Algebraic number theory
Solutions to exercise sheet for chapter 2

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk)
Aurel Page (a.r.page@warwick.ac.uk)
TA: Pedro Lemos (lemos.pj@gmail.com)

Version: March 2, 2017

Exercise 1

Is $\frac{3+2\sqrt{6}}{\sqrt{6}-1}$ *an algebraic integer ?*

We have

$$\frac{3+2\sqrt{6}}{\sqrt{6}-1} = \frac{(3+2\sqrt{6})(\sqrt{6}+1)}{(\sqrt{6}-1)(\sqrt{6}+1)} = \frac{15+5\sqrt{6}}{5} = 3+\sqrt{6}.$$

Since 3 and $\sqrt{6}$ clearly are algebraic integers (the latter because it is a root of monic $x^2-6 \in \mathbb{Z}[x]$), so is their sum, so the answer is yes.

Exercise 2

Let $b, c, n \in \mathbb{Z}$, $n \geqslant 2$, *and let* $P(x) = x^n + bx + c$. *Prove that*

$$\operatorname{disc} P = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big).$$

Hint : start by proving that $\operatorname{disc} P = (-1)^{n(n-1)/2} n^n \prod_{k=0}^{n-2}\Big(\left(1-\frac{1}{n}\right)\beta\zeta^k b + c\Big)$, *where* $\zeta = e^{2\pi i/(n-1)}$ *and* $\beta \in \mathbb{C}$ *is such that* $\beta^{n-1} = -b/n$.

The discriminant is essentially the resultant of P and P'. This resultant can be computed in two ways : as the product of the values of P at the roots of P' (essentially), and vice versa. Here, the first way is easier, because the roots of P' are easy to express and manipulate. Explicitly, we have $P'(x) = nx^{n-1} + b$, whose complex roots are the $\zeta^k\beta$, $0 \leqslant k < n-1$, and

$$P(\zeta^k\beta) = \zeta^{kn}\beta^n + b\zeta^k\beta + c = \zeta^k\left(-\frac{\beta}{n}\right) + b\zeta^k\beta + c = \left(1-\frac{1}{n}\right)\beta\zeta^k b + c.$$

Therefore,

$$\begin{aligned}
\operatorname{Res}(P, P') &= n^n \prod_{k=0}^{n-2} P(\zeta^k \beta) \qquad \text{because the leading coefficient of } P' \text{ is } n \\
&= n^n \prod_{k=0}^{n-2} \left(\left(1 - \frac{1}{n}\right) \beta \zeta^k b + c \right) \\
&= n^n (-1)^{n-1} \prod_{k=0}^{n-2} \left(-c - \zeta^k \left(1 - \frac{1}{n}\right) \beta b \right) \\
&= n^n (-1)^{n-1} \left(\left(-c \right)^{n-1} - \left((1 - 1/n) \beta b \right)^{n-1} \right) \qquad \text{because } \prod_{k=0}^{n-2} (x - \zeta^k y) = x^{n-1} - y^{n-1} \\
&= n^n c^{n-1} - n^n \beta^{n-1} b^{n-1} (1/n - 1)^{n-1} \\
&= n^n c^{n-1} - n \left(-\frac{b}{n} \right) (1 - n)^{n-1} b^{n-1} \\
&= n^n c^{n-1} + (1 - n)^{n-1} b^n.
\end{aligned}$$

The result then follows since $\operatorname{disc} P = (-1)^{n(n-1)/2} \operatorname{Res}(P, P')$.

Exercise 3

Let $K = \mathbb{Q}(\alpha)$, where α satisfies $\alpha^3 - \alpha - 4 = 0$.

1. *Compute the discriminant of $\mathbb{Z}[\alpha]$.*

   According to the previous exercise,

   $$\operatorname{disc} \mathbb{Z}[\alpha] = \operatorname{disc}(x^3 - x - 4) = -(4(-1)^3 + 27 \cdot 4^2) = -428.$$

2. *At this point, what are the possibilities for $\operatorname{disc} K$?*

   Since $-428 = -2^2 \cdot 107$ and 107 is prime, either $\mathbb{Z}[\alpha] = \mathbb{Z}_K$ is the whole ring of integers of K, in which case $\operatorname{disc} K = -428$, or $\mathbb{Z}[\alpha]$ has index 2 and $\operatorname{disc} K = -107$.

3. *Prove that $\frac{\alpha^2+\alpha}{2}$ is an algebraic integer.*

   $1, \alpha, \alpha^2$ is a $\mathbb{Q}$-basis of K, and the matrix of the multiplication by $\frac{\alpha^2+\alpha}{2}$ on this basis is

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

   Since its characteristic polynomial $x^3 - x^2 - 3x - 2$ lies in $\mathbb{Z}[x]$, $\frac{\alpha^2+\alpha}{2}$ is an algebraic integer.

4. *What is the ring of integers of K ?*

We now have the new order $\mathbb{Z}[\alpha, \frac{\alpha^2+\alpha}{2}] \subseteq \mathbb{Z}_K$. It admits $1, \alpha, \frac{\alpha^2+\alpha}{2}$ as a $\mathbb{Z}$-basis, so it contains $\mathbb{Z}[\alpha]$ with index 2, and so its discriminant is 2^2 times smaller, i.e. is -107. Since this is squarefree, we can conclude that

$$\mathbb{Z}_K = \mathbb{Z}\left[\alpha, \frac{\alpha^2+\alpha}{2}\right].$$

In particular, $\operatorname{disc} K = -107$.

Remark: Actually, if $\beta = \frac{\alpha^2+\alpha}{2}$, it can be checked that $\alpha = \beta^2 - \beta - 2 \in \mathbb{Z}[\beta]$; as a result, $\mathbb{Z}_K = \mathbb{Z}[\beta]$, and in particular, the discriminant of the characteristic polynomial of β must be -107. But of course, you did not need to say that to get full marks.