

1 HW SOLUTIONS

Sunday, November 11, 2007

4:48 PM

1. Show that a non-zero square is never followed by a cube

Sol The statement is equivalent to showing that

$$x^2 + 1 = y^3$$

has only the obvious solution $x=0, y=1$.

If x is odd, then $x^2 + 1$ is never a cube as it is congruent to 2 mod 4

Suppose that (x, y) is a solution to the equation

Let us pass to the number ring $\mathbb{Z}[i]$ where the following equality holds: $(x+i)(x-i) = y^3$

A prime element in $\mathbb{Z}[i]$ that divides both $x+i$ and $x-i$ divides their difference $2i$ so it is up to units equal to $1+i$. However, $1+i$ does not divide $x+i$ if x is even, so one concludes that $x+i$

and $x-i$ are coprime in $\mathbb{Z}[i]$. Their product is a cube, so unique factorization in $\mathbb{Z}[i]$

shows that each of them is the product of a unit and a cube in $\mathbb{Z}[i]$. As all units in $\mathbb{Z}[i]$ are cubes, there must be integers

$a, b \in \mathbb{Z}$ s.t. $x+i = (a+bi)^3$. This yields

the equations:

$$x = a(a^2 - 3b^2) \quad \text{and} \quad 1 = (3a^2 - b^2)b$$

It follows that one has $b = \pm 1$ and an

inspection of both cases shows that the only solution to the original equation is the obvious one $x=0, y=1$.

2. Show that $\mathbb{Z}[\sqrt{-2}]$ is a P.I.D.

Sol $\mathbb{Z}[\sqrt{-2}]$ is Euclidean, hence P.I.D.

In fact: one defines the following norm

$$\phi: \mathbb{Z}[\sqrt{-2}] \rightarrow \mathbb{N} \quad \phi(a+b\sqrt{-2}) = a^2 + 2b^2$$

For $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, one considers $\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}}$

Notice that $\beta\bar{\beta} = \phi(\beta)$, so $\frac{\alpha\bar{\beta}}{\beta\bar{\beta}} \in \mathbb{Q}$

Also, $\bar{\beta} \in \mathbb{Z}[\sqrt{-2}]$, so $\alpha\bar{\beta} \in \mathbb{Z}[\sqrt{-2}]$, so

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = c + d\sqrt{-2} \quad \text{for some } c, d \in \mathbb{Q}$$

Choose m and n as the closest integers to

c and d , i.e. so that $|m-c| \leq \frac{1}{2}$ and $|n-d| \leq \frac{1}{2}$

Write $q = m + n\sqrt{-2}$. One gets:

$$\phi\left(\frac{\alpha}{\beta} - q\right) = (c-m)^2 + 2(d-n)^2 \leq \frac{1}{4} + \frac{1}{2} < 1$$

So one writes: $\alpha = q\beta + r$ and $r = \alpha - q\beta$

If $r \neq 0$, then $\phi(r) = \phi(\beta)\phi\left(\frac{\alpha}{\beta} - q\right) < \phi(\beta)$.

3. Let $K = \mathbb{Q}(\sqrt{d})$, with d a square free integer.

Find an integral basis for \mathcal{O}_K

Sol. An arbitrary element $\alpha \in K$

is of the form $\alpha = r_1 + r_2\sqrt{d}$; $r_1, r_2 \in \mathbb{Q}$

Since $[K:\mathbb{Q}] = 2$, α has only one conjugate

$r_1 - r_2 \sqrt{d}$. Moreover:
 $\text{Tr}_K(\alpha) = 2r_1$, $N_K(\alpha) = r_1^2 - dr_2^2$
 are both integers

Since α satisfies the monic polynomial
 $x^2 - 2r_1x + r_1^2 - dr_2^2$,

if $\text{Tr}_K(\alpha), N_K(\alpha) \in \mathbb{Z}$, then α is an algebraic integer.

If $2r_1 \in \mathbb{Z}$, ($r_1 \in \mathbb{Q}$) then the denominator of r_1 can be at most 2

If $r_1^2 - dr_2^2 \in \mathbb{Z}$, the denominator of r_2 cannot be more than 2.

Then, let $r_1 = g_1/2$, $r_2 = g_2/2$, $g_1, g_2 \in \mathbb{Z}$

The second condition amounts to:

$$\frac{g_1^2 - dg_2^2}{4} \in \mathbb{Z},$$

which means that $g_1^2 - dg_2^2 \equiv 0 \pmod{4}$

$$\text{or } g_1^2 \equiv dg_2^2 \pmod{4}$$

CASE 1. $d \equiv 1 \pmod{4}$

if $d \equiv 1 \pmod{4}$ and $g_1^2 \equiv dg_2^2 \pmod{4}$, then

g_1 and g_2 are either both even or both odd.

So if $\alpha = r_1 + r_2\sqrt{d}$ is an algebraic integer of $\mathbb{Q}(\sqrt{d})$, then either r_1 and r_2 are both

integers, or they are both fractions with denominator 2.

Also, if $r \mid (-d+1)$, then $\frac{1+\sqrt{d}}{2}$ is an algebraic integer. This suggests that one may use $1, \frac{1+\sqrt{d}}{2}$ as a basis: it is clear from

the discussion above that this is in fact an integral basis.

CASE 2. $d \equiv 2, 3 \pmod{4}$

If $g_1^2 \equiv d g_2^2 \pmod{4}$, then both g_1 and g_2 must be even. Then a basis for \mathcal{O}_K is $1, \sqrt{d}$: again it is clear that this is an integral basis.

4. Show that every non-zero prime ideal in the ring of integers of a number field contains exactly one integer prime.

Sol If \mathfrak{p} is a prime ideal of \mathcal{O}_K , then certainly it contains an integer. By the definition of a prime ideal, if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. So \mathfrak{p} must contain some rational prime. If \mathfrak{p} contained 2 distinct rational primes p and q say, then it would necessarily contain their greatest common denominator which is 1. But this contradicts the assumption of non-triviality.

5. Let $u_1, u_2, \dots, u_n \in \mathcal{O}_K$ be linearly independent elements over \mathbb{Q} ($K =$ number field, $[K:\mathbb{Q}] = n$, $\mathcal{O}_K =$ ring of integers) Let

$$M = u_1 \mathbb{Z} + \dots + u_n \mathbb{Z}, \quad m = [\mathcal{O}_K : M]$$

Prove that $d_{K/\mathbb{Q}}(u_1, \dots, u_n) = m^2 d_K$

where d_K is the discriminant of K
 and $d_{K/\mathbb{Q}}(u_1, \dots, u_n) := (\det(\sigma_j^i))^{-2}$, for
 $\{\sigma_i, i=1, \dots, n\}$ a set of embeddings of K
 extending a fixed inclusion of $\mathbb{Q} \hookrightarrow \bar{\mathbb{Q}}$

Sol Let $\alpha_1, \dots, \alpha_n$ be an integral basis
 of \mathcal{O}_K . Then M has a basis $\beta_1, \beta_2, \dots, \beta_n$
 s.t. $\beta_i = \sum_{j=1}^n p_{ij} \alpha_j$. Then
 $d_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n) = (\det(p_{ij}))^{-2} d_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = \det^2 d_K$

From this one deduces that

$$d_{K/\mathbb{Q}}(\beta_1, \dots, \beta_n) = d_{K/\mathbb{Q}}(u_1, \dots, u_n)$$

6. Let K and K_1 be two algebraic number fields
 of degree m and m_1 respectively over \mathbb{Q} .

Let $d = \gcd(d_K, d_{K_1})$. Show that if
 $[K_1 K : \mathbb{Q}] = mm_1$, then $\mathcal{O}_{KK_1} \subseteq \frac{1}{d} \mathcal{O}_K \mathcal{O}_{K_1}$

Sol Let $\{\alpha_1, \dots, \alpha_m\}$ be a \mathbb{Z} -basis for \mathcal{O}_K and
 $\{\beta_1, \dots, \beta_{m_1}\}$ be a \mathbb{Z} -basis for \mathcal{O}_{K_1} .

Then $\alpha_i \beta_j \quad 1 \leq i \leq m, 1 \leq j \leq m_1$ is a \mathbb{Q} -basis
 for KK_1 over \mathbb{Q} since $[KK_1 : \mathbb{Q}] = mm_1$

Any $w \in \mathcal{O}_{KK_1}$ can therefore be written as

$$w = \sum_{i,j} \frac{m_{ij}}{r} \alpha_i \beta_j$$

$r, m_{ij} \in \mathbb{Z}$ and $\gcd(r, \gcd(m_{ij})) = 1$.

It suffices to show that $r | d_K$ and by
 symmetry $r | d_{K_1}$, so that $r | d$.

Since $[KK_1 : \mathbb{Q}] = mm_1$, every embedding

σ of K into \mathbb{C} can be extended to KK_1 ,
 acting trivially on K_1 . Hence:

$$\sigma(\omega) = \sum_{j=1}^m \frac{m_{ij}}{r} \sigma(\alpha_i) \beta_j$$

Set $x_i = \sum_{j=1}^m m_{ij} \beta_j / r$. We then obtain m equations:

$$\sum_{i=1}^m \sigma(\alpha_i) x_i = \sigma(\omega)$$

one for each $\sigma: K \hookrightarrow \mathbb{C}$. We solve for x_i by Cramer's rule: $x_i = \delta_i / \delta$ where $\delta = \det(\sigma(\alpha_i))$. Since $\delta^2 = d_K$, one finds

$$\delta \delta_i = \sum_{j=1}^m \frac{\delta^2 m_{ij}}{r} \beta_j \in \mathcal{O}_K$$

since δ and each of β_j are algebraic integers. Hence $d_K m_{ij} / r$ are all integers. It follows that r divides all $d_K m_{ij}$. Since $\gcd(r, \gcd(m_{ij})) = 1$

one deduces that $r | d_K$.

7. Find an integral basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Sol. If $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{3})$, then $d_K = 8$, $d_L = -3$ which are coprime.

By the previous question, a \mathbb{Z} -basis for the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is

given by:

$$\left\{ 1, \sqrt{2}, \frac{1+\sqrt{3}}{2}, \sqrt{2} \left(\frac{1+\sqrt{3}}{2} \right) \right\}$$