Lisbon Summer School (2011) Problem Set 3
Keith Conrad

1. For $\alpha = r + s\sqrt{d} \in \mathbf{Q}[\sqrt{d}]$, where $r$ and $s$ are rational, set $\overline{\alpha} = r - s\sqrt{d}$ and $\mathrm{N}(\alpha) = r^2 - ds^2$, so $\mathrm{N}(\alpha) \in \mathbf{Z}$ when $\alpha$ is an integer of $\mathbf{Q}[\sqrt{d}]$.

   a) For squarefree $d \equiv 1 \bmod 4$, let $A_d = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$, which is the ring of integers of $\mathbf{Q}[\sqrt{d}]$. Show an element $\alpha$ of $A_d$ is in $A_d^\times$ if and only if $\mathrm{N}(\alpha) = \pm 1$.

   b) Check $\frac{1+\sqrt{5}}{2}$ is a unit in $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$ and $(\frac{1+\sqrt{5}}{2})^3 = 2 + \sqrt{5}$, which is a unit in $\mathbf{Z}[\sqrt{5}]$.

   c) Check $\frac{3+\sqrt{13}}{2}$ is a unit in $\mathbf{Z}\left[\frac{1+\sqrt{13}}{2}\right]$ and find the smallest positive power of this unit which belongs to $\mathbf{Z}[\sqrt{13}]$.

   d) For a quadratic field $K = \mathbf{Q}[\sqrt{d}]$ with $d < 0$, show $\mathcal{O}_K^\times = \{\pm 1\}$ except for $K = \mathbf{Q}[i]$ (where $\mathcal{O}_K^\times$ contains 4th roots of unity) and $K = \mathbf{Q}[\sqrt{-3}]$ (where $\mathcal{O}_K^\times$ contains 6th roots of unity).

2. a) In $\mathbf{Z}[\sqrt{-14}]$, verify the following equality of ideals:

$$(2, 1 + \sqrt{-14}) = (1), \quad (2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14}),$$

   and

$$(4 + \sqrt{-14}, 2 - \sqrt{-14}, 7 - 2\sqrt{-14}, 7 + \sqrt{-14}) = (3, 1 + \sqrt{-14}).$$

   b) Show $(5 + \sqrt{-14}, 2 + \sqrt{-14})(4 + \sqrt{-14}, 2 - \sqrt{-14}) = 3(2, \sqrt{-14})$.

   c) Show $(2, \sqrt{-14})$ is a prime ideal of norm 2.

   d) Show $(3, 1 + \sqrt{-14})$ and $(3, 1 - \sqrt{-14})$ are prime ideals of norm 3.

3. In $\mathbf{Z}[\sqrt{15}]$, show $1 + \sqrt{15}$ is irreducible and $(1 + \sqrt{15}) = (2, 1 + \sqrt{15})(7, 1 + \sqrt{15})$, where the ideals on the right side are prime with norms 2 and 7 and are not principal. (Could elements have norms $\pm 2$ or $\pm 7$?)

4. In $\mathbf{Z}[\sqrt{-5}]$, let $\mathfrak{p} = (2, 1 + \sqrt{-5})$ and $\mathfrak{q} = (3, 1 + \sqrt{-5})$, so $\overline{\mathfrak{q}} = (3, 1 - \sqrt{-5})$.

   a) Show $\mathfrak{p}$ is a prime ideal of norm 2, $\overline{\mathfrak{p}} = \mathfrak{p}$, and $\mathfrak{p}$ is non-principal.

   b) Show $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ are prime ideals of norm 3 and are non-principal.

   c) Show $(1 + \sqrt{-5}) = \mathfrak{p}\mathfrak{q}$ and $(1 - \sqrt{-5}) = \mathfrak{p}\overline{\mathfrak{q}}$.

   d) In $\mathbf{Z}[\sqrt{-5}]$ we have the nonunique irreducible factorization $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ from Set 2. This equation of numbers implies the equation of ideals $(2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Use parts a, b, and c to explain how this equality of multiplication of principal ideals is consistent with unique prime ideal factorization in $\mathbf{Z}[\sqrt{-5}]$.

5. Let $K$ be a quadratic field. For all nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, show $\overline{\mathfrak{a}\mathfrak{b}} = \overline{\mathfrak{a}}\overline{\mathfrak{b}}$. Then explain from this formula why $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$.