ALGEBRA: HOMEWORK 6

Problem 1. Is it possible to construct (with ruler and compass) a square whose area is equal to the area of a given triangle?

Proof. Yes, we can construct it. Given a triangle with edge length a, b, c, its area is $A = \sqrt{b^2c^2 + c^2a^2 + a^2b^2 - a^4 - b^4 - c^4}/4$. We just need to construct a segment with length $\sqrt{A}$. This can be done since $\mathbb{Q}(\sqrt{A}) = \mathbb{Q}(A)(\sqrt{A})$ can be obtained by finite quadratic extensions from $\mathbb{Q}$. $\square$

Problem 2. Let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt[3]{a}$ with $a \in \mathbb{Z}$, a squarefree. Show that if $a \neq \pm 1 \pmod 9$ then $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$.

Proof. Since $1, \alpha, \alpha^2 \in \mathcal{O}_K$ and $\mathcal{O}_K$ is a ring, we easily have

$$\mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 \subset \mathcal{O}_K.$$

Assume $b = a_0 + a_1\alpha + a_2\alpha^2 \in \mathcal{O}_K$, where $a_0, a_1, a_2 \in \mathbb{Q}$. It remains to prove $a_0, a_1, a_2 \in \mathbb{Z}$.

Since $\alpha, \zeta_3\alpha, \zeta_3^2\alpha$ are three roots of $x^3 - a = 0$, then $b' = a_0 + a_1\zeta_3\alpha + a_2\zeta_3^2\alpha^2, b'' = a_0 + \zeta_3^2 a_1 + \zeta_3 a_2$ are the other two roots of the minimal polynomial of b, and both are algebraic integers. So

$$b + b' + b'' \in \bar{\mathbb{Z}}$$
$$bb' + bb'' + b'b'' \in \bar{\mathbb{Z}}$$
$$bb'b'' \in \bar{\mathbb{Z}},$$

i.e.,

$$3a_0 \in \mathbb{Z} \tag{1}$$
$$3a_0^2 - 3a_1a_2a \in \mathbb{Z} \tag{2}$$
$$a_0^3 + aa_1^3 + a^2a_2^3 - 3aa_0a_1a_2 \in \mathbb{Z}. \tag{3}$$

For $i = 0, 1, 2$, assume $a_i = p_i/q_i$ where $\gcd(p_i, q_i) = 1, q_i > 0$.

If at least one of a_0, a_1, a_2 is not an integer, we may modify a_0, a_1, a_2 by multiplying a constant integer such that $q_i | p$ for some prime p and at least one of q_0, q_1, q_2 is p.

(i) if $a_0 \in \mathbb{Z}$, then

$$3aa_1a_2 \in \mathbb{Z} \tag{4}$$
$$aa_1^3 + a^2a_2^3 \in \mathbb{Z}. \tag{5}$$

If $a_1 \in \mathbb{Z}$ or $a_2 \in \mathbb{Z}$, by (5) we have that $p^3|a^2$, which is contradictory to that a is a squarefree. So $q_1 = q_2 = p$, then by (4) we have $3 = p$ and $3||a$, and identity (5) cannot be true, contradictory!

(ii) now we assume $a_0 \notin \mathbb{Z}$, then by (1) we have $p = 3$. By (2) we have $3aa_1a_2 \notin \mathbb{Z}$, and thus $3 \nmid a$ and $q_1 = q_2 = 3$. Then by (3) we have

$$a^2p_2^3 + a(p_1^3 - 3p_0p_1p_2) + p_0^3 = 0 \pmod{27}.$$

Let $r = p_0/p_2, s = p_0/p_2 \pmod{27}$ and we have

$$a^2 + a(s^3 - 3rs) + r^3 = 0 \pmod{27}.$$

It is easy to verify that $r = 1 \pmod 3$.

Assume $s = 1 \pmod 3$, otherwise we can substitute (a, s) by $(-a, -s)$. Then

$$r^2 + s^2 + 1 - 3rs = (r + s + 1)[(r + s + 1)^2 - 3(rs + r + s)],$$

and $3|(r+s+1), 9|(r+s+1)^2, 9|3(rs+r+s)$, so $r^2+s^2+1-3rs = 0 \pmod{27}$. So

$$0 = a^2+a(s^3-3rs)+r^3 = a^2-(1+r^3)a+r^3 = (a-1)(a-r^3) \pmod{27}.$$

since $a \neq \pm 1 \pmod 9$, so $9|(a - r^3)$. But $r^3 = \pm 1 \pmod 9$ for any r not divisible by 3, contradictory! □

Problem 3. Find an integral basis for $\mathcal{O}_K$, where $K = \mathbb{Q}(\alpha)$ and $\alpha^3 - \alpha + 1 = 0$.

Proof. It is easy to see that $\mathcal{O} := \mathbb{Z}(\alpha) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 \subset \mathcal{O}_K$, and

$$disc(\mathcal{O}) = disc(1, \alpha, \alpha^2) = -4(-1)^3 - 27 = -23$$
$$disc(\mathcal{O}) = disc(\mathcal{O}_K)[\mathcal{O}_K, \mathcal{O}]^2.$$

Since -23 is a squarefree, $[\mathcal{O}_K, \mathcal{O}] = 1$ and $\mathcal{O}_K = \mathcal{O} = \mathbb{Z}(\alpha)$. □

Problem 4. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - x + 1$. Find the irreducible polynomial for $\gamma := 1 + \alpha^2$ over $\mathbb{Q}$.

Proof. Assume α, β, γ are three roots of $x^3 - x + 1 = 0$. Then

$$\alpha + \beta + \gamma = 0$$
$$\alpha\beta + \beta\gamma + \gamma\alpha = -1$$
$$\alpha\beta\gamma = -1.$$

We can compute

$$(x - (1 + \alpha^2))(x - (1 + \beta^2))(x - (1 + \gamma^2)) = x^3 - 5x^2 + 8x - 5$$

is an irreducible polynomial. □

Problem 5. Let I be an integral ideal in $\mathcal{O}_K$. Then

$$\cap_{n=1}^{\infty} I = \begin{cases} \mathcal{O}_K & \text{if } I = \mathcal{O}_K \\ (0) & \text{otherwise.} \end{cases}$$

Proof. If $I = \mathcal{O}_K$ or (0), the conclusion is trivial. In the other cases, assume $I_\infty = \cap_{n=1}^{\infty} I \neq (0)$ and by unique factorization theorem, $I_\infty = \prod_{i=1}^{n} p_i$ where p_i is a prime ideal. By the definition of I we have that $I_\infty = I_\infty^2$. So $\prod_{i=1}^{n} p_i = \prod_{i=1}^{n} p_i^2$, which is contradictory to the uniqueness of factorization. □