Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 1

Delivery: 27/10/2015

The goal of this Problem Set is to give two proofs (a geometric one and an algebraic one) of the following result[1]:

Characterization of the Pythagorean Triplets (CPT). If x, y, z are positive integers satisfying
$$x^2 + y^2 = z^2,$$
in which case (x, y, z) is called a *Pythagorean triple*, then there exists a positive integer d and two relatively prime integers u and v such that
$$x = d(u^2 - v^2), \quad y = 2duv, \quad z = d(u^2 + v^2),$$
up to permutation of x and y.

Geometric proof. Consider, on the affine XY-plane, the circle
$$C\colon X^2 + Y^2 = 1$$
and the line
$$L_m\colon Y + m(X + 1) = 0,$$
for $m \in \mathbb{Q}$. Let $P_m = (A_m, B_m)$ denote the intersecting point of L_m and C distinct from $(-1, 0)$.

Exercise 1A. Show that for every $P = (A, B) \in C$ with $A, B \in \mathbb{Q}$ and distinct from $(-1, 0)$, there exists $m \in \mathbb{Q}$ such that $(A, B) = (A_m, B_m)$.

Exercise 1B. Compute (A_m, B_m) in terms of m.

Exercise 1C. Deduce (CPT) from the previous two exercises.

Algebraic proof. We will consider the *field of rational Gauss numbers*
$$\mathbb{Q}(i) = \{a + ib \,|\, a, b \in \mathbb{Q}\},$$
where $i = \sqrt{-1}$. We define the *norm* of a rational Gauss number $\alpha = a + ib$ as
$$N(\alpha) = \alpha\bar{\alpha} = (a + ib)(a - ib) = a^2 + b^2.$$

Exercise 2A. Show that for $\alpha \in \mathbb{Q}(i)$:
$$N(\alpha) = 1 \quad \text{if and only if} \quad \alpha = \frac{\beta}{\bar{\beta}} \text{ for some nonzero } \beta \in \mathbb{Q}(i).$$
(Hint: $\alpha(1 + \bar{\alpha}) = \alpha + \alpha\bar{\alpha}$).

Exercise 2B. If (x, y, z) is Pythagorean a triple, define $\alpha = \frac{x}{z} + i\frac{y}{z}$. Deduce (CPT) by applying the previous exercise to α.

[1] In a future Problem Set we will give a third proof of this result (an arithmetic proof).

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 2

Delivery: 3/11/2015

Exercise 1. Let $\mathbb{F}$ denote a finite field. Show that for every $a \in \mathbb{F}$, there exist $x, y \in \mathbb{F}$ such that $a = x^2 + y^2$.

Hint: Compute the cardinality of the sets $\{x^2 \mid x \in \mathbb{F}\}$ *and* $\{a - y^2 \mid y \in \mathbb{F}\}$. *Distinguish whether* $\mathbb{F}$ *has characteristic* 2 *or* $\neq 2$.

Exercise 2.

i) Let M be $\mathbb{Z}^2$ and $M' \subseteq M$ the submodule generated by

$$v_1 = (2, 0) \qquad \text{and} \qquad v_2 = (3, 2)\,.$$

Find a basis b_1, b_2 for M and $\alpha_1, \alpha_2 \in \mathbb{Z}$ with $\alpha_1 | \alpha_2$ such that $M' = \langle \alpha_1 b_1, \alpha_2 b_2 \rangle_{\mathbb{Z}}$.

ii) Let M be $\mathbb{Z}^3$ and $M' \subseteq M$ the submodule generated by

$$v_1 = (4, 54, 0), \qquad v_2 = (2, 0, 12), \qquad \text{and} \qquad v_3 = (0, 24, -12)\,.$$

Find a basis b_1, b_2, b_3 for M and $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$ with $\alpha_1 | \alpha_2 | \alpha_3$ such that $M' = \langle \alpha_1 b_1, \alpha_2 b_2, \alpha_3 b_3 \rangle_{\mathbb{Z}}$.

Exercise 3. Let R be a PID and let $A \in \mathrm{M}_{n \times n}(R)$ be a square matrix with coefficients in R. Show that there exist $\alpha_1, \dots, \alpha_n \in R$ with $\alpha_1 | \dots | \alpha_n$ and invertible matrices $S, T \in \mathrm{GL}_n(R)$ such that

$$\begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \alpha_n \end{pmatrix} = SAT\,.$$

The diagonal matrix on the left is called the *Smith normal form* of A and the elements $\alpha_i \in R$ are called its *invariant factors*.

Hint: View A *as a linear map* $R^n \to R^n =: M$, *and denote its image by* M'. *Use the elementary divisor theorem to find a basis* $B = (b_1, \dots, b_n)$ *of* M *and* $\alpha_1, \dots, \alpha_q \in R$ *with* $\alpha_1 | \dots | \alpha_q$ *such that* M' *is generated by the* $\alpha_i b_i$, $i = 1, \dots, q$. *Set* $\alpha_i = 0$ *for* $i = q + 1, \dots, n$.

Show that $R^n \cong \ker(A) \oplus M'$, *and that* $\ker(A)$ *is a free* R*-module of rank* $s := n - q$. *Conclude by assembling everything into a commutative diagram*

$$\begin{tikzcd} R^n \arrow[r] \arrow[d, "\cong"] & M' \arrow[r] \arrow[d, "\cong"] & M \arrow[d, "\cong"] \\ R^{q+s} \arrow[r] & R^q \arrow[r] & R^n \end{tikzcd}$$

where the map $R^{q+s} \to R^n$ in the lower row is given, with respect to the standard bases, by a map of the desired form. Define the matrices S and T using the outer column isomorphisms.

Exercise 4. Let k be a field.

i) Let $g(T) = T^d + a_{d-1}T^{d-1} + \cdots + a_0 \in k[T]$ be a monic polynomial with coefficients in k. Denote by V the k-vector space $k[T]/(g)$. Consider the endomorphism
$$\phi\colon V \to V$$
defined by $\phi(f) = fT$. Give the matrix of $\mathrm{M}_{d\times d}(k)$ corresponding to the endomorphism ϕ with respect to the basis $1, T, \ldots, T^{d-1}$.

ii) Let V be a finite dimensional k-vector space and $\phi\colon V \to V$ an endomorphism. Consider the ring homomorphism
$$k[T] \to \mathrm{End}(V)$$
that maps T to ϕ. It endows V with a structure of $k[T]$-module. Show that there exists a k-basis of V so that the matrix of ϕ with respect to this basis is a block diagonal matrix all of whose blocks are of the form
$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & * \\ 1 & 0 & 0 & \ldots & 0 & * \\ 0 & 1 & 0 & \ldots & 0 & * \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & * \\ 0 & 0 & 0 & \ldots & 1 & * \end{pmatrix}.$$
Hint: Apply the structure theorem of finitely generated modules over PIDs to the $k[T]$-module V.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 3

Delivery: 10/11/2015

Exercise 1. Let K be a field and G a finite subgroup of $K^\times$. Show that G is cyclic.

Hint: Use that there exists $z \in G$ *such that* $\mathrm{ord}(x)|\mathrm{ord}(z)$ *for every* $x \in G$.

Exercise 2. Let $\mathbb{F}_q$ be the finite field of cardinality q. Show that the set

$$\{(x, y, z) \in \mathbb{F}_q^3 \,|\, x^2 = yz\}$$

has cardinality q^2.

Exercise 3. Let p be a prime and $a_1, \dots, a_{2p-1} \in \mathbb{Z}$. Show that there exists a subset $I \subseteq \{1, \dots, 2p-1\}$ of cardinality $|I| = p$ such that

$$\sum_{i \in I} a_i \equiv 0 \pmod{p}.$$

Hint: Consider the polynomials $\sum_{i=1}^{2p-1} x_i^{p-1}$, $\sum_{i=1}^{2p-1} a_i x_i^{p-1} \in \mathbb{F}_p[x_1, \dots, x_{2p-1}]$.

Exercise 4. Show that the ring $R = \mathbb{Q}[X, Y]/(Y^2 - X^3)$ is a domain. Show that there exists an element in $\mathrm{Frac}(R)$ which is integral over R, but not contained in R.

Hint: Identify R *with a subring of* $\mathbb{Q}[T]$ *by giving a ring homomorphism* $\mathbb{Q}[X, Y] \to \mathbb{Q}[T]$ *with kernel* $(Y^2 - X^3)$.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 4

Delivery: 17/11/2015

Exercise 1. Let A be an integrally closed domain and let K be its fraction field.

i) Let L/K be a finite extension and let B be the integral closure of A in L. Show that for every $x \in L$, there exists $b \in B$ and $a \in A$ such that $x = b/a$.

ii) Let $f, g \in K[T]$ be monic polynomials such that $f \cdot g \in A[T]$. Show that $f, g \in A[T]$.

Exercise 2. Let $\mathbb{F}_q$ denote the finite field of cardinality q. Consider the norm map

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q \,.$$

Fix a basis B of the n-dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$. Show that there exists a homogenous polynomial $N(y_1, \ldots, y_n) \in \mathbb{F}_q[y_1, \ldots, y_n]$ of degree n and with no non-trivial zero such that if $(x_1, \ldots, x_n)$ are the coordinates of $x \in \mathbb{F}_{q^n}$ in the basis B, then

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = N(x_1, \ldots, x_n) \,.$$

Exercise 3. Let L/K be a finite separable extension of degree $n = [L : K]$. By the primitive element theorem, $L = K(x)$ for some $x \in L$. Let f denote the minimal polynomial of x. Show that

$$D(1, x, \ldots, x^n) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(x)) \,.$$

Compute the above expression in terms of $a, b \in K$ in the case that $f(T) = T^n + aT + b$ for $n = 2, 3$.

Hint: For $n = 3$, the result is $-27b^2 - 4a^3$.

Exercise 4.

i) Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$. Show that the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

ii) Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - d = 0$ with $d \neq \pm 1$ a squarefree integer. Show that $[K : \mathbb{Q}] = 3$ and that $\mathcal{O}_K \subseteq \frac{1}{3}\mathbb{Z}[\alpha]$.

Hint: Let $\theta = u + \alpha v + w\alpha^2$ with $u, v, w \in \mathbb{Q}$ be an element of $\mathcal{O}_K$. Compute

$\mathrm{Tr}_{K/\mathbb{Q}}(\theta) = 3u \in \mathbb{Z}$, $\qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\theta) = 3wd \in \mathbb{Z}$, $\qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2\theta) = 3vd \in \mathbb{Z}$,

$$\mathrm{N}_{K/\mathbb{Q}}(\theta) = u^3 + v^3 d + w^3 d^2 - 3uvwd \in \mathbb{Z}\,.$$

By considering $3^3 \cdot d \cdot \mathrm{N}_{K/\mathbb{Q}}(\theta)$ *and* $3^3 \cdot \mathrm{N}_{K/\mathbb{Q}}(\theta)$ *deduce that* $3u, 3v, 3w \in \mathbb{Z}$.

iii) Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - 17 = 0$. Show that the ring of integers of K is

$$\mathcal{O}_K = \mathbb{Z}\left[1, \alpha, \frac{\alpha^2 - \alpha + 1}{3}\right].$$

Hint: Combining Exercise 3 and Exercise 4 ii), first note that the discriminant of K *is either* $-3^3 \cdot 17^2$ *or* $-3 \cdot 17^2$. *Show that* $\beta := (\alpha^2 - \alpha + 1)/3$ *satisfies* $\beta^3 - \beta^2 + 6\beta - 12 = 0$. *For this you may use that* $\beta = 6/(\alpha + 1)$. *Compute* $D(1, \alpha, \beta)$ *from* $D(1, \alpha, \alpha^2)$ *to deduce that the discriminant of* K *is* $-3 \cdot 17^2$.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 5

Delivery: 24/11/2015

Exercise 1. Let p be an odd prime and ζ_p a primitive pth root of unity in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

i) Show that the discriminant $D(1, \zeta_p, \dots, \zeta_p^{p-2})$ of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ is $(-1)^{\frac{p-1}{2}} p^{p-2}$.

   Hint: Use Exercise 3 of Problem Set 4 and note that $(\zeta_p - 1)(\Phi_p'(\zeta_p)) = p\zeta_p^{-1}$, *where* Φ_p *denotes the pth cyclotomic polynomial.*

ii) Show that $\sqrt{(-1)^{\frac{p-1}{2}} p}$ is an element of the ring of integers of $\mathbb{Q}(\zeta_p)$. Which is its expression with respect to the basis $1, \zeta_p, \dots, \zeta_p^{p-2}$?

   Hint: You have already seen this in a different context.

iii) Deduce that $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield, which is real if $p \equiv 1 \pmod 4$ and imaginary if $p \equiv 3 \pmod 4$.

Exercise 2. Let K be a number field of degree n. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ are algebraic integers of K, show that

$$D(\alpha_1, \dots, \alpha_n) \equiv 0 \pmod 4 \quad \text{or} \quad D(\alpha_1, \dots, \alpha_n) \equiv 1 \pmod 4 .$$

Hint: Let $\mathfrak{A}_n$ *denote the alternating group, that is, the subgroup of the symmetric group* $\mathfrak{S}_n$ *made of permutations of positive sign. Let* $\sigma_1, \dots, \sigma_n$ *be the embeddings of* K *into* $\overline{\mathbb{Q}}$*. Show that if we set*

$$P = \sum_{\pi \in \mathfrak{A}_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}), \qquad N = \sum_{\pi \in \mathfrak{S}_n \setminus \mathfrak{A}_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\pi(i)}),$$

then $PN, P + N \in \mathbb{Z}$*. Conclude by expressing the discriminant in terms of* P *and* N *in a suitable way.*

Exercise 3.

i) Let $p \neq q$ be primes. Show that the following are equivalent:

   a) There exists $a \in \mathbb{Z}$ such that $\Phi_q(a) \equiv 0 \pmod p$.
   b) $p \equiv 1 \pmod q$.

ii) Let q be a prime number. Prove that there exist infinitely many primes p such that

$$p \equiv 1 \pmod q .$$

Hint: Suppose that there exist only finitely many primes p with $p \equiv 1 \pmod q$ and let Π denote their product. Show that $\Phi_q(q\Pi) > 1$, that any prime dividing $\Phi_q(q\Pi)$ is $\equiv 1 \pmod q$, and that this is a contradiction with the initial claim.

Exercise 4.

i) Give an example of a ring A, a finitely generated A-module M, and a submodule $N \subseteq M$ which is not finitely generated.

ii) Give an example of a noetherian ring B and a subring $A \subseteq B$ which is not a noetherian ring.

iii) Let A be a ring, M an A-module, $M' \subseteq M$ a submodule, and $M'' = M/M'$. Show that M is noetherian if and only if so are M' and M''.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 6

Delivery: 1/12/2015

Exercise 1. Let R be a Dedekind domain. Show that R is a UFD if and only if R is a PID.

Exercise 2. Show that a Dedekind domain R with only finitely many non-zero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ is a PID.

Hint: For $i = 1, \dots, r$, consider $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Use the Chinese Remainder Theorem to find $z_i \in R$ such that $z_i \equiv \pi_i \pmod{\mathfrak{p}_i}$ and $z_i \equiv 1 \pmod{\mathfrak{p}_j}$ for every $j \neq i$. Determine the factorization into prime ideals of (z_i).

Exercise 3.

i) Show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

ii) Give the factorization into prime ideals of $(6) \subseteq \mathbb{Z}[\sqrt{-5}]$.

Exercise 4. Let $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt[3]{2}$. Let $R = \mathcal{O}_K$ denote the ring of integers of K.

i) Show that α and $\alpha + 1$ are prime elements of R.

ii) Determine the factorization into prime ideals of $(2) \subseteq R$ and $(3) \subseteq R$.

Hint: Note that $3 = (\alpha - 1)(\alpha + 1)^3$.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 7

Delivery: 8/12/2015

Exercise 1. Let K be a number field and let $2r_2$ be the number of complex non-real embeddings of K. If $x_1, \ldots, x_n$ is a $\mathbb{Q}$-basis of K, show that

$$\operatorname{sign}(D(x_1, \ldots, x_n)) = (-1)^{r_2}.$$

Hint: Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K into $\mathbb{C}$. What is the complex conjugate of $\det(\sigma_j(x_i))$*?*

Exercise 2. (Minkowski's theorem on linear forms). Let

$$\lambda_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} a_{ij} x_j, \qquad i = 1, \ldots, n,$$

be real linear forms such that $\det(a_{ij}) \neq 0$, and let $c_1, \ldots, c_n$ be positive real numbers such that $c_1 \cdots c_n > |\det(a_{ij})|$. Show that there exist integers $m_1, \ldots, m_n \in \mathbb{Z}$ such that

$$|\lambda_i(m_1, \ldots, m_n)| < c_i, \qquad i = 1, \ldots, n.$$

Exercise 3. Show that $\sum_{j \geq 1} 10^{-(j!)} \in \mathbb{R}$ is a transcendental number.

Hint: Apply Liouville's theorem.

Exercise 4. Let $K = \mathbb{Q}(\sqrt{-23})$ and let $\mathcal{O}_K$ denote its ring of integers.

i) Determine prime ideals $\mathfrak{p}, \overline{\mathfrak{p}} \subset \mathcal{O}_K$ such that $\mathfrak{p}\overline{\mathfrak{p}} = (2) \subset \mathcal{O}_K$. Deduce that $\mathfrak{p}$ is not a principal ideal.

ii) Show that $\mathfrak{p}^3$ is a principal ideal.

Hint: Consider the prime ideal factorization of $\left(\frac{3+\sqrt{-23}}{2}\right) \subset \mathcal{O}_K$.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 8

Delivery: 15/12/2015

Exercise 1.

i) Show that the quadratic fields

$$\mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{13}),\ \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7})$$

have class number 1.

Hint: Note that if K is a quadratic field, then the Minkowski bound is $\sqrt{|\mathrm{disc}(K)|}/2$ if K is real and $2\sqrt{|\mathrm{disc}(K)|}/\pi$ if K is imaginary.

ii) Compute the class number of $K = \mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$.

Exercise 2. Let K be a quadratic field and let $\mathcal{O}_K$ be its ring of integers. Let $\alpha \in \mathcal{O}_K$ be such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and let $q(x)$ denote its minimal polynomial. Let $\overline{q}(x) \in \mathbb{F}_p[x]$ be the reduction of $q(x)$ modulo p. Show that the decomposition of the ideal generated by a rational prime p in $\mathcal{O}_K$, denoted $p\mathcal{O}_K$, is as follows:

i) If $\overline{q}(x)$ is the product of two distinct linear polynomials in $\mathbb{F}_p[x]$, then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct prime ideals of $\mathcal{O}_K$.

ii) If $\overline{q}(x)$ is irreducible over $\mathbb{F}_p[x]$, then $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.

iii) If $\overline{q}(x)$ is the square of a linear polynomial in $\mathbb{F}_p[x]$, then $p\mathcal{O}_K = \mathfrak{p}^2$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$.

Hint: Note that $\mathcal{O}_K/p\mathcal{O}_K \simeq (\mathbb{Z}[x]/q(x))/(p) \simeq \mathbb{F}_p[x]/\overline{q}(x)$.

Exercise 3.

i) Show that $K = \mathbb{Q}(\sqrt{-5})$ has class group isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Hint: Show that the class group is generated by the prime ideal dividing $2\mathcal{O}_K$ and that it is non principal.

ii) Show that $K = \mathbb{Q}(\sqrt{-23})$ has class group isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

Hint: Show that the class group is generated by the prime ideals dividing $2\mathcal{O}_K$ and $3\mathcal{O}_K$, show that they are non principal, and find relations among them by looking at the prime ideal decomposition of $\left(\frac{3+\sqrt{-23}}{2}\right)\mathcal{O}_K$ and $\left(\frac{1+\sqrt{-23}}{2}\right)\mathcal{O}_K$.

Exercise 4. Show that, for every number field K, there is a finite extension L/K such that, for every ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the ideal $\mathfrak{a}\mathcal{O}_L$ of $\mathcal{O}_L$ is principal.

Hint: Use the finiteness of the class group.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 9

Delivery: 12/1/2016

Exercise 1.

i) Show that $K = \mathbb{Q}(\sqrt{-14})$ has class group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Hint: Show that the class group is generated by the prime ideals dividing $2\mathcal{O}_K$ and $3\mathcal{O}_K$, show that they are non principal, and find relations among them by looking at the prime ideal decomposition of $(2+\sqrt{-14})\mathcal{O}_K$.

ii) Show that $K = \mathbb{Q}(\sqrt{-30})$ has class group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Hint: Show that the class group is generated by the prime ideals dividing $2\mathcal{O}_K$, $3\mathcal{O}_K$, and $5\mathcal{O}_K$, show that they are non principal, and find relations among them by finding a principal ideal of norm 30.

iii) Show that $K = \mathbb{Q}(\sqrt{-26})$ has class group isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

Exercise 2. Show that if K is a quadratic imaginary field, then

i) $\mu_K = \{1, -1, i, -i\}$ if $K = \mathbb{Q}(i)$, where $i = \sqrt{-1}$.

ii) $\mu_K = \{\omega^j \mid 0 \le j \le 5\}$ if $K = \mathbb{Q}(\omega)$, where $\omega = \frac{1+\sqrt{-3}}{2}$.

iii) $\mu_K = \{\pm 1\}$, otherwise.

Exercise 3. Let $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ be a number field of degree 4. Prove that the cardinality of μ_K is 2, 4, 6, 8, or 12. Give examples of K showing that all these values can occur.

Hint: Use that if ζ_n denotes a primitive n-th root of unity, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$ denotes the Euler φ-function. Note that by the Chinese Remainder Theorem, we have that $\varphi(nm) = \varphi(n)\varphi(m)$ if $(n,m) = 1$. From the easy fact that $\varphi(p^i) = p^{i-1}(p-1)$ if p is a prime and $i \ge 1$, one has

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product runs over primes p dividing n.

Exercise 4. Let p be an odd prime, ζ_p a primitive pth root of unity, and $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ the ring of integers of $K = \mathbb{Q}(\zeta_p)$.

i) Show that if k is an integer such that $0 \le k \le p-1$, then

$$\xi = 1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{k-1} \in \mathcal{O}_K^\times .$$

Hint: Recall that $|N_{K/\mathbb{Q}}(1-\zeta_p)| = |N_{K/\mathbb{Q}}(1-\zeta_p^k)| = p$ and note that $\xi(1-\zeta_p) = 1-\zeta_p^k$.

ii) Show that the roots of unity of K are of the form $\pm\zeta_p^k$ for $0 \le k \le p-1$.

Hint: Let $G \subseteq K^\times$ be the subgroup generated by the roots of unity of K. Thus $G = \langle \zeta_n \rangle$ for a certain primitive n-th root of unity ζ_n. Note that $2p|n$ and $\varphi(n) = \varphi(2p)$.

iii) Take an embedding $K \subseteq \mathbb{C}$. Show that any unit $u \in \mathcal{O}_K^\times$ can be written as $u = \zeta_p^i v$, where $0 \le i \le p-1$ and $v \in \mathbb{R} \cap \mathcal{O}_K^\times$.

Hint: Let c denote complex conjugation and note that it restricts to an automorphism of K. Show that $u/c(u)$ is a root of unity in K by noting that the absolute value of all of its Galois conjugates is 1. Note that $\mathfrak{p} = (1-\zeta_p) = (1-c(\zeta_p)) \subseteq \mathcal{O}_K$ by i), and this is a prime ideal by the hint in i). Rule out the possibility $u/c(u) = -\zeta_p^j$, for some $0 \le j \le p-1$, by finding a contradiction by reducing modulo $\mathfrak{p}$. Deduce the statement from $u/c(u) = \zeta_p^j$.

iv) Show that the fundamental unit of $\mathbb{Q}(\sqrt{5})$ is $\frac{1+\sqrt{5}}{2}$.

v) Let now $p = 5$, $\zeta = \zeta_5$. Show that

$$\mathcal{O}_K^\times = \{\pm\zeta^i(1+\zeta)^j \,|\, 0 \le i \le 4, j \in \mathbb{Z}\}.$$

Hint: Use that $-\zeta^2(1+\zeta) = (1+\sqrt{5})/2$ (see Ex.1.ii) of PS5, for example) and also take iii) and iv) into consideration.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 10

Delivery: 19/1/2016

Exercise 1. Let A be a Dedekind ring and let K be its fraction field. Let L/K be a finite extension and let B be the integral closure of A in L. Given an ideal $\mathfrak{b} \subseteq B$, let $N_{L/K}(\mathfrak{b}) \subseteq A$ be the ideal generated by all the elements $N_{L/K}(b)$, where $b \in \mathfrak{b}$. The ideal $N_{L/K}(\mathfrak{b})$ is called the *relative norm* of $\mathfrak{b}$.

i) Show that $N_{L/K}(bB) = N_{L/K}(b)A$ for all $b \in B$.

ii) Let $S \subseteq A$ be a multiplicative set. If $\mathfrak{a} \subseteq A$ (resp. $\mathfrak{b} \subseteq B$) is an ideal, denote by $\mathfrak{a}_S$ (resp. $\mathfrak{b}_S$) the ideal in $S^{-1}A$ (resp. $S^{-1}B$) generated by $\mathfrak{a}$ (resp. $\mathfrak{b}$). Prove that $N_{L/K}(\mathfrak{b})_S = N_{L/K}(\mathfrak{b}_S)$.

iii) Show that $N_{L/K}(\mathfrak{b}_1\mathfrak{b}_2) = N_{L/K}(\mathfrak{b}_1)N_{L/K}(\mathfrak{b}_2)$ for all ideals $\mathfrak{b}_1, \mathfrak{b}_2 \in B$.

Hint: Check the equality of ideals locally. For a maximal ideal $\mathfrak{p} \subseteq A$, write $S = A \setminus \mathfrak{p}$. Note that A_S is a DVR and that B_S is a PID by Ex. 2 of PS6.

Exercise 2. Let A be a DVR with uniformizer π and let K be its fraction field. Let L/K be a finite Galois extension and let B be the integral closure of A in L. Then B is a PID with only finitely many prime ideals $(\Pi_1), \ldots, (\Pi_q)$, where $\Pi_i \in B$ are such that

$$\pi = u \cdot \Pi_1^{e_1} \cdots \Pi_q^{e_q}\,,$$

for some $u \in A^\times$ and some integers $e_i \geq 1$. Show that $\mathrm{Gal}(L/K)$ acts transitively on the set $\{(\Pi_1), \ldots, (\Pi_q)\}$ and deduce that $e_1 = \cdots = e_q$ and that $N_{L/K}(\Pi_1) = \cdots = N_{L/K}(\Pi_q)$.

Exercise 3. Let A be a Dedekind ring and let K be its fraction field. Let L/K be a finite Galois extension and let B be the integral closure of A in L. Let $\mathfrak{P}$ be a nonzero prime ideal of B and $\mathfrak{p} = \mathfrak{P} \cap A$. Prove that

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f,$$

where f is the residue degree of $\mathfrak{P}$ over K.

Exercise 4. Let K be a number field. For an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, recall that we have defined the *absolute norm*

$$\mathcal{N}(\mathfrak{a}) = \#\mathcal{O}_K/\mathfrak{a}\,.$$

Show that there is an equality $N_{K/\mathbb{Q}}(\mathfrak{a}) = (\mathcal{N}(\mathfrak{a}))$ of ideals of $\mathbb{Z}$.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 11

Delivery: 26/1/2016

Exercise 1. Show that $L = \mathbb{Q}(\zeta_{23})$ is not a PID.

Hint: By Ex. 1 of PS5, $K = \mathbb{Q}(\sqrt{-23})$ *is a subfield of* L*. By Ex. 4 of PS7,* $2\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$*, where* $\mathfrak{p}$ *and* $\overline{\mathfrak{p}}$ *are two distinct non principal prime ideals of* $\mathcal{O}_K$ *such that* $\mathfrak{p}^3$ *and* $\overline{\mathfrak{p}}^3$ *are principal. Let* $\mathfrak{P} \subseteq \mathcal{O}_L$ *be a prime ideal lying above* $\mathfrak{p} \subseteq \mathcal{O}_K$*. Show that* $\mathfrak{P}$ *is non principal. For this, argue that* $N_{L/K}(\mathfrak{P})$ *cannot be a principal ideal of* $\mathcal{O}_K$ *by using Ex. 3 of PS10, and conclude by applying Ex. 1 of PS10.*

Exercise 2.

i) Let p be a prime number, and let $K/\mathbb{Q}$ be a number field such that $[K : \mathbb{Q}] > p$. Show that if (p) splits completely in $\mathcal{O}_K$, then $\mathcal{O}_K$ can not be of the form $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for any $\alpha \in \mathcal{O}_K$.

ii) Let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$. Show that $\beta = (\alpha + \alpha^2)/2 = (\alpha - 4)/\alpha$ is in $\mathcal{O}_K$, that $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with

$$\mathfrak{p}_1 = (2, 1+\alpha), \qquad \mathfrak{p}_2 = (2, \beta), \qquad \mathfrak{p}_3 = (2, 1+\alpha+\beta),$$

and that the $\mathfrak{p}_i$ are primes pairwise coprime (and in particular distinct). Deduce that $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for any $\alpha \in \mathcal{O}_K$.

Hint: Note that first $\beta^3 - 2\beta^2 + 3\beta - 10 = 0$*. Deduce the required equality of ideals from the formulas*

$$\begin{aligned} \supseteq&: \quad (1+\alpha)\beta(1+\alpha+\beta) = -2(2a+7) \\ \subseteq&: \quad -2\cdot 2\cdot 2 - (1+\alpha)\beta(1+\alpha+\beta) - 2\cdot 2\cdot(1+\alpha) = 2 \end{aligned}$$

Note that checking coprimality of the $\mathfrak{p}_i$ *amounts to showing that* $(2, 1+\alpha, \beta) = \mathcal{O}_K$*. For this note that* $(1+\alpha)(\beta-1) - \beta = 5$*.*

Exercise 3.

i) Show that for every integer $d < -11$, the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-d})$ is not a euclidean ring.

ii) Show that the ring of integers of $\mathbb{Q}(\sqrt{-163})$ is a PID but not a euclidean ring.

Hint: You may show that $\mathbb{Q}(\sqrt{-163})$ *has class number* 1*, using the same method as in Ex. 3 of PS8 or Ex. 1 of PS9.*

Exercise 4. Let R be an artinian ring. Denote by $\mathfrak{M}_1, \dots, \mathfrak{M}_n$ its maximal ideals. Prove that the natural homomorphism $R \to \prod_{i=1}^n R_{\mathfrak{M}_i}$ is an isomorphism.

Hint: You may use the fact without proof that an artinian ring is noetherian.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 12

Delivery: 2/2/2016

Exercise 1. Show that if A is a local noetherian ring with maximal ideal $\mathfrak{m}$ generated by a non-nilpotent element π, then A is a DVR.

Hint: You may use without proof[1] *that* $\cap_{i=0}^{\infty}\mathfrak{m}^i = 0$.

Exercise 2. Let R be a discrete valuation ring with maximal ideal $\mathfrak{m} = (\pi)$ and residue class field $k = R/\mathfrak{m}$. Let $f \in R[x]$ be an Eisenstein polynomial[2] and $R' = R[x]/(f)$. Let K and K' be the fraction fields of R and R', respectively. Prove that R' is a discrete valuation ring, that R' is equal to the integral closure of R in K' and that $\mathfrak{M}$ is totally ramified in R', that is, that the ramification index of the maximal ideal $\mathfrak{M}'$ of R' is $[K' : K]$.

Hint: Use Exercise 1.

Exercise 3. Let $K \subseteq K' \subseteq K''$ be number fields. Let $\mathfrak{P}''$ be a maximal ideal of $\mathcal{O}_{K''}$ and $\mathfrak{P}' = \mathfrak{P}'' \cap \mathcal{O}_{K'}$. Prove that

$$f_{K''/K}(\mathfrak{P}'') = f_{K''/K'}(\mathfrak{P}'')\cdot f_{K'/K}(\mathfrak{P}'), \quad e_{K''/K}(\mathfrak{P}'') = e_{K''/K'}(\mathfrak{P}'')\cdot e_{K'/K}(\mathfrak{P}').$$

Exercise 4. Let α be a root of $x^3 - 13x + 7$ and L the normal closure of $K = \mathbb{Q}(\alpha)$. Show that:

i) $\mathcal{O}_K = Z[\alpha]$.

ii) $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2$ for certain prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of $\mathcal{O}_K$.

iii) $\mathfrak{p}_1\mathcal{O}_L = \mathfrak{P}_1^2$ and $\mathfrak{p}_2\mathcal{O}_L = \mathfrak{P}_2\mathfrak{P}_3$ for certain prime ideals $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$ of $\mathcal{O}_L$.

iv) K is the subfield of L fixed by the decomposition group of $\mathfrak{P}_1$.

Hint: 1493 *is a prime number.*

[1] In fact, for every ideal $\mathfrak{a}$ in a noetherian ring, the intersection $\cap_{i=0}^{\infty}\mathfrak{a}^i$ is $= 0$, Atiyah-McDonald, *An introduction to commutative algebra*, Corollary 10.18. For a simpler proof in the situation at hand, see Serre, *Local fields*, Springer, Proposition 2, Chapter 1.

[2] I.e., the leading coefficient is 1, all other coefficients are in $\mathfrak{m}$, and the constant coefficient is not in $\mathfrak{m}^2$. This implies that f is irreducible.

Prof. Dr. U. Görtz
Dr. F. Fité

Wintersemester 2015/16

ALGEBRAIC NUMBER THEORY I

Problem Set 13

Delivery: 9/2/2016

Exercise 1. Let $L = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$.

i) Show that the ring of integers of L is $\mathbb{Z}\left[\sqrt{-1}, \frac{1+\sqrt{5}}{2}\right]$. Compute the absolute discriminant of L.

ii) Show that the only primes that ramify in L are 2 and 5, and that the corresponding ramification indices are both 2.

iii) Compute the Frobenius automorphism $\left(\frac{L/\mathbb{Q}}{p}\right)$ for every prime p distinct from 2 and 5. Determine the inertia and decomposition groups of 2 and 5.

iv) Show that no prime ideal of $\mathbb{Q}(\sqrt{-5})$ ramifies in L.

Exercise 2. Let p be a prime and $n > 2$ an integer such that $p \nmid n$. Prove that (p) splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \pmod{n}$.

Exercise 3. .

i) Let k be a finite field and $|\cdot|\colon k \to \mathbb{R}_{\geq 0}$ an absolute value. Prove that $|x| = 1$ for every $x \in k^\times$.

ii) Let k be a field of characteristic p. Show that there does not exist an archimedean absolute value on k.

iii) Give two non-equivalent archimedean absolute values on $\mathbb{Q}(\sqrt{2})$.

Exercise 4. Let k be a field with a non-archimedean absolute value $|\cdot|$. For $x, y \in k$, define $d(x, y) = |x - y|$.

i) Show that if $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$.

ii) For $a \in k$ and $r \in \mathbb{R}_{>0}$, let $D(a, r) = \{x \in k \mid d(x, a) \leq r\}$ be the "closed" disc of center a and radius r. Show that $D(a, r)$ is open and closed in k.

iii) Show that two discs D and D' are either disjoint or concentric (that is, there exists $a \in k$ and $r, r' \in \mathbb{R}_{>0}$ such that $D = D(a, r)$ and $D' = D(a, r')$).

iv) Show that every triangle is isosceles: if for $x, y, z \in k$ one has $d(x, z) < d(y, z)$, then $d(y, z) = d(x, y)$.