Uppsala University
Department of Mathematics
Ernst Dieterich

Master Programme in Mathematics
Examination in mathematics
2012-06-01

Algebraic number theory

Time: 8.00-13.00. No tools are allowed except paper and pen. All solutions must be accompanied by explanatory text. Every problem gives at most 5 points.

1. (a) What is an *integrally closed domain*? Reproduce the definition.

(b) Show that the ring $\mathcal{Z}$ of all algebraic integers is an integrally closed domain.

2. Let $p \geq 5$ be a prime number, and $\zeta = e^{\frac{2\pi}{p}i}$. Let $x, y \in \mathbb{Z}$ be such that $x + \zeta y = \varepsilon\alpha^p$ holds true for certain cyclotomic integers $\varepsilon \in \mathbb{Z}[\zeta]^\iota$ and $\alpha \in \mathbb{Z}[\zeta]$.

(a) Apply Kummer's first lemma on cyclotomic units to derive the congruence

$$x + \zeta y \equiv \zeta^s r \pmod{p}$$

for certain numbers $r \in \mathbb{R}$ and $s \in \mathbb{N}$.

(b) Use complex conjugation to deduce from (a) the further congruence

$$x\zeta^s + y\zeta^{s-1} - x\zeta^{-s} - y\zeta^{1-s} \equiv 0 \pmod{p}$$

(c) Conclude that $x \equiv y \equiv 0 \pmod{p}$, provided that the numbers $\zeta^s, \zeta^{s-1}, \zeta^{-s}, \zeta^{1-s}, \zeta^{p-1}$ are distinct.

3. Let R be a Dedekind domain, with field of fractions K.

(a) What is a *fractional R-ideal*? Reproduce the definition.

(b) What is an *integral R-ideal*? Reproduce the definition.

(c) We know that every fractional R-ideal is invertible. An integral R-ideal A is said to be weakly invertible if $xA \subset R$ for some $x \in K \setminus R$. Show that every proper integral R-ideal A is weakly invertible, while R is not weakly invertible.

4. Let p be a regular prime number, and $\zeta = e^{\frac{2\pi}{p}i}$. Let D_0 and D_1 be non-zero ideals in $\mathbb{Z}[\zeta]$, both not divisible by $(1-\zeta)$ and such that the fractional ideal $(D_1 D_0^{-1})^p$ is principal fractional.

(a) Prove that $D_1 D_0^{-1}$ is principal fractional.

(b) Conclude that there are cyclotomic integers $\alpha, \beta \in \mathbb{Z}[\zeta] \setminus \{0\}$ such that $D_0(\alpha) = D_1(\beta)$.

(c) Prove that $\text{mult}_{(\alpha)}(1-\zeta) = \text{mult}_{(\beta)}(1-\zeta)$.

(d) Conclude that there are cyclotomic integers $\alpha', \beta' \in \mathbb{Z}[\zeta] \setminus (1-\zeta)$ such that $D_1 D_0^{-1} = (\frac{\alpha'}{\beta'})$.

Please turn over!

5. (a) When is a commutative ring called *noetherian*? Reproduce the definition.

(b) Find a finite $\mathbb{Z}$-basis for the $\mathbb{Z}$-module $\mathbb{Z}[\sqrt{5}\,]$.

(c) Show that the commutative ring $\mathbb{Z}[\sqrt{5}\,]$ is noetherian.

6. Show that every non-zero prime ideal in $\mathbb{Z}[\sqrt{5}\,]$ is maximal.

7. (a) What is a *Dedekind domain*? Reproduce the definition.

(b) Is the number $\frac{1+\sqrt{5}}{2}$ an algebraic integer? Motivate your answer.

(c) Is $\mathbb{Z}[\sqrt{5}\,]$ a Dedekind domain? Motivate your answer.

8. Let p and q be prime natural numbers, $\zeta = e^{\frac{2\pi}{q}i}$ and $\mathcal{O} = \mathbb{Z}[\zeta]$. Let P be a prime $\mathcal{O}$-ideal that contains $p\mathcal{O}$. Prove the following assertions.

(a) The quotient ring $\mathcal{O}/P$ is a finite field of order $p \leq |\mathcal{O}/P| \leq p^{q-1}$.

(b) The $\mathcal{O}$-ideal $p\mathcal{O}$ is prime if and only if $|\mathcal{O}/P| = p^{q-1}$.

Good luck!