Dijana Kreso (kreso@math.tugraz.at)

Exercises in Number Theory MAT.413

Due: January 11, 2016

Graz University of Technology

---

1. (2 points) Let α be an algebraic number. Show that $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

2. Let K be a number field of degree 2.
   (a) (1 point) Show that there exists squarefree integer $d \neq 0, 1$ such that $K = \mathbb{Q}[\sqrt{d}]$.
   (b) (2 points) Show that for the ring of integers $\mathscr{O}_K$ of K the following holds:
   $$\mathscr{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2,3 \pmod 4, \\ \mathbb{Z}[(1+\sqrt{d})/2], & d \equiv 1 \pmod 4. \end{cases}$$
   (c) (1 point) Deduce that $\mathscr{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}] = 2$.
   (d) (1 point) Let τ_1 and τ_2 be two distinct elements in $\mathrm{Hom}_{\mathbb{Q}}(K)$ with $K = \mathbb{Q}[\sqrt{d}]$ so that $\tau_{1,2}(\sqrt{d}) = \pm\sqrt{d}$. Show that if $\alpha \in \mathscr{O}_K$, then $\tau_{1,2}(\alpha) \in \mathscr{O}_K$ and $\tau_1(\alpha)\cdot\tau_2(\alpha) \in \mathbb{Z}$.
   (e) (1 point) A basic result from algebra states that if $d \in \mathbb{N}$ and I, J are $\mathbb{Z}$-modules such that
   - $dI \subset J \subset I$,
   - I is free and of rank $t > 0$,

   then J is free and of rank t. Use this to prove that any nonzero ideal in $\mathscr{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}] = 2$.
   (f) (2 points) Let $\tau : K \to \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^2$ be the Minkowski embedding. Show that if $(0) \neq \mathscr{U}$ is an ideal in $\mathscr{O}_K$, then $\tau\mathscr{U}$ is a lattice in $\mathbb{R}^2$.

3. Let K be a number field and $\mathscr{O}_K$ the ring of integers of K.
   (a) (1 point) Show that if $\alpha \in K$, then there exists $m \in \mathbb{N}$ such that $m\alpha \in \mathscr{O}_K$.
   (b) (1 point) Conclude that the field of fractions of $\mathscr{O}_K$ is K.

   Recall that the field of fractions K of an integral domain R is the smallest field containing R.

4. (2 points) An integral domain R with field of fractions F is called integrally closed if whenever $\alpha \in F$ is integral over R, then $\alpha \in R$. Show that the ring of integers $\mathscr{O}_K$ of K is integrally closed.

5. (a) (1 point) Show that the equation $y^2 = x^3 + 7$ has no solutions in integers x, y.
   (b) (2 points) Show that the equation $x^4 + y^4 = z^2$ has no solutions in integers x, y, z with $xyz \neq 0$.