Algebraic Number Theory, Fall 2018
Homework 1

Joshua Ruiter

October 16, 2019

Proposition 0.1. *Let $K/\mathbb{Q}$ be a number field, and let $N_{\mathbb{Q}}^{K} : K^\times \to \mathbb{Q}^\times$ be the norm map. Then*

1. *$N_{\mathbb{Q}}^{K}$ maps $\mathcal{O}_K^\times$ to $\{\pm 1\}$.*
2. *Conversely, if $a \in \mathcal{O}_K$ satisfies $N_{\mathbb{Q}}^{K}(a) = \pm 1$, then $a \in \mathcal{O}_K^\times$.*

Proof. Let $a \in \mathcal{O}_K^\times$, with inverse $a^{-1} \in \mathcal{O}_K^\times$. Then

$$1 = N_{\mathbb{Q}}^{K}(1) = N_{\mathbb{Q}}^{K}(aa^{-1}) = N_{\mathbb{Q}}^{K}(a) N_{\mathbb{Q}}^{K}(a^{-1})$$

Since we know that $N_{\mathbb{Q}}^{K}$ maps $\mathcal{O}_K$ to $\mathbb{Z}$ (Corollary 2.21 of Milne [1]), this says that $N_{\mathbb{Q}}^{K}(a)$ is a unit in $\mathbb{Z}$, hence $N_{\mathbb{Q}}^{K}(a) = \pm 1$. For the converse, we know that a^{-1} exists in $K^\times$, we just need to show $a^{-1} \in \mathcal{O}_K^\times$. Suppose $N_{\mathbb{Q}}^{K}(a) = \pm 1$, so the minimal polynomial of a in $\mathbb{Z}[x]$ is

$$a^n + b_{n-1}a^{n-1} + \ldots + b_1 a + (\pm 1) = 0$$

We multiply this equation by a^{-n}, and obtain

$$1 + b_{n-1}a^{-1} + \ldots + b_1 \left(a^{-1}\right)^{n-1} + (\pm 1)\, a^{-n} = 0$$

Up to sign, this is a monic polynomial in $\mathbb{Z}[x]$, so $a^{-1} \in \mathcal{O}_K^\times$. $\square$

For the next proposition, recall that the ring of integers of a quadratic extension $K = \mathbb{Q}\left(\sqrt{-D}\right)$ is $\mathbb{Z}[\sqrt{-D}]$ if $-D \equiv 2, 3 \bmod 4$, and $\mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right]$ if $-D \equiv 1 \bmod 4$.

Proposition 0.2. *Let $K = \mathbb{Q}(\sqrt{-D})$ where $D \geq 1$ is a square free integer. Then*

1. *$\mathcal{O}_K^\times = \{\pm 1\}$ if $D \neq 1, D \neq 3$.*
2. *$\mathcal{O}_K^\times = \{\pm 1, \pm i\}$ if $D = 1$.*
3. *$\mathcal{O}_K^\times = \left(\pm 1, \pm\frac{1+\sqrt{-3}}{2}, 1 - \frac{1+\sqrt{-3}}{2}, -1 + \frac{1+\sqrt{-3}}{2}\right)$ if $D = 3$.*

Proof. When $-D \equiv 2, 3 \bmod 4$, the norm map is given by

$$N_{\mathbb{Q}}^{K}\left(a + b\sqrt{-D}\right) = \left(a + b\sqrt{-D}\right)\left(a - b\sqrt{-D}\right) = a^2 + Db^2$$

When $-D \equiv 1 \bmod 4$, the norm map is given by

$$N_{\mathbb{Q}}^{K}\left(a + b\frac{1+\sqrt{-D}}{2}\right) = \left(a + b\frac{1+\sqrt{-D}}{2}\right)\left(a + b\frac{1-\sqrt{-D}}{2}\right) = a^2 + ab + b^2\left(\frac{1+D}{4}\right)$$

By Proposition 0.1, $a \in \mathcal{O}_K$ is a unit if and only if $N_{\mathbb{Q}}^{K}(a) = \pm 1$.

First, we consider the case $D = 1$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The norm of $a + bi \in \mathbb{Z}[i]$ is $a^2 + b^2$, which is ± 1 only if one of a, b is zero and the other is ± 1 (since $a, b \in \mathbb{Z}$). Thus units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

Now consider $D = 3$, so $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, and the norm of $a + b\left(\frac{1+\sqrt{-3}}{2}\right)$ is $a^2 + ab + b^2$, so we analyze integral solutions to this. If one of a, b is zero, the other must be ± 1, and one checks that $(\pm 1, 0), (0, \pm 1)$ are solutions. If one of a, b is ± 1, say $a = \pm 1$, then b satisfies one of the four equations

$$b(b \pm 1) = -1 \pm 1$$

Two of these have no solutions, and the other two give the solutions $(1, -1), (-1, 1)$. The six solutions mentioned give rise to the listed units. We claim there are no other solutions.

Suppose (a, b) is a solution not already listed, with $|a|, |b| \geq 2$. Note that a, b must have opposite signs. Taking absolute values, we obtain

$$1 = |\pm 1| = |a^2 + ab + b^2| \geq |a^2| + |b^2| - |ab|$$

Without loss of generality, suppose $|a| \leq |b|$. Note that $a \neq 0$ implies $|a| \geq 2$, so

$$|ab| \leq |b^2| \implies |b^2| - |ab| \geq 0 \implies |a^2| + |b^2| - |ab| \geq 2$$

Combining our two strings of inequalities, we obtain $1 \geq 2$, which is false, so no such solution exists.

Now we consider more generally $D \neq 1, 3$. If $-D \equiv 2, 3 \bmod 4$, units are $a + b\sqrt{-D}$ so that $a^2 + Db^2 = 1$. Since $D > 1$, we must have $b = 0$, and then the only solutions are $a = \pm 1$. If $-D \equiv 1 \bmod 4$, units are $a + b\left(\frac{1+\sqrt{-D}}{2}\right)$ satisfying $a^2 + ab + b^2\left(\frac{1+D}{4}\right) = \pm 1$. Since $D \neq 3$, $\left|\frac{1+D}{4}\right| > 1$, so the same chain of absolute values as in the case $D = 3$ prohibits any units with $|a|, |b| \geq 2$. Then one may tediously check the possibilities with $a, b \in \{0, \pm 1\}$ to conclude that only $a = \pm 1, b = 0$ are solutions. $\square$

Exercise 3. For each of the following irreducible polynomials, we let α be a root and $K = \mathbb{Q}(\alpha)$. Then we compute $\mathcal{O}_K, \operatorname{disc}(K/\mathbb{Q})$, and factorizations of $2, 3, 5, 7$ in $\mathcal{O}_K$.

(a) $f(x) = x^2 + 31$

(b) $f(x) = x^2 + 39$

(c) $f(x) = x^2 - 29$

(d) $f(x) = x^3 + x - 1$

Solution. (a) In this case, $\alpha = \sqrt{-31}$ and $K = \mathbb{Q}(\sqrt{-31})$. Since $-31 \equiv 1 \bmod 4$, the ring of integers is $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-31}}{2}\right]$. Let $\beta = \frac{1+\sqrt{-31}}{2}$. We compute the discriminant using the basis $1, \beta$. Note that $\beta^2 = \frac{1}{2}(\alpha - 15)$, so

$$\operatorname{Tr}\beta = \frac{1}{2}\operatorname{Tr}\alpha - \frac{1}{2}\operatorname{Tr}15 = 0 - 15 = -15$$

$$D(1,\beta) = \det\begin{pmatrix}\operatorname{Tr}1 & \operatorname{Tr}\beta \\ \operatorname{Tr}\beta & \operatorname{Tr}\beta^2\end{pmatrix} = \det\begin{pmatrix}2 & 1 \\ 1 & -15\end{pmatrix} = -31$$

To factor $2, 3, 5, 7$ in $\mathcal{O}_K$, we use Kummer's theorem which says that a factorization of the minimal polynomial of β mod p gives a factorization of p in $\mathcal{O}_K$. The minimal polynomial of β is $x^2 - x + 8$.

$$\begin{aligned}
&x^2 - x + 8 \equiv x^2 + x = x(x+1) \bmod 2 \\
&x^2 - x + 8 \equiv x^2 - x + 2 \text{ is irreducible mod } 3 \\
&x^2 - x + 8 \equiv (x-2)(x-4) \bmod 5 \\
&x^2 - x + 8(x-3)(x-5) \bmod 7
\end{aligned}$$

Thus

$$\begin{aligned}
&(2)\mathcal{O}_K = (2,\beta)\,(2,\beta+1) \\
&(3)\mathcal{O}_K \text{ is prime} \\
&(5)\mathcal{O}_K = (5,\beta-2)(5,\beta-4) \\
&(7)\mathcal{O}_K = (7,\beta-3)(7,\beta-5)
\end{aligned}$$

(b) In this case $\alpha = \sqrt{-39}$. Since $-39 \equiv 1 \bmod 4$, the ring of integers is $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-39}}{2}\right]$. Let $\beta = \frac{1+\sqrt{-39}}{2}$. Note that $\beta^2 = \frac{1}{2}(\alpha - 19)$.Using the basis $1, \beta$, the discriminant is

$$\operatorname{Tr}\beta^2 = \frac{1}{2}\operatorname{Tr}\alpha - \frac{1}{2}\operatorname{Tr}(19) = -19$$

$$D(1,\beta) = \det\begin{pmatrix}\operatorname{Tr}1 & \operatorname{Tr}\beta \\ \operatorname{Tr}\beta & \operatorname{Tr}\beta^2\end{pmatrix} = \det\begin{pmatrix}2 & 1 \\ 1 & -19\end{pmatrix} = -39$$

To factor $2, 3, 5, 7$ in $\mathcal{O}_K$, we factor the minimal polynomial of β modulo the prime in question. The minimal polynomial of β is $x^2 - x + 10$.

$$\begin{aligned}
&x^2 - x + 10 \equiv x(x+1) \bmod 2 \\
&x^2 - x + 10 \equiv (x-2)^2 \bmod 3 \\
&x^2 - x + 10 \equiv x(x-1) \bmod 5 \\
&x^2 - x + 10 \text{ is irreducible mod } 7
\end{aligned}$$

Thus

$$
\begin{aligned}
2\mathcal{O}_K &= (2,\beta)(2\beta+1)\\
3\mathcal{O}_K &= (3,\beta-2)^2\\
5\mathcal{O}_K &= (5,\beta)(5,\beta-1)\\
7\mathcal{O}_K & \text{ is prime}
\end{aligned}
$$

(c) In this case $\alpha = \sqrt{29}$ and $K = \mathbb{Q}(\sqrt{29})$. Since $29 \equiv 2 \bmod 3$, the ring of integers is $\mathbb{Z}[\sqrt{29}]$. Using the basis $1, \alpha$, the discriminant is

$$D(1,\alpha) = \det\begin{pmatrix}\operatorname{Tr} 1 & \operatorname{Tr}\alpha\\ \operatorname{Tr}\alpha & \operatorname{Tr}\alpha^2\end{pmatrix} = \det\begin{pmatrix}2 & 0\\ 0 & 2(29)\end{pmatrix} = 4(29)$$

We factor x^2+29 modulo the primes $2,3,5,7$ to calculate their factorizations in $\mathcal{O}_K$.

$$
\begin{aligned}
&x^2+29 \equiv (x+1)^2 \bmod 2\\
&x^2+29 \equiv (x+1)(x+2) \bmod 3\\
&x^2+29 \equiv (x-1)(x-4) \bmod 5\\
&x^2+29 \text{ is irreducible mod } 7
\end{aligned}
$$

Thus

$$
\begin{aligned}
2\mathcal{O}_K &= (2,\alpha+1)^2\\
3\mathcal{O}_K &= (3,\alpha+1)(3,\alpha+2)\\
5\mathcal{O}_K &= (5,\alpha-1)(5,\alpha-4)\\
7\mathcal{O}_K & \text{ is prime}
\end{aligned}
$$

(d) Let $f(x) = x^3+x-1$ and let α be a root of f, and let $K = \mathbb{Q}(\alpha)$. Let $N = \mathbb{Z}[\alpha] \subset \mathcal{O}_K$. In class we showed that

$$D(1,\alpha,\alpha^2) = [\mathcal{O}_K : N]^2 \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$$

so if $D(1,\alpha,\alpha^2)$ is square-free, we can conclude that $\mathcal{O}_K = N$. Denote $\operatorname{Tr}_{\mathbb{Q}}^K$ by Tr. Since f is the minimal polynomial of α, we can read off $\operatorname{Tr}\alpha = 0$. Using a CAS, the minimal polynomial of α^2 is x^3+2x^2+x-1, so $\operatorname{Tr}\alpha^2 = -2$. Since $\alpha^3 = 1-\alpha$, we have

$$\operatorname{Tr}(1-\alpha) = \operatorname{Tr}1 - \operatorname{Tr}\alpha = 3 \qquad \operatorname{Tr}\alpha^4 = \operatorname{Tr}(\alpha-\alpha^2) = \operatorname{Tr}\alpha - \operatorname{Tr}\alpha^2 = 2$$

$$D(1,\alpha,\alpha^2) = \det\begin{pmatrix}\operatorname{Tr}1 & \operatorname{Tr}\alpha & \operatorname{Tr}\alpha^2\\ \operatorname{Tr}\alpha & \operatorname{Tr}\alpha^2 & \operatorname{Tr}\alpha^3\\ \operatorname{Tr}\alpha^2 & \operatorname{Tr}\alpha^3 & \operatorname{Tr}\alpha^4\end{pmatrix} = \det\begin{pmatrix}3 & 0 & -2\\ 0 & -2 & 3\\ -2 & 3 & 2\end{pmatrix} = -31$$

Since -31 is a square-free integer, we conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. By the calculation we just did, $\operatorname{disc}(K/\mathbb{Q}) = -31$, since $1,\alpha,\alpha^2$ is a basis for $\mathcal{O}_K$ over $\mathbb{Z}$. To factor $2,3,5,7$ in $\mathbb{Z}[\alpha]$, we use Kummer's theorem.

$$
\begin{aligned}
&x^3+x-1 \text{ is irreducible mod } 2\\
&x^3+x-1 \equiv (x-2)(x^2+2x+2) \bmod 3\\
&x^3+x-1 \text{ is irreducible mod } 5\\
&x^3+x-1 \text{ is irreducible mod } 7
\end{aligned}
$$

and note that $x^2 + 2x + 2$ is irreducible mod 3. Thus $2\mathcal{O}_K, 5\mathcal{O}_K, 7\mathcal{O}_K$ are prime, and

$$3\mathcal{O}_K = (3, \alpha - 2)(3, \alpha^2 + 2\alpha + 2)$$

Remark 0.1. We clarify the statement of the next proposition. Let K be a number field with ring of integers $\mathcal{O}_K$, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a (nonzero, proper) prime ideal. Since $\mathcal{O}_K$ is a Dedekind domain, $\mathfrak{p}$ is maximal, so $\mathcal{O}_K/\mathfrak{p}$ is a field. We also know that $\mathcal{O}_K/\mathfrak{p}$ is finite.

Proposition 0.3 (Exercise 4)**.** *Let K be a number field, with ring of integers $\mathcal{O}_K$, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal, and let $p = \operatorname{char} \mathcal{O}_K/\mathfrak{p}$. Then there exists $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} = (p, \alpha)$.*

Proof. The fact that $\mathcal{O}_K/\mathfrak{p}$ has characteristic p says that $p \equiv 0 \bmod \mathfrak{p}$, which is to say, $p \in \mathfrak{p}$. Since $\mathcal{O}_K$ is a Dedekind domain, by Corollary 3.16 of Milne [1], there exists $\alpha \in \mathfrak{p}$ so that $\mathfrak{p} = (p, \alpha)$. □

Proposition 0.4 (Exercise 5)**.** *Let p, q be distinct primes in $\mathbb{Z}$, and let n be the order of q in $\mathbb{F}_p^\times$. Let ζ_p be a primitive pth root of unity, and $K = \mathbb{Q}(\zeta_p)$. Then*

(a) q is unramified in K.

(b) If q factors as

$$q\mathcal{O}_K = \mathfrak{P}_1 \dots \mathfrak{P}_r$$

then $r = \frac{p-1}{n}$.

Proof. (a) We computed in class that the discriminant of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is $\pm p^{p-2}$, and we know that the only primes that ramify are ones dividing the discriminant. Thus p is the only prime that ramifies, and since $q \neq p$, q is unramified.

(b) (Incomplete proof) By part (a), we know that $q\mathcal{O}_K$ factors as $\mathfrak{P}_1 \dots \mathfrak{P}_r$ with $\mathfrak{P}_i$ distinct primes of $\mathcal{O}_K$. We computed in class that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Since $K/\mathbb{Q}$ is Galois and $[K : \mathbb{Q}] = p - 1$, by the fundamental relation, we have $efr = fr = p - 1$, where $f = \dim_{\mathbb{F}_q} \mathbb{Z}[\zeta_p]/\mathfrak{P}_1$. To finish the proof, it suffices to show that $f = n$.

Since $\mathcal{O}_K$ is a Dedekind domain, $\mathfrak{P}_1$ is maximal, so $\mathbb{Z}[\zeta_p]/\mathfrak{P}_1$ is a field, and by the classification of finite fields, it must be $\mathbb{F}_{q^f}$. Since $\mathbb{Z}[\zeta_p]$ is generated over $\mathbb{Z}$ by ζ_p, $\mathbb{Z}[\zeta_p]/\mathfrak{P}_1$ is generated over $\mathbb{F}_q$ by ζ_p, so $\mathbb{Z}[\zeta_p]/\mathfrak{P}_1 \cong \mathbb{F}_q(\zeta_p) \cong \mathbb{F}_{q^f}$. I don't know how to finish the proof from here.

Another approach: The minimal polynomial of ζ_p over $\mathbb{Z}$ is $\phi_p(x) = 1 + x + \ldots + x^{p-1}$. By a theorem of Kummer from class, the factorization of $q\mathbb{Z}[\zeta_p]$ is determined by the factorization of ϕ_p modulo q, so it suffices to factor $1 + x + \ldots + x^{p-1}$ modulo q. If what we want is true, then ϕ_p should split into $\frac{p-1}{n}$ irreducible factors. I don't know how to finish the proof from here. □

Proposition 0.5 (Exercise 6)**.** *Let $K \subset L \subset M$ be a tower of number fields, with respective rings of integers $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_M$. Let $\mathfrak{p}_K \subset_K$ be a prime ideal, and let $\mathfrak{p}_L \subset \mathcal{O}_L, \mathfrak{p}_M \subset \mathcal{O}_M$ be prime ideals such that*

$$\mathfrak{p}_L \cap \mathcal{O}_K = \mathfrak{p}_K \qquad \mathfrak{p}_M \cap \mathcal{O}_K = \mathfrak{p}_K$$

Then

$$e(\mathfrak{p}_M/\mathfrak{p}_K) = e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K) \qquad f(\mathfrak{p}_M/\mathfrak{p}_K) = f(\mathfrak{p}_M/\mathfrak{p}_L)f(\mathfrak{p}_L/\mathfrak{p}_K)$$

Proof. Recall that $\mathfrak{p}_L \cap \mathcal{O}_K \mathfrak{p}_K$ is equivalent to saying that $\mathfrak{p}_L$ appears in the (unique) factorization of $\mathfrak{p}_K\mathcal{O}_L$, and that $e(\mathfrak{p}_L/\mathfrak{p}_K)$ is, by definition, the power of $\mathfrak{p}_L$ in that factorization. We use $(\cdots)$ to denote the irrelevant part of the factorization.

$$\begin{aligned}
\mathfrak{p}_K\mathcal{O}_L &= \mathfrak{p}_L^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots) \\
\mathfrak{p}_K\mathcal{O}_M &= \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_K)}(\cdots) \\
\mathfrak{p}_L\mathcal{O}_M &= \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_L)}(\cdots)
\end{aligned}$$

Putting these together, we obtain

$$\begin{aligned}
\mathfrak{p}_K\mathcal{O}_M &= (\mathfrak{p}_K\mathcal{O}_L)\mathcal{O}_M \\
&= \left(\mathfrak{p}_L^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots)\right)\mathcal{O}_M \\
&= (\mathfrak{p}_L\mathcal{O}_M)^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots) \\
&= \left(\mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_L)}(\cdots)\right)^{e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots) \\
&= \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K)}(\cdots)
\end{aligned}$$

Note that in each step, the unwritten parts of the factorization $(\cdots)$ do not include any factors of $\mathfrak{p}_M$. Comparing this with the factorization $\mathfrak{p}_K\mathcal{O}_M = \mathfrak{p}_M^{e(\mathfrak{p}_M/\mathfrak{p}_K)}(\cdots)$, by uniqueness we conclude that the powers of $\mathfrak{p}_M$ are equal, that is,

$$e(\mathfrak{p}_M/\mathfrak{p}_K) = e(\mathfrak{p}_M/\mathfrak{p}_L)e(\mathfrak{p}_L/\mathfrak{p}_K)$$

The statement for f is simpler to prove. Since $\mathfrak{p}_K \subset \mathfrak{p}_L \subset \mathfrak{p}_M$, we have a tower of fields $\mathcal{O}_K/\mathfrak{p}_K \subset \mathcal{O}_L/\mathfrak{p}_L \subset \mathcal{O}_M/\mathfrak{p}_M$, and then from multiplicativity of field degrees in towers, we get

$$\begin{aligned}
f(\mathfrak{p}_M/\mathfrak{p}_K) &= [\mathcal{O}_M/\mathfrak{p}_M : \mathcal{O}_K/\mathfrak{p}_K] \\
&= [\mathcal{O}_M/\mathfrak{p}_M : \mathcal{O}_L/\mathfrak{p}_L][\mathcal{O}_L/\mathfrak{p}_L : \mathcal{O}_K/\mathfrak{p}_K] \\
&= f(\mathfrak{p}_M/\mathfrak{p}_L)f(\mathfrak{p}_L/\mathfrak{p}_K)
\end{aligned}$$

□

Proposition 0.6 (Exercise 7)**.** *Let* $K = \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{11})$*. Then*

$$7\mathcal{O}_K = \mathfrak{P}_1^2\mathfrak{P}_2^2$$

for some prime ideals $\mathfrak{P}_1, \mathfrak{P}_2 \subset \mathcal{O}_K$*.*

Proof. First, note that $K/\mathbb{Q}$ is the splitting field of $(x^2-5)(x^2-7)(x^2-11)$, so it is Galois. By Galois theory, $[K : \mathbb{Q}] = 8$ [1]. We can write $7\mathcal{O}_K = \mathfrak{P}_1^e \ldots \mathfrak{P}_r^e$, and the fundamental relation gives $efr = 8$. Now we just need to show $e = f = r = 2$. As a first step, consider

[1] In fact, $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$. For a general computation, see Proposition 0.18 of `http://users.math.msu.edu/users/ruiterj2/Math/Documents/Spring%202017/Algebra/Homework_4.pdf`

the tower $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{7}) \subset K$. From our study of quadratic extensions, we know that 7 ramifies, that is,

$$7\mathcal{O}_L = \mathfrak{P}^2$$

so $e(7\mathcal{O}_L/7\mathbb{Z}) = 2$, with $f = r = 1$ here. By Exercise 6 (multiplicativity in towers), this tower gives a lower bound $e(7\mathcal{O}_K/7\mathbb{Z}) \geq 2$. Now consider the tower

$$\mathbb{Q} \subset M = \mathbb{Q}(\sqrt{5}, \sqrt{11}) = \mathbb{Q}(\sqrt{5} + \sqrt{11}) \subset K$$

Using a computer algebra system, the minimal polynomial of $\mathbb{Q}(\sqrt{5}+\sqrt{11})$ is $x^4 - 32x^2 + 36$, which factors into two irreducible quadratics modulo 7.

$$x^4 - 32x^2 + 36 \equiv (x^2 + 3x + 6)(x^2 + 4x + 6) \bmod 7$$

Thus by a theorem of Kummer, $7\mathcal{O}_M = \mathfrak{P}_1\mathfrak{P}_2$, so

$$e(7\mathcal{O}_M/7\mathbb{Z}) = 1 \qquad r(7\mathcal{O}_M/7\mathbb{Z}) = 2 \qquad f(7\mathcal{O}_M/7\mathbb{Z}) = 2$$

By mutliplicativity in towers, we get lower bounds $f(7\mathcal{O}_K/7\mathbb{Z}) \geq 2$ and $r(7\mathcal{O}_K/7\mathbb{Z}) \geq 2$. Now we have $e, f, r \geq 2$, and $efr = 8$, so the only possibility is $e = f = r = 2$. □

Proposition 0.7 (Exercise 8)**.** *Let A be an integral domain, and $K = \mathrm{Frac}(A)$, and L/K a finite extension. Let B be the integral closure of A in L, and $S \subset A$ a multiplicative subset. Then $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.*

Proof. First we show that every element of $S^{-1}B$ is integral over $S^{-1}A$. Let $x = \frac{b}{s} \in S^{-1}B$. Since B is integral over A, b satisfies a monic polynomial in $A[x]$, so we have a relation in B of the form

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$$

Since B is an integral domain, the canonical map $B \to S^{-1}B$ is injective, so may view this as a relation in $S^{-1}B$. Then we multiply by s^{-n} to obtain

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_0}{s^n} = 0$$

which says that $\frac{b}{s}$ satisfies a monic polynomial in $S^{-1}A$, hence $\frac{b}{s}$ is integral over $S^{-1}A$. To finish the proof, we need to show that every integral element of L over $S^{-1}A$ lies in $S^{-1}B$. Let $\alpha \in L$ be integral over $S^{-1}A$, so there is a relation in $S^{-1}A$ of the form

$$\alpha^n + \left(\frac{a_{n-1}}{s_{n-1}}\right)\alpha^{n-1} + \ldots + \frac{a_0}{s_0} = 0$$

with $a_i \in A, s_i \in S$. Clearing denominators, there exists $s \in S$ so that αs is integral over A, so $s\alpha \in B$, so $\alpha \in S^{-1}B$. □

Proposition 0.8. *Let $v : K^\times \to \mathbb{Z}$ be a discrete valuation.*

1. *If $x \in K^\times$ is an element of finite order, then $v(x) = 0$. In particular, $v(a) = v(-a)$.*

2. If $a, b \in K^\times$ and $v(a) > v(b)$, then $v(a+b) = v(b)$.

3. Suppose there are $a_1, \dots, a_n \in K^\times$ with

$$a_1 + \ldots + a_n = 0$$

Then the minimal value of $v(a_i)$ is attained for at least two indices i.

Proof. (1) If $x^n = 1$, then $0 = v(1) = v(x^n) = nv(x)$ so $v(x) = 0$. Consequently,

$$v(-a) = v(-1) + v(a) = 0 + v(a) = v(a)$$

(2) Suppose $v(a) > v(b)$. Then

$$v(a+b) \geq \min\Big(v(a), v(b)\Big) = v(b)$$

On the other hand,

$$v(b) = v(a+b-a) \geq \min\Big(v(a+b), v(-a)\Big) = \min\Big(v(a+b), v(a)\Big)$$

Since $v(b) < v(a)$, this min can't be $v(a)$, so it is $v(a+b)$. Thus $v(b) \geq v(a+b)$. Since we have inequality both ways, $v(b) = v(a+b)$. (3) Suppose $a_1 + \ldots + a_n = 0$ with $a_i \in K^\times$. Fix j so that $v(a_j)$ is minimal. Then rearrange the equation to

$$-a_j = a_1 + \ldots + \widehat{a_j} + \ldots + a_n$$

Applying v to this, we obtain

$$v(-a_j) = v(a_j) = v\Big(a_1 + \ldots + \widehat{a_j} + \ldots + a_n\Big) \geq \min\Big(v(a_1), \dots, \widehat{v(a_j)}, \dots, v(a_n)\Big)$$

Since j was chosen so that $v(a_j)$ is minimal among $v(a_i)$, we also get

$$\min\Big(v(a_1), \dots, \widehat{v(a_j)}, \dots, v(a_n)\Big) \geq v(a_j)$$

Thus we get equality. Thus there is another index k so that $v(a_k) = v(a_j)$. □

References

[1] James S. Milne. Algebraic number theory (v3.07), 2017. Available at www.jmilne.org/math/.