Algebraic number theory
Solutions to exercise sheet for chapter 1

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk)
Aurel Page (a.r.page@warwick.ac.uk)
TAs: Chris Birkbeck (c.d.birkbeck@warwick.ac.uk),
George Turcas(g.c.turcas@warwick.ac.uk)

Version: February 20, 2017

Answers must be submitted by Tuesday January 31, 14:00

Exercise 1 (10 points)

Let $K = \mathbb{Q}(\sqrt{3})$, and let $\alpha = a + b\sqrt{3}$ $(a, b \in \mathbb{Q})$ be an element of K. Compute the trace, norm, and characteristic polynomial of α in terms of a and b

1. (5 points) *by writing down the matrix of the multiplication-by-α map with respect to the $\mathbb{Q}$-basis of K of your choice,*

   Since $\sqrt{3} \notin \mathbb{Q}$ but $x^2 - 3 \in \mathbb{Q}[x]$, we find that $\sqrt{3}$ is algebraic over $\mathbb{Q}$ of degree 2, so that 1 and $\sqrt{3}$ from a $\mathbb{Q}$-basis of K.

   With respect to this basis, the matrix of the multiplication-by-α map is

   $$M = \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$$

   since $\alpha \cdot 1 = a + b\sqrt{3}$ and $\alpha \cdot \sqrt{3} = 3b + a\sqrt{3}$, so that

   $$\operatorname{Tr}^K_{\mathbb{Q}}(\alpha) = \operatorname{Tr} M = 2a,$$

   $$N^K_{\mathbb{Q}}(\alpha) = \det M = a^2 - 3b^2,$$

   $$\text{and } \chi^K_{\mathbb{Q}}(\alpha) = \text{char. poly.}(M) = x^2 - 2ax + a^2 - 3b^2.$$

2. (5 points) *by considering complex embeddings.*

   Since α is algebraic of degree 2, we have $[K : \mathbb{Q}] = 2$, so there are 2 embeddings of K into $\mathbb{C}$, which correspond to the complex roots of the minimal polynomial of $\sqrt{3}$ in that they send $\sqrt{3}$ to the root they correspond to. Here, these complex roots are $\pm\sqrt{3}$, so one of the embeddings sends $\sqrt{3}$ to $\sqrt{3}$, and the other one sends $\sqrt{3}$ to $-\sqrt{3}$. As they are embeddings, they are also $\mathbb{Q}$-linear, so the first one sends α to $u = a + b\sqrt{3}$, and the other one sends α to $v = a - b\sqrt{3}$ (so actually both these embeddings are actually embeddings in $\mathbb{R} \subset \mathbb{C}$). As a result,

$$\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha) = u + v = 2a,$$

$$N_{\mathbb{Q}}^{K}(\alpha) = uv = a^2 - 3b^2,$$

$$\text{and } \chi_{\mathbb{Q}}^{K}(\alpha) = (x-u)(x-v) = x^2 - 2ax + a^2 - 3b^2.$$

Exercise 2 (40 points)

In this exercise, you may assume[1] *that the polynomial* $x^3 - 2$ *is irreducible over* $\mathbb{Q}$.

1. (8 points) *Let* $K = \mathbb{Q}(\sqrt[3]{2})$, *and let* $\alpha = \frac{\sqrt[3]{2}+1}{\sqrt[3]{2}-1} \in K$. *Find* $a, b, c \in \mathbb{Q}$ *such that* $\alpha = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$.

   Let us first express $\frac{1}{\sqrt[3]{2}-1}$ as a polynomial in $\sqrt[3]{2}$. For this, we want to find polynomials $U, V \in \mathbb{Q}[x]$ such that $U(x)(x^3-2) + V(x)(x-1) = 1$; indeed, evaluating at $x = \sqrt[3]{2}$ will then yield $V(\sqrt[3]{2})(\sqrt[3]{2}-1) = 1$ (notice that this is a concrete example of the argument used in the proof of the fact that $K[\alpha]$ is a field whenever α is algebraic over K).

   To find U and V, we perform the Euclidian division of $x^3 - 2$ by $x - 1$, which yields
   $$x^3 - 2 = (x^2 + x + 1)(x - 1) - 1.$$

   We may thus take $U = -1$, $V = x^2 + x + 1$, and we find that

   $$\frac{1}{\sqrt[3]{2} - 1} = \sqrt[3]{2}^2 + \sqrt[3]{2} + 1.$$

   Therefore,

   $$\alpha = (\sqrt[3]{2} + 1)(\sqrt[3]{2}^2 + \sqrt[3]{2} + 1) = 2\sqrt[3]{2}^2 + 2\sqrt[3]{2} + 3,$$

   we may thus take $a = 3$, $b = c = 2$.

2. (4 points) *Are these rational numbers* a, b, c *unique ?*

   Yes. Indeed, since $x^3 - 2$ is irreducible over $\mathbb{Q}$, it is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$, so $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ is a $\mathbb{Q}$-basis of K.

3. (2 points) *What is the degree of* K *?*

   This degree is the same as the degree of the minimal polynomial of $\sqrt[3]{2}$, that is to say 3.

[1] We will see an efficient way (Eisenstein's criterion) to prove this in chapter 3.

4. (7 points) *Prove that* $\sqrt{2} \notin K$.

   If we had $\sqrt{2} \in K$, then we would have $\mathbb{Q}(\sqrt{2}) \subseteq K$. But this would imply

   $$3 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[K : \mathbb{Q}(\sqrt{2})],$$

   which is impossible since $[K : \mathbb{Q}(\sqrt{2})]$ is an integer.

5. (7 points) *Prove that* $K = \mathbb{Q}(\alpha)$.

   If α were rational, then writing $\alpha = \alpha + 0 \cdot \sqrt[3]{2} + 0 \cdot (\sqrt[3]{2})^2$ would contradict the unicity of the rationals a, b, c. So $\alpha \notin \mathbb{Q}$, and thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$.

   But we also have

   $$3 = [K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}],$$

   and since 3 is prime and $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$, we must have $[K : \mathbb{Q}(\alpha)] = 1$, which means that $\mathbb{Q}(\alpha) = K$.

6. (12 points) *Compute the trace, norm, and characteristic polynomial of* α, *and use the previous question to prove that this polynomial is irreducible over* $\mathbb{Q}$.

   Using complex embeddings would lead us to computing with both $\sqrt[3]{2}$ and $e^{2\pi i/3}$, which sounds really tedious, so instead we compute that the matrix of the multiplication-byα map with respect to the $\mathbb{Q}$-base $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ of K, which turns out to be

   $$\begin{pmatrix} 3 & 4 & 4 \\ 2 & 3 & 4 \\ 2 & 2 & 3 \end{pmatrix}.$$

   We then compute $\chi_{\mathbb{Q}}^{K}(\alpha)$ as the characteristic polynomial of this matrix; after some effort, we find

   $$\chi_{\mathbb{Q}}^{K}(\alpha) = x^3 - 9x^2 + 3x - 3.$$

   From the coefficients of x^2 and x^0 respectively, we finally deduce that $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha) = 9$ and that $N_{\mathbb{Q}}^{K}(\alpha) = 3$.

Exercise 3 (30 points)

1. (3 points) *Let* $K = \mathbb{Q}(\sqrt{2})$. *Prove that* $i \notin K$.

   The field K may be embedded in $\mathbb{R}$. As a consequence, if $i \in K$, then there exists a $\iota \in \mathbb{R}$ such that $\iota^2 = -1$, but this is clearly not the case.

2. (5 points) *Let* $L = \mathbb{Q}(\sqrt{2}, i)$. *Compute* $[L : \mathbb{Q}]$.

   Since i is a root of $F(x) = x^2 + 1 \in K[x]$, it is algebraic of degree at most 2 over K. But $F(x)$ cannot be reducible over K, else it would split into degree 1 factors and i would lie in K, so $F(x)$ is the minimal polynomial of i over K and thus $\deg_K i = 2$. Therefore,

   $$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = [K(i) : K][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = (\deg_K i)(\deg_{\mathbb{Q}} \sqrt{2}) = 2 \cdot 2 = 4.$$

3. (5 points) *What is the signature of L ?*

   Since $i \in L$, L cannot be embedded into $\mathbb{R}$ for the same reason as in question 1. Therefore, its signature is of the form $(0, r_2)$, and since $2r_2 = [L : \mathbb{Q}]$, this signature is actually $(0, 2)$.

4. (6 points) *Let $\alpha = \sqrt{2} + i \in L$. Compute the characteristic polynomial $\chi_{\mathbb{Q}}^{L}(\alpha)$ of α with respect to the extension $L/\mathbb{Q}$.*

   As in exercise 1, we have two methods. We could write down the matrix of the multiplication-by-α map, but since $[L : \mathbb{Q}] = 4$ this matrix has size 4 × 4 and computing its characteristic polynomial would be tedious. So we use the complex embeddings, but first we must determine them.

   We know that $[K : \mathbb{Q}] = 2$, so K has two embeddings into $\mathbb{C}$, one that sends $\sqrt{2}$ to $\sqrt{2}$ whereas the other one sends $\sqrt{2}$ to $-\sqrt{2}$. As $[L : K] = 2$, both these embeddings extend into 2 embeddings of L into $\mathbb{C}$, one that sends i to i whereas the other one sends i to $-i$. We thus have 4 embeddings, which send α to $\pm\sqrt{2} \pm i$ with all 4 possible combinations of signs, so the characteristic polynomial of α with respect to $L/\mathbb{Q}$ is

$$\begin{aligned} & (x-\sqrt{2}-i)(x-\sqrt{2}+i)(x+\sqrt{2}-i)(x+\sqrt{2}+i) \\ =& \big((x-\sqrt{2})^2+1\big)\big((x+\sqrt{2})^2+1\big) \\ =& (x^2+3-2\sqrt{2}x)((x^2+3+2\sqrt{2}x) \\ =& (x^2+3)^2-(2\sqrt{2}x)^2 \\ =& x^4-2x^2+9. \end{aligned}$$

5. (5 points) *Is the polynomial $\chi_{\mathbb{Q}}^{L}(\alpha)$ squarefree? What does this tell us about α?*

   We could determine if this polynomial is squarefree by computing its GCD with its derivative by successive Euclidian divisions, but this would be rather tedious. Instead, we can just notice from the previous answer that $\chi_{\mathbb{Q}}^{L}(\alpha)$ has no repeated roots in $\mathbb{C}$, so it is squarefree.

   This implies that α is actually a *primitive element* for the extension $L/\mathbb{Q}$, so that
$$\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i).$$

6. (6 points) *Compute the characteristic polynomial $\chi_{K}^{L}(\alpha)$ of α with respect to the extension L/K.*

   Again, two methods : matrix and complex embeddings. Here, both are reasonable, so we explain both.

   Matrix: With respect to the K-basis $1, i$ of L, the matrix of the multiplication by α is
$$\begin{pmatrix} \sqrt{2} & -1 \\ 1 & \sqrt{2} \end{pmatrix},$$

whose characteristic polynomial is

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x + 3.$$

Embeddings: Let us fix an embedding σ of K into $\mathbb{C}$, for instance the one that sends $\sqrt{2}$ to $\sqrt{2}$. This embedding extends into $[L : K] = 2$ embeddings of L into $\mathbb{C}$, that send i to $\pm i$ and thus α to $\sqrt{2} \pm i$. Thus

$$\chi_K^L(\alpha)^\sigma = (x - \sqrt{2} - i)(x - \sqrt{2} + i) = x^2 - 2\sqrt{2}x + 3 \in \mathbb{C}[x].$$

To recover $\chi_K^L(\alpha)$ from $\chi_K^L(\alpha)^\sigma$, we apply σ^{-1} to the coefficients and we find

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x + 3 \in K[x].$$

Just to be complete, here's what would happen if, for some obscure reason, we had picked σ such that $\sigma(\sqrt{2}) = -\sqrt{2}$: The embeddings of L that extend σ send α to $-\sqrt{2} \pm i$, so

$$\chi_K^L(\alpha)^\sigma = (x + \sqrt{2} - i)(x + \sqrt{2} + i) = x^2 + 2\sqrt{2}x + 3 \in \mathbb{C}[x].$$

Applying σ^{-1} affects the coefficient of x nontrivially, and we find again that

$$\chi_K^L(\alpha) = x^2 - 2\sqrt{2}x + 3 \in K[x].$$

Exercise 4 (20 points)

In this exercise, you may freely assume that π and e are both transcendental over $\mathbb{Q}$.

1. (5 points) *Prove that e and π are both algebraic over the field $\mathbb{Q}(e + \pi, e\pi)$.*

   Simply notice that the coefficients of the polynomial

   $$(x - e)(x - \pi) = x^2 - (e + \pi)x + e\pi$$

   all lie in $\mathbb{Q}(e + \pi, e\pi)$.

2. (15 points) *Deduce that at least one of the numbers $e+\pi$ and $e\pi$ is transcendental over $\mathbb{Q}$.*

   Suppose on the contrary that $e + \pi$ and $e\pi$ are both algebraic over $\mathbb{Q}$, and let $S(x) \in \mathbb{Q}[x]$ and $P(x) \in \mathbb{Q}[x]$ de their respective minimal polynomials, and s and $p \in \mathbb{N}$ their degrees. Then $K = \mathbb{Q}(e + \pi)$ is an extension of $\mathbb{Q}$ of degree s, over which $P(x)$ may or may not factor. If it does, let $F(x) \in K[x]$ an the irreducible factor which vanishes at $e\pi$, else let $F(x) = P(x)$. Either way, $F(x)$ is the minimal polynomial of $e\pi$ over K, and its degree is at most p. As a consequence, if we let $L = \mathbb{Q}(e + \pi, e\pi) = K(e\pi)$, we have

   $$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = \deg F \cdot s \leqslant ps.$$

Besides, we have seen that π is the root of a polynomial of degree 2 and coefficients in L, so π is algebraic over L of degree at most 2. Therefore, $L(\pi)$ is a finite extension of L, so

$$[L(\pi) : \mathbb{Q}] = [L(\pi) : L][L : \mathbb{Q}] \leqslant 2ps,$$

so π lies in a finite extension of $\mathbb{Q}$. But this contradicts the fact that π is transcendental over $\mathbb{Q}$.

UNASSESSED QUESTIONS

Exercise 5

Let K be a field, L a finite extension of K of degree n, and $f(x) \in K[x]$ a polynomial of degree m which is irreducible over K.

1. *Prove that if m and n are coprime, then $f(x)$ remains irreducible over L. Hint: Consider a root α of $f(x)$ in some large enough field containing L, what is the degree of $L(\alpha)$ over K ?*

   As suggested, let us consider a root α of $f(x)$ in some large enough extension of L. If $f(x)$ were reducible over L, then the minimal polynomial of α over L would be a strict factor of $f(x)$; in particular, its degree, say d, would be strictly less than m.

   Consider now the following extension diagram, which summarises our situation:

$$\begin{tikzcd}
& L(\alpha) \arrow[dl, equal] \arrow[dr, equal] & \\
K(\alpha) \arrow[dr, equal] & & L \arrow[dl, equal] \\
& K &
\end{tikzcd}$$

   We see that we have two ways to compute $[L(\alpha) : K]$:

$$[L(\alpha) : K] = [L(\alpha) : L][L : K] = dn,$$

   and

$$[L(\alpha) : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K] = m[L(\alpha) : K(\alpha)],$$

   since $f(x)$, being irreducible over K, is (up to scaling) the minimal polynomial of α over K.

   In particular, both m and n divide $[L(\alpha) : K]$, and since they are coprime, $[L(\alpha) : K]$ is actually divisible by mn. But this contradicts $[L(\alpha) : K] = dn$ and $m < d$.

2. *Is the conclusion the same if m and n are not coprime ?*

   Certainly not ! For instance, if we take $L = K(\alpha)$, then $f(x)$ has at least one root in L, namely α, so $x - \alpha \in L[x]$ divides $f(x)$, which is therefore reducible unless it has degree 1. For instance, take $K = \mathbb{R}$ and $f(x) = x^2 + 1$, which is irreducible over $\mathbb{R}$, but not over $L = \mathbb{C}$.

Exercise 6

Let $K = \mathbb{Q}(\alpha)$ be a number field, let $A(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α, and let $\beta = B(\alpha) \in K$, where $B(x) \in \mathbb{Q}[x]$ is some polynomial. Express the characteristic polynomial $\chi_{\mathbb{Q}}^{K}$ of β in terms of a resultant involving A and B.

Let Σ be the set of embeddings of K into $\mathbb{C}$. When σ ranges over Σ, then $\sigma(\alpha)$ ranges over the complex roots of $A(x)$, so that

$$\begin{aligned}
\chi_{\mathbb{Q}}^{K}(\beta) &= \prod_{\sigma \in \Sigma} \big(x - \sigma(\beta)\big) \\
&= \prod_{\sigma \in \Sigma} \big(x - \sigma(B(\alpha))\big) \\
&= \prod_{\sigma \in \Sigma} \big(x - B(\sigma(\alpha))\big) \\
&= \prod_{\substack{z \in \mathbb{C} \\ A(z)=0}} \big(x - B(z)\big) \\
&= \operatorname{Res}_y \big(A(y), x - B(y)\big)
\end{aligned}$$

where the resultant is computed in $\mathbb{C}(x)[y]$.

Remark: Algorithmically speaking, this is in general the fastest way to compute characteristic polynomials.