MATH7421 Problems Week 3

Rings of Integers

1. Show that every algebraic number α can be written as $\alpha = \frac{1}{d}\beta$ for some $d \in \mathbb{Z}$ and β an algebraic integer. Hence prove that every number field K is of the form $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$.

   (Hint: By Exercise 3 of Week 2 we know that $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$).

2. (a) Compute the ring of integers of the number field $K = \mathbb{Q}(\sqrt{2})$

   (b) Compute the ring of integers of the number field $K = \mathbb{Q}(\sqrt{-3})$

3. In this question we'll show that the ring of integers of the number field $K = \mathbb{Q}(\sqrt[3]{2})$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$.

   (a) Show that $\mathbb{Z}[\sqrt[3]{2}] \subseteq \mathcal{O}_K$.

   Now let $\alpha = a + b\sqrt[2]{3} + c\sqrt[2]{3}^2 \in \mathcal{O}_K$ with $a, b, c \in \mathbb{Q}$. We'll show that $a, b, c \in \mathbb{Z}$ so that $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt[3]{2}]$.

   (b) Let $\sigma_1, \sigma_2, \sigma_3 : K \hookrightarrow \mathbb{C}$ be the complex embeddings of K. Calculate $\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha)$ and show that:

   $$\begin{aligned} \sigma_1(\alpha) + \sigma_2(\alpha) + \sigma_3(\alpha) &= 3a \\ \sigma_1(\alpha)\sigma_2(\alpha) + \sigma_1(\alpha)\sigma_3(\alpha) + \sigma_2(\alpha)\sigma_3(\alpha) &= 3a^2 - 6bc \\ \sigma_1(\alpha)\sigma_2(\alpha)\sigma_3(\alpha) &= a^3 + 2b^3 + 4c^3 - 6abc \end{aligned}$$

   are all in $\mathbb{Z}$.

   (c) Let $A = 3a, B = 3b, C = 3c$. Show that $A^2 - 2BC \equiv 0 \bmod 3$ and $A^3 + 2B^3 + 4C^3 - 6ABC \equiv 0 \bmod 27$.

   (d) Deduce that $A, B, C \in \mathbb{Z}$.

   (e) Show via contradiction that we must have that $3|A$. (Hint: Show that the congruences have no solutions if $3 \nmid A$).

   (f) Hence show that $3|B$ and $3|C$ too, so that $a, b, c \in \mathbb{Z}$.

4. For a challenge, let's compute the ring of integers of a more complicated number field. Let $\zeta = e^{\frac{2\pi i}{5}}$, i.e. a primitive 5th root of unity.

   (a) Show that ζ is an algebraic integer, that $\mathbb{Q}(\zeta) = \{a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$ and that the conjugates of ζ are ζ^i for $1 \leq i \leq 4$.
   (Hint: Exercise 6 of Week 1 might be useful).

   (b) Show that
$$T(\zeta^i) = \begin{cases} 4 & \text{if } i = 0 \\ -1 & \text{if } i = 1, 2, 3, 4 \end{cases}$$

We claim that the ring of integers of the number field $K = \mathbb{Q}(\zeta)$ is
$$\mathcal{O}_K = \mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}\}.$$

Let's take an arbitrary $\alpha = a_0+a_1\zeta+a_2\zeta^2+a_3\zeta^3 \in \mathcal{O}_K$ and try to show that $a_0, a_1, a_2, a_3 \in \mathbb{Z}$.

   (c) Use part (b) to calculate the values $T(\alpha), T(\alpha\zeta), T(\alpha\zeta^2), T(\alpha\zeta^3), T(\alpha\zeta^4)$. Why must these values be integers, and why does it then follow that $5a_i \in \mathbb{Z}$ for each i?

Now consider $5\alpha = b_0 + b_1\zeta + b_2\zeta^2 + b_3\zeta^3$, with $b_i = 5a_i \in \mathbb{Z}$. Our aim is to show that $5|b_i$ for each i, so that $\alpha \in \mathbb{Z}[\zeta]$ (showing that $\mathcal{O}_K \subseteq \mathbb{Z}[\zeta]$). To do this, we'll need the special element $\lambda = 1 - \zeta \in \mathbb{Q}(\zeta)$.

   (d) Show that if $5\alpha = c_0 + c_1\lambda + c_2\lambda^2 + c_3\lambda^3$ then:
$$\begin{aligned} c_0 &= b_0 + b_1 + b_2 + b_3 \\ c_1 &= -b_1 - 2b_2 - 3b_3 \\ c_2 &= b_2 + 3b_3 \\ c_3 &= -b_3 \end{aligned}$$
   so that $c_0, c_1, c_2, c_3 \in \mathbb{Z}$.

   (e) Show that $N(\lambda) = 5$ and hence that $\lambda^4|5$ in $\mathbb{Z}[\zeta]$.

   (f) Show that $5|c_i$ for each i and that this implies that $5|b_i$ for each i. This finishes the proof that $\alpha \in \mathbb{Z}[\zeta]$.

We've now shown that $\mathcal{O}_K \subseteq \mathbb{Z}[\zeta]$.

   (g) Finish the proof by showing that $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$.
   (Hint: Use part (a)).

5. You should complete Exercise 8(a) of Week 2 before attempting this one. Let $\mathbb{Q}(\alpha)$ be a number field of degree d and let $\beta_1, \beta_2, ..., \beta_d \in \mathcal{O}_K$ be a basis for K. Show that $\Delta(\beta_1, \beta_2, ..., \beta_d) \in \mathbb{Z}\backslash\{0\}$.

6. Suppose that $K = \mathbb{Q}(\alpha)$ has degree d and that there exist $\beta_1, \beta_2, ..., \beta_d \in \mathcal{O}_K$ such that $|\Delta(\beta_1, \beta_2, ..., \beta_d)| \geq 1$ is square-free. Show that $\mathcal{O}_K = \{a_1\beta_1+a_2\beta_2+...a_d\beta_d \mid a_1, a_2, ..., a_d \in \mathbb{Z}\}$.
(Hint: Go back to the proof that $\mathcal{O}_K$ has a $\mathbb{Z}$-basis. How were the values D and D' related?)

Rings, Ideals and Factorisation

7. (a) Show that every field is an integral domain.
   (b) Show that the ring of integers $\mathcal{O}_K$ of a number field K is an integral domain.
   (c) Is the ring $\mathbb{Z}/30\mathbb{Z}$ an integral domain?
   (d) Show that the polynomial ring $R[x_1, x_2, ..., x_n]$ over an integral domain R is also an integral domain. (Hint: Use induction)

8. Let R be a commutative ring. Show that $R^\times$ is an abelian group under multiplication.

9. Let R be a commutative ring and $x, y \in R$. Show the following properties of principal ideals:
   (a) $\langle x \rangle$ is an ideal of R.
   (b) $\langle x \rangle \subseteq \langle y \rangle$ if and only if $y|x$.
   (c) If further R is an integral domain then $\langle x \rangle = \langle y \rangle$ if and only $x = uy$ for some unit $u \in R^\times$.

10. Let R be a commutative ring and $\beta_1, \beta_2, ..., \beta_n \in R$. Show that

$$\langle \beta_1, \beta_2, ..., \beta_n \rangle = \{a_1\beta_1 + a_2\beta_2 + ... + a_n\beta_n \mid a_1, a_2, ..., a_n \in R\}$$

is an ideal of R.

11. Let R be an integral domain. Show that the following are equivalent, as claimed in the notes:
    - R is Noetherian, i.e. every non-empty collection of ideals of R has a maximal element (under inclusion).
    - Every ideal of R is finitely generated.
    - Every infinite sequence of ideals $I_1, I_2, I_3...$ of R such that:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$$

      eventually stabilises, i.e. at some point we have $I_n = I_{n+1} = I_{n+2} = ...$

    (Hint: Show that the third condition holds if and only if the first holds. Then show that the third condition holds if and only if the second holds).

12. Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Show that if $I \subseteq \mathcal{O}_K$ is a non-zero ideal then the quotient ring $\mathcal{O}_K/I$ is finite.

    (Hint: Pick some non-zero $\alpha \in I$ and show that $N(\alpha) \in I$.)