d})$ for some square-free integer $d\neq 0,1$.

6. Compute the norms and traces of the following elements in the following number fields:

   (a) $2+7\sqrt{3}\in\mathbb{Q}(\sqrt{3})$

   (b) $1+\sqrt[3]{2}\in\mathbb{Q}(\sqrt[3]{2})$

   (c) $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$ (Hint: as we saw earlier, the minimal polynomial is x^4-10x^2+1).

7. Let $K=\mathbb{Q}(\alpha)$ be a number field and $m_\alpha(x)$ be the minimal polynomial of the algebraic number α. Show that if $a,b\in\mathbb{Q}$ then $N(a-b\alpha)=b^d m_\alpha\left(\frac{a}{b}\right)$. Use this formula to efficiently find the norm in Exercise 6(b).

   (Hint: Use the factorisation of $m_\alpha(x)$ into linears).

8. Let $\mathbb{Q}(\alpha)$ be a number field of degree d and $\beta_1,\beta_2,...,\beta_d\in\mathbb{Q}(\alpha)$ be a basis.

   (a) Show that $\Delta(\beta_1,\beta_2,...,\beta_d)\in\mathbb{Q}\backslash\{0\}$.
   (Hint: If M is a matrix then $\det(M)^2=\det(M^TM)$. What is the matrix M^TM in this case? Where does its entries live? What happens if $\det(M)=0$?)

   (b) If $\beta'_j=\sum_{i=1}^d c_{i,j}\beta_i$ for some $c_{i,j}\in\mathbb{Q}$ then

   $$\Delta(\beta'_1,\beta'_2,...,\beta'_d)=(\det(C))^2\Delta(\beta_1,\beta_2,...,\beta_d)$$

   where C is the matrix having (i,j)-entry $c_{i,j}$.

9. (a) Let $x_1,x_2,...,x_n$ be variables and consider the Vandermonde matrix:

   $$V=\begin{pmatrix}1 & x_1 & x_1^2 & \dots & x_1^{n-1}\\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & x_n & x_n^2 & \dots & x_n^{n-1}\end{pmatrix}$$

   Show that $\det(V)=\prod_{1\leq i<j\leq n}(x_j-x_i)$.

   (Hint: Show that it's a polynomial in $\mathbb{Q}[x_1,x_2,...,x_n]$ of degree $\binom{n}{2}$ and show that it must be divisible by (x_j-x_i) for each $1\leq i<j\leq n$).

(b) Use part (a) to show that if γ is an algebraic number with $\deg(m_\gamma(x)) = d$ then

$$\Delta(1, \gamma, \gamma^2, ..., \gamma^{d-1}) = (-1)^{\frac{d(d-1)}{2}} N(m'_\alpha(\alpha))$$

where $m'_\alpha(x)$ is the derivative of $m_\alpha(x)$.

10. Earlier we saw how to rationalise denominators in the unfamiliar situation of cubic denominators, but there was no explanation of how this was done. It's time to reveal to you how to rationalise the denominator in general...

(a) Let $d \neq 0, 1$ be square-free and $(a, b) \neq (0, 0)$ be rational. Remind yourself of how to rationalise the denominator of $\frac{1}{a+b\sqrt{d}} \in \mathbb{Q}(\sqrt{d})$ and rewrite the recipe in the language of conjugates and norms.

(b) Let K be a number field of degree d with embeddings σ_i for $1 \leq i \leq d$. If $\beta \in K \backslash \{0\}$ then construct an explicit $\gamma \in K$ that rationalises the denominator of $\frac{1}{\beta} \in K$. Prove that your construction works.