Yale University Department of Mathematics
Math 373/573 Algebraic Number Theory
Spring 2019

Problem Set # 1 (due in class on Thursday 31 January)

Notation: As usual, write $\omega = (1+\sqrt{3}i)/2$ for our favorite choice of primitive 3rd root of unity. For a quadratic extension $K/\mathbb{Q}$, recall that the field norm $N : K \to \mathbb{Q}$ is the map $\alpha \mapsto \alpha\,\overline{\alpha}$, where $\overline{\alpha}$ is the result of applying the unique $\mathbb{Q}$-automorphism of K to α.

Problems:

1. *Quadratic fields.* Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}(\sqrt{d})$.

(a) For $\alpha = a + b\sqrt{d} \in K$, determine the minimal polynomial of α over $\mathbb{Q}$.

(b) Prove that the ring of integers $\mathcal{O}_K$ is either $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod 4$ or $\mathbb{Z}[(1+\sqrt{d})/2)] = \{(A + B\sqrt{d})/2 \mid A \equiv B \pmod 2\}$ if $d \equiv 1 \pmod 4$.

(c) Let $\delta = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ or $\delta = (1 + \sqrt{d})/2$ if $d \equiv 1 \pmod 4$ and let D be the discriminant of the minimal polynomial of δ. Prove that $D = 4d$ if $d \equiv 2, 3 \pmod 4$ and $D = d$ if $d \equiv 1 \pmod 4$. In fact, D is the **discriminant** of $\mathcal{O}_K$, as we'll learn later.

2. *Euclidean domains.*

(a) Let R be an integral domain with fraction field K and $N : K \to \mathbb{N}$ be a multiplicative function (i.e., $N(xy) = N(x)N(y)$ for all $x, y \in K$) satisfying $N(0) = 0$. Prove that R is a Euclidean domain with respect to (the restriction to R of) N if and only if for every $x \in K$ there exists $y \in R$ such that $N(x - y) < 1$.

(b) Use this to prove the result of Gauss that $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are Euclidean domains with respect to the field norm. Make a geometrical argument with a picture!

(c) Assume that $d < 0$ and let $K = \mathbb{Q}(\sqrt{d})$. Prove that $\mathcal{O}_K$ is a Euclidean domain with respect to the field norm if and only if $d = -11, -7, -3, -2, -1$. Hint: Just as above, look at the picture of the lattice $\mathcal{O}_K \subset \mathbb{C}$; how close are the lattice points?

3. We say that two prime elements are **associates** if they differ up to multiplication by a unit. Find all prime elements in $\mathbb{Z}[\omega]$ up to associates. Hint: Show, using the field norm, that it suffices to factor the rational prime numbers in $\mathbb{Z}[\omega]$.

4. *Units in quadratic fields.* Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}(\sqrt{d})$. We say that K is **real** or **imaginary** if $d > 0$ or $d < 0$, respectively. Write $U_K = \mathcal{O}_K^\times$.

(a) Let $\alpha \in \mathcal{O}_K$ and write $\alpha = x + y\sqrt{d}$ with $x, y \in \frac{1}{2}\mathbb{Z}$, noting that the $\frac{1}{2}$ is required only when $d \equiv 1 \pmod 4$. Prove that $\alpha \in U_K$ if and only if $N(\alpha) = \pm 1$ if and only if $x^2 - dy^2 = \pm 1$.

(b) Assume that K is imaginary. Prove that $U_K = \{\pm 1\}$ unless $d = -1$ or $d = -3$, in which case $U_K = \{\pm 1, \pm i\}$ or $U_K = \{\pm 1, \pm\omega, \pm\omega^2\}$, respectively. In particular, all units in imaginary quadratic fields are roots of unity.

(c) Assume that K is real. Prove that if there exists $u \in U_K$ with $u \neq \pm 1$, then there exists $u \in U_K$ with $u > 1$. In this case, prove that U_K is infinite.

(d) For $d = 2, 3, 5$ find $u \in U_K$ with $u > 1$.

Yale University, Department of Mathematics, 10 Hillhouse Ave, New Haven, CT 06511
E-mail address: asher.auel@yale.edu