A

Excellent

Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 2

B3.3: Algebraic Number Theory

13 February, 2021

Topics covered: integral bases, unique factorisation, Euclidean domains.

Question 1

Show that $f(X) := X^3 - X + 2$ is an irreducible integer polynomial. Let θ be a root of $f(X) = 0$, and calculate the discriminant $\Delta^2(\Theta)$ of $\Theta := \{1, \theta, \theta^2\} \subseteq K := \mathbb{Q}(\theta)$. Using Stickelberger's theorem (Sheet 1 Question 7), show that Θ is an integral basis for K.

Proof. Suppose that f has a root $p/q \in \mathbb{Q}$ with $\gcd(p,q) = 1$. By the rational root test, we have $p \mid 2$ and $q \mid 1$. Hence $p/q = 1$ or 2. But $f(1) = 2$ and $f(2) = 8$. This is impossible. f has no rational roots, and hence is irreducible over $\mathbb{Q}$.

By Lemma 2.3, we have

$$\Delta^2(\Theta) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) \\ \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) & \mathrm{Tr}(\theta^4) \end{pmatrix}$$

Let $\theta_1, \theta_2, \theta_3$ be the roots of f. By Vieta's theorem, we have $\theta_1 + \theta_2 + \theta_3 = 0$ and $\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = -1$. Next we compute the traces:

A

$$\begin{aligned} \mathrm{Tr}(1) &= 3 \\ \mathrm{Tr}(\theta) &= \theta_1 + \theta_2 + \theta_3 = 0 \\ \mathrm{Tr}(\theta^2) &= (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) = 2 \\ \mathrm{Tr}(\theta^3) &= \mathrm{Tr}(\theta - 2) = -6 \\ \mathrm{Tr}(\theta^4) &= \mathrm{Tr}(\theta^2 - 2\theta) = 2 \end{aligned}$$

Therefore

$$\Delta^2(\Theta) = \det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & -6 \\ 2 & -6 & 2 \end{pmatrix} = -104$$

Let $L = \langle \Theta \rangle_{\mathbb{Z}}$. Then L is a $\mathbb{Z}$-submodule of $\mathcal{O}_K$. By Notes 3.13, we have

$$\Delta^2(\Theta) = \Delta^2(L) = m^2 \Delta^2(\mathcal{O}_K) = m^2 \Delta^2(K)$$

for some $m \in \mathbb{Z}_+$. The factorisation of $\Delta^2(\Theta) = -104$ is $-104 = -2^3 \times 13$. Then either $\Delta^2(K) = -104$ or $\Delta^2(K) = -26$. By Stickelberger's Theorem, $\Delta^2(K) \equiv 0$ or $1 \bmod 4$. Hence $\Delta^2(K) = -104$, $m = 1$, and $\mathcal{O}_K = L$. we deduce that Θ is an integral basis of K. □

Question 2

Let K be a number field and let $L = K(\sqrt{\delta})$, where $\delta \in K$ and $\sqrt{\delta} \notin K$. Let $\alpha = \beta + \gamma\sqrt{\delta} \in L$, where $\beta, \gamma \in K$. Show that if $\alpha \in \mathcal{O}_L$ then $\beta - \gamma\sqrt{\delta} \in \mathcal{O}_L$ and $\beta^2 - \gamma^2\delta \in \mathcal{O}_K$.

Proof. By transitivity of integral closure, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L. In particular, $\mathcal{O}_K = K \cap \mathcal{O}_L$.

Since $\alpha \in \mathcal{O}_L$, there exists a monic polynomial $f \in \mathcal{O}_K[x]$ such that $f(\alpha) = 0$. Consider the K-automorphism $\varphi \in \mathrm{Gal}(L \mid K)$ given by $\varphi(\sqrt{\delta}) = -\sqrt{\delta}$. Since φ fixes $\mathcal{O}_K \subseteq K$, we have

A

$$f(\beta - \gamma\sqrt{\delta}) = f(\varphi(\alpha)) = \varphi(f(\alpha)) = 0$$

Hence $\beta - \gamma\sqrt{\delta}$ is integral over $\mathcal{O}_K$. $\beta - \gamma\sqrt{\delta} \in \mathcal{O}_L$.

Since $\mathcal{O}_L$ is a ring, we have

$$\left(\beta + \gamma\sqrt{\delta}\right)\left(\beta - \gamma\sqrt{\delta}\right) = \beta^2 - \gamma^2\delta \in \mathcal{O}_L$$

In addition, $\beta^2 - \gamma^2\delta \in K$ as $\beta, \gamma, \delta \in K$. Hence $\beta^2 - \gamma^2\delta \in K \cap \mathcal{O}_L = \mathcal{O}_K$. □

Question 3

Let R be an integral domain. Show that every prime element in R is irreducible. Suppose now that factorisation into irreducible elements in R is possible. Show that this factorisation is unique if and only if every irreducible element in R is prime.

Proof. Suppose that R is an integral domain. Let $a \in R$ be a prime element. For $x, y \in R$ such that $a = xy$, since a is prime, we have $a = xy \implies a \mid xy \implies a \mid x \vee a \mid y$. But also $a = xy \implies x \mid a \wedge y \mid a$. Hence we have $a \sim x$ or $a \sim y$. Since R is an integral domain, we have $x \in R^\times$ or $y \in R^\times$. Hence a is irreducible.

Now suppose that R is a factorisation domain.

" $\implies$ ": Suppose that R is a UFD. Suppose that a is an irreducible and $a \mid bc$. Since R is a UFD, the irreducible factor of a, which is a itself, is the subset of the union of the irreducible factors of b and c (counting multiplicities). Then we must have $a \mid b$ or $a \mid c$. Hence a is a prime element.

" $\impliedby$ ": Suppose that every irreducible element in R is prime. For $r \in R$, suppose that it has two factorizations into irreducibles:

$$r = q_1 \cdots q_n = p_1 \cdots p_m$$

A We have $p_1 \cdots p_m \in \langle q_1 \rangle$. By hypothesis $\langle q_1 \rangle$ is prime. Then we must have $p_i \in \langle q_1 \rangle$ for some $i \in I$. After possible permutations we may assume that $p_1 \in \langle q_1 \rangle$. Since p_1 is irreducible, we must have $\langle p_1 \rangle = \langle q_1 \rangle$ or $p_1 \sim q_1$. Then $q_2 \cdots q_n \sim p_2 \cdots p_m$. We can repeat this process. If $n \neq m$ then after some steps we will have $1 \sim a$ where a is a product of irreducibles, which is impossible. Hence $n = m$ and $q_i \sim p_i$ for all $i \in \{1, ..., n\}$ after possible permutations. We conclude that R is a UFD.

□

Question 4

Let K be a number field. Prove that $\mathcal{O}_K$ is Euclidean with norm function $\left|\mathrm{Norm}_{K/\mathbb{Q}}\right| : \mathcal{O}_K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ if and only if for each $\alpha \in K$ there exists $\beta \in \mathcal{O}_K$ such that $\left|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha - \beta)\right| < 1$. Verify this condition for $K = \mathbb{Q}(\sqrt{-d})$ where $d = 1, 2, 3, 7$. [Hint: Consider the nearest point on a lattice.

Proof. (*In my own notation, the set of natural numbers $\mathbb{N}$ always contains zero.*)

By Corollary 3.8, $\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathcal{O}_K$. Then $\left|\mathrm{Norm}_{K|\mathbb{Q}}\right| : \mathcal{O}_K \setminus \{0\} \to \mathbb{N}$ is well-defined. Note that $\left|\mathrm{Norm}_{K|\mathbb{Q}}\right|$ is multiplicative and $\left|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha)\right| = 0$ if and only if $\alpha = 0$.

" $\implies$ " Suppose that $\left(\mathcal{O}_K, \left|\mathrm{Norm}_{K|\mathbb{Q}}\right|\right)$ is an Euclidean domain. Let $\alpha \in K$.

A Let $m(x) := x^n + \sum_{i=0}^{n-1} a_i x^i$ be the minimal polynomial of α, where $a_i = p_i / q_i \in \mathbb{Q}$ and $p_i, q_i \in \mathbb{Z}$. Let $d := \mathrm{lcm}(q_0, ..., q_{n-1})$. Then

$$f(x) := d^n m\left(\frac{x}{d}\right)$$

is a monic polynomial with a root $d\alpha$. We deduce that $d\alpha \in \mathcal{O}_K$.

Since $\mathcal{O}_K$ is an ED, and $d \in \mathcal{O}_K \setminus \{0\}$, there exists $\beta, r \in \mathcal{O}_K$ such that $d\alpha = d\beta + r$, with $\left|\mathrm{Norm}_{K|\mathbb{Q}}(r)\right| < \left|\mathrm{Norm}_{K|\mathbb{Q}}(d)\right|$. (In fact $\left|\mathrm{Norm}_{K|\mathbb{Q}}\right|$ is defined on the whole $\mathcal{O}_K$.) Therefore

$$\left|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha - \beta)\right| = \frac{\left|\mathrm{Norm}_{K|\mathbb{Q}}(d\alpha - d\beta)\right|}{\left|\mathrm{Norm}_{K|\mathbb{Q}}(d)\right|} = \frac{\left|\mathrm{Norm}_{K|\mathbb{Q}}(r)\right|}{\left|\mathrm{Norm}_{K|\mathbb{Q}}(d)\right|} < 1$$

" $\impliedby$ ": Suppose that for each $\alpha \in K$ there exists $\beta \in \mathcal{O}_K$ such that $\left|\mathrm{Norm}_{K/\mathbb{Q}}(\alpha - \beta)\right| < 1$.

- For $a \in \mathcal{O}_K$ and $b \in \mathcal{O}_K \setminus \{0\}$, by hypothesis there exists $q \in \mathcal{O}_K$ such that

$$\left|\mathrm{Norm}_{K|\mathbb{Q}}\left(\frac{a}{b} - q\right)\right| < 1$$

If $a = qb$, then we are done. Now suppose that $r := a - qb \neq 0$. Then

$$\frac{\left|\mathrm{Norm}_{K|\mathbb{Q}}(r)\right|}{\left|\mathrm{Norm}_{K|\mathbb{Q}}(b)\right|} = \frac{\left|\mathrm{Norm}_{K|\mathbb{Q}}(a - qb)\right|}{\left|\mathrm{Norm}_{K|\mathbb{Q}}(b)\right|} = \left|\mathrm{Norm}_{K|\mathbb{Q}}\left(\frac{a}{b} - q\right)\right| < 1 \implies \left|\mathrm{Norm}_{K|\mathbb{Q}}(r)\right| < \left|\mathrm{Norm}_{K|\mathbb{Q}}(b)\right|$$

- For $a, b \in \mathcal{O}_K \setminus \{0\}$,
$$\left|\mathrm{Norm}_{K|\mathbb{Q}}(ab)\right| = \left|\mathrm{Norm}_{K|\mathbb{Q}}(a)\right|\left|\mathrm{Norm}_{K|\mathbb{Q}}(b)\right| > \left|\mathrm{Norm}_{K|\mathbb{Q}}(a)\right|$$
because $\left|\mathrm{Norm}_{K|\mathbb{Q}}(b)\right| \neq 0$.

We deduce that $\left(\mathcal{O}_K, \left|\mathrm{Norm}_{K|\mathbb{Q}}\right|\right)$ is an Euclidean domain.

Let $K = \mathbb{Q}\left(\sqrt{-d}\right)$. K has a $\mathbb{Q}$-basis $\left\{1, \sqrt{d}\mathrm{i}\right\}$. The Galois group $\mathrm{Gal}(K \mid \mathbb{Q}) = \left\{\mathrm{id},\ z \mapsto \overline{z}\right\}$. Therefore, for $\alpha = a + b\sqrt{d}\mathrm{i} \in K$ with $a, b \in \mathbb{Q}$, the norm is
$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = \left(a + b\sqrt{d}\mathrm{i}\right)\left(a - b\sqrt{d}\mathrm{i}\right) = a^2 + b^2 d$$

By Example 3.12, $\mathcal{O}_K$ has integral basis
$$\begin{cases} \left\{1, \sqrt{d}\mathrm{i}\right\}, & \text{if } d \equiv 1, 2 \bmod 4; \\ \left\{1, \dfrac{1+\sqrt{d}\mathrm{i}}{2}\right\}, & \text{if } d \equiv 3 \bmod 4. \end{cases}$$

- For $d = 1$ or 2, consider $\alpha = a + b\sqrt{d}\mathrm{i} \in K$. Let $a', b' \in \mathbb{Z}$ such that $|a - a'| \leqslant 1/2$ and $|b - b'| \leqslant 1/2$. We have $\beta := a' + b'\sqrt{d}\mathrm{i} \in \mathcal{O}_K$ and
$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha - \beta) = (a - a')^2 + (b - b')^2 d \leqslant \frac{1+d}{4} < 1$$
which gives the desired β for each α.

- For $d = 3$ or 7, consider $\alpha = a + b\sqrt{d}\mathrm{i} \in K$. We choose $a', b' \in \frac{1}{2}\mathbb{Z}$ as follows:

  First choose $a', b' \in \mathbb{Z}$ such that $|a - a'| \leqslant 1/2$ and $|b - b'| \leqslant 1/2$. If $|b - b'| > 1/4$, we can replace a', b' with $a' + \frac{1}{2}, b' + \frac{1}{2}$ or $a' - \frac{1}{2}, b' - \frac{1}{2}$ such that $|b - b'| \leqslant 1/4$.

  Now we have $\beta := a' + b'\sqrt{d}\mathrm{i} \in \mathcal{O}_K$, and
$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha - \beta) = (a - a')^2 + (b - b')^2 d \leqslant \frac{1}{4} + \frac{d}{16} < 1$$
  which gives the desired β for each α.

We conclude that $\mathcal{O}_K$ is an ED for $d = 1, 2, 3, 7$. □

Question 5

Prove that if p is a prime with $p \equiv 1$ or $3 \bmod 8$, then $p = X^2 + 2Y^2$ for some $X, Y \in \mathbb{Z}$ unique up to sign.

Proof. First we claim that -2 is a quadratic residue of p. From Part A Number Theory we know that
$$\left(\frac{-1}{p}\right) = 1 \text{ if and only if } p \equiv 1 \bmod 4, \qquad \left(\frac{2}{p}\right) = 1 \text{ if and only if } p \equiv \pm 1 \bmod 8$$

Hence
$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} -1 \cdot (-1) = 1 & p \equiv 1 \bmod 8 \\ 1 \cdot 1 = 1 & p \equiv 3 \bmod 8 \end{cases}$$
which proves the claim. Hence there exists $r \in \mathbb{Z}$ such that $2r^2 \equiv -2 \bmod p$. That is, $p \mid (1 + 2r^2)$.

$\mathbb{Z}[\sqrt{-2}]$ is the ring of integers in $\mathbb{Q}(\sqrt{-2})$. By Question 4, $\mathbb{Z}[\sqrt{-2}]$ is an Euclidean domain, and hence is a unique factorisation domain, in which $1 + 2r^2 = (1 + \sqrt{2}\mathrm{i})(1 - \sqrt{2}\mathrm{i})$.

Suppose that p is irreducible in $\mathbb{Z}[\sqrt{-2}]$. Then p is prime in $\mathbb{Z}[\sqrt{-2}]$. We have either $p \mid (1 + \sqrt{2}\mathrm{i})$ or $p \mid (1 - \sqrt{2}\mathrm{i})$ in $\mathbb{Z}[\sqrt{-2}]$. But this is impossible. as
$$\mathbb{Z}[\sqrt{-2}] = \left\{a + b\sqrt{2}\mathrm{i} :\ a, b \in \mathbb{Z}\right\}$$

Hence there exists non-units $a + b\sqrt{2}\mathrm{i}, c + d\sqrt{2}\mathrm{i} \in \mathbb{Z}[\sqrt{-2}]$ such that $p = (a + b\sqrt{2}\mathrm{i})(c + d\sqrt{2}\mathrm{i})$. Taking the norm:
$$p^2 = (a^2 + 2b^2)(c^2 + 2d^2)$$

Since neither $a^2 + 2b^2$ nor $c^2 + 2d^2$ is not 1, we deduce that $p = a^2 + 2b^2 = c^2 + 2d^2$ as required.

A

Next we shall prove the uniqueness of X, Y in the expression.

If $X + Y\sqrt{2}\mathrm{i} = \alpha\beta$ in $\mathbb{Z}[\sqrt{-2}]$, then taking the norm we have

$$p = X^2 + 2Y^2 = \mathrm{Norm}(\alpha)\,\mathrm{Norm}(\beta)$$

Then either α or β is a unit in $\mathbb{Z}[\sqrt{-2}]$. Hence $X + Y\sqrt{2}\mathrm{i}$ is irreducible in $\mathbb{Z}[\sqrt{-2}]$. Similarly $X - Y\sqrt{2}\mathrm{i}$ is also irreducible in $\mathbb{Z}[\sqrt{-2}]$.

Now suppose that $p = X'^2 + 2Y'^2$ for some $X', Y' \in \mathbb{Z}$. Then

$$p = \left(X + Y\sqrt{2}\mathrm{i}\right)\left(X - Y\sqrt{2}\mathrm{i}\right) = \left(X' + Y'\sqrt{2}\mathrm{i}\right)\left(X' - Y'\sqrt{2}\mathrm{i}\right)$$

Since $\mathbb{Z}[\sqrt{-2}]$ is a UFD, the two factorisation of p are equal up to permutation and associates. But we also know that the only units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1. We conclude that $X^2 = X'^2$ and $Y^2 = Y'^2$, so that the expression for p is unique. □

Question 6

Show that $\mathbb{Z}[\sqrt{3}]$ is Euclidean. Write down the factorisations into irreducibles of 2,3 and 11. Show using congruences modulo 3 and 4 that the elements 5 and 7 are irreducible in $\mathbb{Z}[\sqrt{3}]$.

Proof. Let $K = \mathbb{Q}(\sqrt{3})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. The Galois group $\mathrm{Gal}(K \mid \mathbb{Q}) = \{\mathrm{id},\ a + b\sqrt{3} \mapsto a - b\sqrt{3}\}$. Hence for $\alpha = a + b\sqrt{3}$,

$$\mathrm{Norm}_{K|\mathbb{Q}}(\alpha) = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$$

We can choose $a', b' \in \mathbb{Z}$ such that $|a - a'| \leqslant 1/2$ and $|b - b'| \leqslant 1/2$. Then $\beta := a' + b'\sqrt{3} \in \mathcal{O}_K$, and

$$\left|\mathrm{Norm}_{K|\mathbb{Q}}(\alpha - \beta)\right| = \left|(a - a')^2 - 3(b - b')^2\right| \leqslant \frac{3}{4}$$

By Question 4, we deduce that $\mathbb{Z}[\sqrt{3}]$ is an Euclidean domain.

The factorisation of $2, 3, 11$ in $\mathbb{Z}[\sqrt{3}]$:

A

$$2 = (1 + \sqrt{3})(-1 + \sqrt{3}), \qquad 3 = \sqrt{3} \cdot \sqrt{3}, \qquad 11 = (1 + 2\sqrt{3})(-1 + 2\sqrt{3})$$

The norms of the factors are $-2, -3, -11$ respectively. These are primes in $\mathbb{Z}$. Hence the factors are irreducibles in $\mathbb{Z}[\sqrt{3}]$.

Suppose that 5 is reducible in $\mathbb{Z}[\sqrt{3}]$. There exists non-units $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ such that $5 = (a + b\sqrt{3})(c + d\sqrt{3})$. Taking the norm:

$$25 = \left|a^2 - 3b^2\right|\left|c^2 - 3d^2\right|$$

By unique factorisation in $\mathbb{Z}$, $a^2 - 3b^2 = \pm 5$ and $c^2 - 3d^2 = \pm 5$. Note that the only quadratic residue of 3 is 1. Using congruences modulo 3,

$$a^2 - 3b^2 \equiv 1 - 3 \cdot 1 \equiv 1 \bmod 3$$

Hence $a^2 - 3b^2 = -5$. Note that the quadratic residue of 4 are 0 and 1. Then using congruences modulo 4,

$$a^2 - 3b^2 \equiv a^2 + b^2 \equiv 3 \bmod 4$$

But this is impossible, as $a^2, b^2 \equiv 0$ or $1 \bmod 4$. We deduce that 5 is irreducible in $\mathbb{Z}[\sqrt{3}]$.

Suppose that 7 is reducible in $\mathbb{Z}[\sqrt{3}]$. There exists non-units $a + b\sqrt{3}, c + d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ such that $7 = (a + b\sqrt{3})(c + d\sqrt{3})$. Taking the norm:

$$49 = \left|a^2 - 3b^2\right|\left|c^2 - 3d^2\right|$$

By unique factorisation in $\mathbb{Z}$, $a^2 - 3b^2 = \pm 7$ and $c^2 - 3d^2 = \pm 7$. Using congruences modulo 3, we have $a^2 - 3b^2 = 7$. Using congruences modulo 4,

$$a^2 - 3b^2 \equiv a^2 + b^2 \equiv 3 \bmod 4$$

This is impossible. We deduce that 7 is irreducible in $\mathbb{Z}[\sqrt{3}]$. □

Question 7

Show that $X^2 - 10Y^2 = \pm 2$ is insoluble in integers. Deduce that if α divides both 2 and $\sqrt{10}$ in $\mathbb{Z}[\sqrt{10}]$, then α is a unit. Show however that one cannot write $\alpha = 2\beta + \sqrt{10}\gamma$ with $\beta, \gamma \in \mathbb{Z}[\sqrt{10}]$.

Proof. Suppose that there exists $X, Y \in \mathbb{Z}$ such that $X^2 - 10Y^2 = \pm 2$. Using congruences modulo 5, we have

$$X^2 \equiv 2, 3 \bmod 5$$

But this is impossible, as the only quadratic residues of 5 are 1 and 4. We deduce that $X^2 - 10Y^2 = \pm 2$ is insolvable by integers.

Suppose that $\varphi, \psi \in \mathbb{Z}[\sqrt{10}]$ such that $\alpha\varphi = 2$ and $\alpha\psi = \sqrt{10}$. Taking the norm:

$$\mathrm{Norm}(\alpha)\,\mathrm{Norm}(\varphi) = 4, \qquad \mathrm{Norm}(\alpha)\,\mathrm{Norm}(\psi) = -10$$

A

Therefore $\mathrm{Norm}(\alpha)$ divides $\gcd(4, -10) = 2$ in $\mathbb{Z}$. Hence $\mathrm{Norm}(\alpha) = \pm 1$ or ± 2. Write $\alpha = X + Y\sqrt{10}$. The previous part shows that $\mathrm{Norm}(\alpha) = X^2 - 10Y^2 \neq \pm 2$. Hence $\mathrm{Norm}(\alpha) = \pm 1$ and α is a unit in $\mathbb{Z}[\sqrt{10}]$.

Suppose that $\alpha = 2\beta + \sqrt{10}\gamma$, where $\beta = a + b\sqrt{10}, \gamma = c + d\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ and $a, b, c, d \in \mathbb{Z}$. Then

$$\alpha = 2(a + b\sqrt{10}) + \sqrt{10}(c + d\sqrt{10}) = (2a + 10d) + (2b + c)\sqrt{10} \implies \mathrm{Norm}(\alpha) = (2a + 10d)^2 - 10(2b + c)^2 \equiv 0 \bmod 2$$

contradicting that $\mathrm{Norm}(\alpha) = \pm 1$. Hence $\alpha \neq 2\beta + \sqrt{10}\gamma$ for all $\beta, \gamma \in \mathbb{Z}[\sqrt{10}]$. □

Question 8

Let K be a number field and let A, B, C, I be ideals of $\mathcal{O}_K$ Recall that A, B are said to be coprime if $A + B = \mathcal{O}_K$. Show that if A, B are coprime and $A \mid BC$ then $A \mid C$. Show that if A, B are coprime and $A|I, B|I$ then $AB \mid I$.

Proof. Proposition 6.23 shows that, for any ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$, $\mathfrak{a} \mid \mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

Since $A + B = \mathcal{O}_K$, there exists $a \in A$ and $b \in B$ such that $a + b = 1$.

Suppose that $A \mid BC$ and $A \nmid C$. Then $BC \subseteq A$ and $C \nsubseteq A$. Pick $c \in C \setminus A$. Then $bc \in BC \subseteq A$. Hence $c = ac + bc \in A$, which is a contradiction. Hence $A \mid C$.

Suppose that $A \mid I$, $B \mid I$ and $AB \nmid I$. Then $I \subseteq A \cap B$ and $I \nsubseteq AB$. This is impossible because $A \cap B \subseteq AB$. (For $r \in A \cap B$, $r = ar + br \in AB$.) □

A