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)
TA: Pedro Lemos (lemos.pj@gmail.com)

March 2, 2017

Exercise 1

Let $K = \mathbb{Q}[\sqrt[3]{2}]$, and let $\beta = 1 + \sqrt[3]{2} \in K$. Use a Bézout identity to compute $1/\beta$ as a polynomial in $\sqrt[3]{2}$ with coefficients in $\mathbb{Q}$.

Let $A = x^3 - 2$, so that $A(\sqrt[3]{2}) = 0$, and let $B = x + 1$, so that $\beta = B(\sqrt[3]{2})$. Since A is irreducible over $\mathbb{Q}$ and $\deg B < \deg A$, A and B are coprime in $\mathbb{Q}[x]$, so there exist $U, V \in \mathbb{Q}[x]$ such that $UA + VB = 1$. For instance, Euclidian division reveals that

$$x^3 - 2 = (x + 1)(x^2 - x + 1) - 3,$$

so we may take

$$U = -\frac{1}{3}, \quad V = \frac{x^2 - x + 1}{3}.$$

Evaluating at $x = \sqrt[3]{2}$, we find that $V(\sqrt[3]{2})\beta = 1$, whence

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

Exercise 2

Let $\alpha \in \mathbb{C}$, $\beta \in \mathbb{C}^*$ be algebraic numbers. Use resultants to prove that α/β is also an algebraic number.

As α and β are algebraic, there exist nonzero polynomials $A, B\mathbb{Q}[x]$ such that $A(\alpha) = B(\beta) = 0$, and which we may assume are monic. These polynomials must factor over $\mathbb{C}$ as

$$A = \prod_{i=1}^{m}(x - \alpha_i), \quad B = \prod_{j=1}^{n}(x - \beta_j)$$

where $\alpha_1 = \alpha$ and $\beta_1 = \beta$, and so, in $\mathbb{C}[x][y]$, we have

$$\begin{aligned}\operatorname{Res}_y\big(A(y), B(xy)\big) &= \prod_{i=1}^m B(x\alpha_i) \\ &= \prod_{i=1}^m \prod_{j=1}^n (x\alpha_i - \beta_j),\end{aligned}$$

which clearly is a nonzero polynomial in $\mathbb{C}[x]$ which vanishes at α/β. Besides, this resultant can also be computed in $\mathbb{Q}[x][y]$, and therefore lies in $\mathbb{Q}[x]$. As a consequence, α/β is a root of a nonzero plynomial with coefficients in $\mathbb{Q}$, which means precisely that it is an algebraic number.

Exercise 3

Let L/K be a finite extension such that $[L : K]$ is a prime number.

1. *Prove that if E is a field such that $K \subset E \subset L$, then $E = K$ or $E = L$.*

   If E is such a field, then we have $[L : E][E : K] = [L : K]$, and since this is prime, we must either have $[L : E] = 1$, in which case $E = L$, or $[E : K] = 1$, in which case $E = K$.

2. *Deduce that every $\alpha \in L \setminus K$ is a primitive element for the extension L/K.*

   Let $E = K(\alpha)$. Since $\alpha \notin K$, we have $E \supsetneq K$, and so $E = L$ by the above, which means precisely that α is a primitive element for L/K.

Exercise 4

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

   We have the extensions $\mathbb{Q} \subset K \subset L$, where $K = \mathbb{Q}(\sqrt{2})$. We have $[K : \mathbb{Q}] = 2$ because 2 is not a square in $\mathbb{Q}$, and also $[L : K] = 2$ because -5 is not a square in K, for instance because K can be embedded into $\mathbb{R}$ (it is even totally real). By multiplicativity of the degrees, we deduce that

   $$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 2 \cdot 2 = 4.$$

2. *What is the signature of L ?*

   Because of the presence of $\sqrt{-5}$, the field L cannot be embedded in $\mathbb{R}$, and so is totally complex. Since it is of degree 4, it must have two pairs of conjugate complex embeddings, and so its signature is $(0, 2)$.

3. *Let $\beta = \sqrt{2} + \sqrt{-5}$. Compute the characteristic polynomial $\chi^L_{\mathbb{Q}}(\beta)$ of β with respect to the extension $L/\mathbb{Q}$.*

We know that $(1, \sqrt{2}, \sqrt{-5}, \sqrt{2}\sqrt{-5})$ is a $\mathbb{Q}$-basis of L. On this basis, the matrix of the multiplication by β is

$$\begin{pmatrix} 0 & 2 & -5 & 0 \\ 1 & 0 & 0 & -5 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

The characteristic polynomial of β is the characteristic polynomial of this matrix, namely

$$x^4 + 6x^2 + 49$$

4. *Is this polynomial squarefree ? What does this tell us about β ?*

   This polynomial χ is squafree iff. it is coprime with its derivative $4x^3+12x$, thus iff. it is coprime with $x^3 + 3x = x(x^2 + 3)$. But it is clearly coprime with x, so we must check whether it is coprime with $x^2 + 3$. Since the latter is irreducible, either χ is a multiple of it or it is coprime with it. Euclidian division of χ by $x^2 + 3$ reveals that $x^2 + 3 \nmid \chi$, and so χ is squarefree. As a consequence, β is a *primitive element* for $L/\mathbb{Q}$.

UNASSESSED QUESTIONS

Exercise 5

1. *Let $K = \mathbb{Q}(\sqrt{-5})$, and let $\alpha = a+b\sqrt{-5}$, $a, b \in \mathbb{Q}$ be an element of K. Compute the trace, norm, and characteristic polynomial of α in terms of a and b.*

   The matrix of the multiplication by α on the $\mathbb{Q}$-basis $(1, \sqrt{5})$ of K is

   $$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix}.$$

   By reading its trace, determinant, and characteristic polynomial, we get $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha) = 2a$, $N^K_{\mathbb{Q}}(\alpha) = a^2 + 5b^2$, and $\chi^K_{\mathbb{Q}}(\alpha) = x^2 - 2ax + a^2 + 5b^2$.

2. *Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{-5})$, and let $\beta = \sqrt{2} + \sqrt{-5}$. Compute the characteristic polynomial $\chi^L_{\mathbb{Q}}(\beta)$ of β with respect to the extension L/K.*

   $(1, \sqrt{2})$ is a K-basis of L, and on this basis, the matrix of the multiplication by β is

   $$\begin{pmatrix} \sqrt{-5} & 2 \\ 1 & \sqrt{-5} \end{pmatrix}.$$

   Thus $\mathrm{Tr}^K_{\mathbb{Q}}(\alpha) = 2\sqrt{-5}$, $N^K_{\mathbb{Q}}(\alpha) = -7$, and $\chi^K_{\mathbb{Q}}(\alpha) = x^2 - 2\sqrt{-5}x - 7$.

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.