MATH7421 Solutions Week 3

Rings of Integers

1. Suppose that α is an algebraic number with minimal polynomial

$$m_\alpha(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Q}[x].$$

Let d be the lowest common multiple of all of the denominators of the a_i. Then:

$$d^n(\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0) = (d\alpha)^n + da_{n-1}(d\alpha)^{n-1} + ... + d^{n-1}a_1(d\alpha) + d^n a_0 = 0,$$

so that $\beta = d\alpha$ is a root of the monic polynomial $x^n + da_{n-1} + ... + d^{n-1}a_1 + d^n a_0 \in \mathbb{Z}[x]$. It follows that β is an algebraic integer, hence $\alpha = \frac{1}{d}\beta$ for some algebraic integer β.

2. (a) If $\beta = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ then $m_\beta(x) = x^2 - 2ax + (a^2 - 2b^2)$. For this to be in $\mathbb{Z}[x]$ we would require:

$$2a \in \mathbb{Z} \qquad \text{and} \qquad (a^2 - 2b^2) \in \mathbb{Z}.$$

The first inclusion tells us that $a \in \frac{1}{2}\mathbb{Z}$ and the second then tells us that $2b^2 \in \frac{1}{4}\mathbb{Z}$, so that $b^2 \in \frac{1}{8}\mathbb{Z}$, hence $b \in \frac{1}{2}\mathbb{Z}$ (if b had denominator 4 then b^2 would have denominator 16, which is too big).

Let $a = \frac{c}{2}$ and $b = \frac{d}{2}$ with $c, d \in \mathbb{Z}$. Then the second inclusion gives $c^2 - 2d^2 \in 4\mathbb{Z}$, so that $c^2 - 2d^2 \equiv 0 \bmod 4$. The only solution to this congruence is $c \equiv d \equiv 0 \bmod 2$ (since c must be even and $c^2 - 2d^2 \equiv 2d^2 \equiv 0 \bmod 4$ implies that d is also even). This means that $a, b \in \mathbb{Z}$ so that $\mathcal{O}_K \subseteq \mathbb{Z}[i]$.

It's clear that every element of $\mathbb{Z}[\sqrt{2}]$ satisfies the two inclusions, hence $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$.

(b) If $\beta = a + b\sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$ then $m_\beta(x) = x^2 - 2ax + (a^2 + 3b^2)$. For this to be in $\mathbb{Z}[x]$ we would require:

$$2a \in \mathbb{Z} \qquad \text{and} \qquad (a^2 + 3b^2) \in \mathbb{Z}.$$

The first inclusion tells us that $a \in \frac{1}{2}\mathbb{Z}$ and the second then tells us that $3b^2 \in \frac{1}{4}\mathbb{Z}$, so that $b^2 \in \frac{1}{12}\mathbb{Z}$, hence $b \in \frac{1}{2}\mathbb{Z}$ (we cannot have 3 dividing the denominator since otherwise 9 would divide the denominator of b^2, which is too big).

Let $a = \frac{c}{2}$ and $b = \frac{d}{2}$ with $c, d \in \mathbb{Z}$. Then the second inclusion gives $c^2 + 3d^2 \in 4\mathbb{Z}$, so that $c^2 + 3d^2 \equiv 0 \bmod 4$. This implies that either c, d are both even or both odd, so that $a, b \in \mathbb{Z}$ or $a, b \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$.

It follows that $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{-3}] \cup \left\{ \frac{a+b\sqrt{-3}}{2} \mid a, b \text{ odd} \right\}$. Note that if a, b are odd then $\frac{a+b\sqrt{-3}}{2} = \frac{(a-b)+b+b\sqrt{-3}}{2} = \frac{(a-b)}{2} + b\left(\frac{1+\sqrt{-3}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Also $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$,

since if $a, b \in \mathbb{Z}$ then $a + b\sqrt{-3} = (a - b) + 2b\left(\frac{1+\sqrt{-3}}{2}\right)$. Conversely, if $a + b\left(\frac{1+\sqrt{-3}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ then either b is even (in which case the element lies in $\mathbb{Z}[\sqrt{-3}]$) or b is odd (in which case the element lies in $\left\{\frac{a+b\sqrt{-3}}{2} \mid a, b \text{ odd}\right\}$. This now implies that $\mathcal{O}_K \subseteq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

To show the reverse inclusion, let $a+b\left(\frac{1+\sqrt{-3}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Then this element can be shown to be a root of the monic integer polynomial $x^2-(2a+b)x+(a^2+ab+b^2) \in \mathbb{Z}[x]$, hence $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

3. (a) We know that $\sqrt[3]{2} \in K$ is an algebraic integer since it is a root of $x^3 - 2$. Hence $\mathbb{Z}[\sqrt[3]{2}] \subseteq \mathcal{O}_K$, since $\mathcal{O}_K$ is a ring.

   (b) We know that the conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$, where $\zeta = e^{\frac{2\pi}{3}} = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity. The three embeddings are defined as follows:

$$\begin{aligned}\sigma_1(\alpha) &= a + b\sqrt[3]{3} + c\sqrt[3]{3}\\ \sigma_2(\alpha) &= a + b\zeta\sqrt[3]{3} + c\zeta^2\sqrt[3]{3}\\ \sigma_3(\alpha) &= a + b\zeta^2\sqrt[3]{3} + c\zeta\sqrt[3]{3}\end{aligned}$$

   Computing the three quantities of interest and using the relation $\zeta^2 + \zeta + 1 = 0$ reveals:

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

   These quantities lie in $\mathbb{Q}$ and are algebraic integers (since α is an algebraic integer by assumption and $\sigma_i(\alpha)$ is a root of $m_\alpha(x)$). Hence they lie in $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

   (c) A simple substitution gives:

$$\begin{aligned}A^2 - 2BC &= (3a)^2 - 2(3b)(3c)\\ &= 3(3a^2 - 6bc) \in 3\mathbb{Z}\\ A^3 + 2B^3 + 4C^3 - 6ABC &= (3a)^3 + 2(3b)^3 + 4(3c)^3 - 6(3a)(3b)(3c)\\ &= 27(a^3 + 2b^3 + 4c^3 - 6abc) \in 27\mathbb{Z}\end{aligned}$$

   (d) We know that $A = 3a \in \mathbb{Z}$ since $\sigma_1(\alpha) + \sigma_2(\alpha) + \sigma_3(\alpha) \in \mathbb{Z}$.

   We also know that $A^2 - 2BC \in \mathbb{Z}$, so that $2BC \in \mathbb{Z}$.

   Finally, we know that $A^3 + 2B^3 + 4C^3 - 6ABC \in \mathbb{Z}$, so that $2(B^3 + 2C^3) \in \mathbb{Z}$.

   Let $B = \frac{r}{s}$ and $C = \frac{t}{u}$ be such that $\gcd(r, s) = \gcd(t, u) = 1$. Then $2BC = \frac{2rt}{su}$ and $2(B^3 + 2C^3) = 2\left(\frac{r^3}{s^3} + \frac{2t^3}{u^3}\right) = \frac{2((ru)^3+2(st)^3)}{(su)^3}$.

   If there exists a prime $p|s$ then since $2(B^3+C^3) \in \mathbb{Z}$ we would require $p^3|2((ru)^3+2(st)^3)$, so that $p^3|2(ru)^3$. Since $p \nmid r$ we would have $p^3|2u^3$. This would require $p|u$, which would contradict the fact that $2BC \in \mathbb{Z}$ (since this would have denominator divisible by p^2).

   If there exists a prime $p|u$ then a similar argument gives $p^3|4s^3$, so that $p|s$, again contradicting the fact that $2BC \in \mathbb{Z}$.

(e) If $3 \nmid A$ then $A \equiv 1, 2 \bmod 3$. The only solutions to:

$$A^2 - 2BC \equiv 0 \bmod 3$$
$$A^3 + 2B^3 + 4C^3 - 6ABC \equiv 0 \bmod 3$$

are $(A, B, C) \equiv (1, 2, 1) \bmod 3$ or $(2, 1, 2) \bmod 3$.

In the first case we let $(A, B, C) = (1 + 3k, 2 + 3l, 1 + 3m)$ for some $k, l, m \in \mathbb{Z}$ and note that:

$$\begin{aligned} A^3 + 2B^3 + 4C^3 - 6ABC &= (1 + 3k)^3 + 2(2 + 3l)^3 + 4(1 + 3m)^3 \\ &\quad - 6(1 + 3k)(2 + 3l)(1 + 3m) \\ &= (1 + 9k + 27k^2 + 27k^3) + 2(8 + 18l + 54l^2 + 27l^3) \\ &\quad + 4(1 + 9m + 27m^2 + 27m^3) \\ &\quad - 6(2 + 6m + 3l + 6k + 9lm + 18km + 9kl + 27klm) \\ &= 9 - 27k - 18l + 27k^2 + 108l^2 + 108m^2 + 9lm + 18km \\ &\quad + 9kl + 27k^3 + 27l^3 + 27m^3 - 162klm \\ &\equiv 9 \bmod 27. \end{aligned}$$

In the second case we let $(A, B, C) = (2 + 3k, 1 + 3l, 2 + 3m)$ for some $k, l, m \in \mathbb{Z}$. A similar calculation once again shows that $A^3 + 2B^3 + 4C^3 - 6ABC \equiv 9 \bmod 27$. It follows that we must have $3 \nmid A$.

(f) Since $3|A$ and $A^2 - 2BC \equiv 0 \bmod 3$ we must have that $2BC \equiv 0 \bmod 3$, so that $B \equiv 0 \bmod 3$ or $C \equiv 0 \bmod 3$. In either case, the congruence $A^3 + 2B^3 + 4C^3 - 6ABC \equiv 0 \bmod 3$ would then imply that all three are divisible by 3.

4. (a) Note that ζ is a root of $x^5 - 1$ and so is an algebraic integer. However, this isn't the minimal polynomial since it is reducible. The minimal polynomial is $m_\zeta(x) = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$ (which is irreducible since $m_\zeta(x + 1) = x^4 + 5x^3 + 10x^2 + 10x + 5$ and we can use Eisenstein's Criterion with $p = 5$).

It follows that the degree of $\mathbb{Q}(\zeta)$ is 4 and that $\mathbb{Q}(\zeta) = \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$.

Note that $\zeta, \zeta^2, \zeta^3, \zeta^4$ all satisfy $x^5 - 1$ and are not equal to 1, hence are the roots of $x^4 + x^3 + x^2 + x + 1$. It follows that the conjugates of ζ are ζ^i for $i = 1, 2, 3, 4$.

(b) We have that $T(\zeta^0) = T(1) = 4$, since the degree of $\mathbb{Q}(\zeta)$ is 4.

Since the conjugates of ζ are $\zeta, \zeta^2, \zeta^3, \zeta^4$ we have the following for $1 \leq i \leq 4$:

$$T(\zeta^i) = \zeta^i + \zeta^{2i} + \zeta^{3i} + \zeta^{4i}.$$

Since $\zeta^5 = 1$ the value of ζ^{ki} depends only on the value of $ki \bmod 5$. Note that the integers $i, 2i, 3i, 4i$ are all distinct and non-zero mod 5 (since $5 \nmid i$) and so $\zeta^i, \zeta^{2i}, \zeta^{3i}, \zeta^{4i}$ are equal to $\zeta, \zeta^2, \zeta^3, \zeta^4$ in some order.

It follows that $T(\zeta^i) = \zeta + \zeta^2 + \zeta^3 + \zeta^4$. We know that $m_\zeta(\zeta) = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$, so $T(\zeta^i) = -1$.

(c) We have that:

$$\begin{aligned}
T(\alpha) &= T(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3) \\
&= a_0T(1) + a_1T(\zeta) + a_2T(\zeta^2) + a_3T(\zeta^3) \\
&= 4a_0 - a_1 - a_2 - a_3 \\
T(\alpha\zeta) &= T(a_0\zeta + a_1\zeta^2 + a_2\zeta^3 + a_3\zeta^4) \\
&= a_0T(\zeta) + a_1T(\zeta^2) + a_2T(\zeta^3) + a_3T(\zeta^4) \\
&= -a_0 - a_1 - a_2 - a_3 \\
T(\alpha\zeta^2) &= T(a_0\zeta^2 + a_1\zeta^3 + a_2\zeta^4 + a_3\zeta^5) \\
&= a_0T(\zeta^2) + a_1T(\zeta^3) + a_2T(\zeta^4) + a_3T(1) \\
&= -a_0 - a_1 - a_2 + 4a_3 \\
T(\alpha\zeta^3) &= T(a_0\zeta^3 + a_1\zeta^4 + a_2\zeta^5 + a_3\zeta^6) \\
&= a_0T(\zeta^3) + a_1T(\zeta^4) + a_2T(1) + a_3T(\zeta) \\
&= -a_0 - a_1 + 4a_2 - a_3 \\
T(\alpha\zeta^4) &= T(a_0\zeta^4 + a_1\zeta^5 + a_2\zeta^6 + a_3\zeta^7) \\
&= a_0T(\zeta^4) + a_1T(1) + a_2T(\zeta) + a_3T(\zeta^2) \\
&= -a_0 + 4a_1 - a_2 - a_3
\end{aligned}$$

Since $\zeta \in \mathcal{O}_K$ and $\alpha \in \mathcal{O}_K$ we know that $\alpha\zeta^i \in \mathcal{O}_K$ for each i. It follows that $T(\alpha\zeta^i) \in \mathbb{Z}$ for each i. Subtracting equation two from the others then gives $5a_i \in \mathbb{Z}$ for each i.

(d) Expanding gives:

$$\begin{aligned}
5\alpha &= c_0 + c_1(1-\zeta) + c_2(1-\zeta)^2 + c_3(1-\zeta)^3 \\
&= (c_0 + c_1 + c_2 + c_3) - (c_1 + 2c_2 + 3c_3)\zeta + (c_2 + 3c_3)\zeta^2 - c_3\zeta^3.
\end{aligned}$$

Comparing coefficients with $5\alpha = b_0 + b_1\zeta + b_2\zeta^2 + b_3\zeta^3$ gives:

$$\begin{aligned}
b_0 &= c_0 + c_1 + c_2 + c_3 \\
b_1 &= -c_1 - 2c_2 - 3c_3 \\
b_2 &= c_2 + 3c_3 \\
b_3 &= -c_3
\end{aligned}$$

Solving this system of equations gives:

$$\begin{aligned}
c_0 &= b_0 + b_1 + b_2 + b_3 \\
c_1 &= -b_1 - 2b_2 - 3b_3 \\
c_2 &= b_2 + 3b_3 \\
c_3 &= -b_3
\end{aligned}$$

Since $b_0, b_1, b_2, b_3 \in \mathbb{Z}$ we find that $c_0, c_1, c_2, c_3 \in \mathbb{Z}$.

(e) We have that $N(\lambda) = (1-\zeta)(1-\zeta^2)(1-\zeta^3)(1-\zeta^4)$. Note that $m_\zeta(x) = x^4 + x^3 + x^2 + x + 1 = (x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)$, so that $N(\lambda) = m_\zeta(1) = 5$.

Note also that if $i \geq 2$ then $(1-\zeta^i) = (1-\zeta)(1+\zeta+\zeta^2+...+\zeta^{i-1})$, so that $\lambda|(1-\zeta^i)$ for each i. It follows that $\lambda^4|N(\lambda) = 5$.

(f) We have that $\lambda | 5\alpha = c_0 + c_1\lambda + c_2\lambda^2 + c_3\lambda^3$. This implies that $\lambda | c_0$, and taking norms gives $5|c_0^4$, so that $5|c_0^4$ (since $c_0 \in \mathbb{Z}$ and 5 is prime in $\mathbb{Z}$).

Thus $5\alpha = 5d_0 + c_1\lambda + c_2\lambda^2 + c_3\lambda^3$ for some $d_0 \in \mathbb{Z}$. We have that $\lambda^2|5$, so that $\lambda|c_1$. Again, taking norms gives $5|c_1$.

Thus $5\alpha = 5d_0 + 5d_1\lambda + c_2\lambda^2 + c_3\lambda^3$ for some $d_1 \in \mathbb{Z}$. We have that $\lambda^3|5$, so that $\lambda|c_2$. Again, taking norms gives $5|c_2$.

Thus $5\alpha = 5d_0 + 5d_1\lambda + 5d_2\lambda^2 + c_3\lambda^3$ for some $d_2 \in \mathbb{Z}$. We have that $\lambda^4|5$, so that $\lambda|c_3$. Again, taking norms gives $5|c_3$.

Now that we know that $5|c_i$ for each i, the equations:

$$\begin{aligned} b_0 &= c_0 + c_1 + c_2 + c_3 \\ b_1 &= -c_1 - 2c_2 - 3c_3 \\ b_2 &= c_2 + 3c_3 \\ b_3 &= -c_3 \end{aligned}$$

show that $5|b_i$ for each i.

(g) Since $\zeta \in \mathcal{O}_K$ and $\mathcal{O}_K$ is a ring, we must have that $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$.

5. We already know from Exercise 8(a) of Week 2 that $\Delta(\beta_1, \beta_2, ..., \beta_d) \in \mathbb{Q}\backslash\{0\}$ and $\Delta(\beta_1, \beta_2, ..., \beta_d) = \det(T(\beta_i\beta_j))$. We already know that $\Delta(\beta_1, \beta_2, ..., \beta_d) = 0$ and so it suffices to show that this is an integer.

   Since $\mathcal{O}_K$ is a ring we know that $\beta_i\beta_j \in \mathcal{O}_K$ for all i and j. We must then have that $T(\beta_i\beta_j) \in \mathbb{Z}$ (since we proved in the notes that the trace of an element of $\mathcal{O}_K$ lies in $\mathbb{Z}$). It follows that the matrix above has integer entries, which implies that it has integer determinant.

6. We know that $\mathcal{O}_K \supseteq \{a_1\beta_1 + a_2\beta_2 + ...a_d\beta_d \,|\, a_1, a_2, ..., a_d \in \mathbb{Z}\}$, since $\beta_1, \beta_2, ..., \beta_d \in \mathcal{O}_K$ and $\mathbb{Z} \in \mathcal{O}_K$ (also the fact that $\mathcal{O}_K$ is a ring). If the claim is false then there must exist $\alpha = a_1\beta_1 + a_2\beta_2 + ... + a_d\beta_d \in \mathcal{O}_K$ with at least one $a_i \in \mathbb{Q}\backslash\mathbb{Z}$. We can reorder the β_i so that $a_1 \in \mathbb{Q}\backslash\mathbb{Z}$.

   Following the proof that $\mathcal{O}_K$ has a $\mathbb{Z}$-basis given in the notes we let $\beta_1' = (a_1 - \lfloor a_1 \rfloor)\beta_1$ and construct a new basis $\beta_1', \beta_2, ..., \beta_d$ for K, consisting of elements of $\mathcal{O}_K$. By the same computation given in the proof we have that:

$$D' = \Delta(\beta_1', \beta_2, ..., \beta_d) = (a_1 - \lfloor a_1 \rfloor)^2\Delta(\beta_1, \beta_2, ..., \beta_d) = (a_1 - \lfloor a_1 \rfloor)^2 D.$$

   Note that by the previous exercise we have that both $D, D' \in \mathbb{Z}\backslash\{0\}$ and $A = (a_1 - \lfloor a_1 \rfloor) \in \mathbb{Q}\backslash\mathbb{Z}$. The equation above tells us that the denominator of A^2 must divide D (in order for $A^2D = D'$ to be an integer). But D is square-free by assumption, and so there is no prime p such that $p^2|D$. Hence this denominator is ± 1, so that $A \in \mathbb{Z}$. This contradicts the fact that $A \in \mathbb{Q}\backslash\mathbb{Z}$. Hence $\mathcal{O}_K = \{a_1\beta_1 + a_2\beta_2 + ...a_d\beta_d \,|\, a_1, a_2, ..., a_d \in \mathbb{Z}\}$.

7. (a) Suppose that $ab = 0$ for a, b in our field. If $a \neq 0$ then a^{-1} exists and so we have that $b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. If $b \neq 0$ then b^{-1} exists and so we have that $a = (ab)b^{-1} = 0 \cdot b^{-1} = 0$. We find that at least one of a, b must be zero, hence our field is an integral domain.

   (b) Suppose $ab = 0$ with $a, b \in \mathcal{O}_K$. Since $\mathcal{O}_K \subset K$, and K is an integral domain (since it's a field), it follows that at least one of a, b is zero. Hence $\mathcal{O}_K$ is an integral domain.

   (c) No, since $3 \cdot 10 \equiv 0 \bmod 30$ but $3 \not\equiv 0 \bmod 30$ and $10 \not\equiv 0 \bmod 30$.

   (d) We use induction on n. If $n = 1$ then suppose that $f(x)g(x) = 0$ for non-zero $f(x) \in R[x]$ and $g(x) \in R[x]$. We can write:

$$f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_sx^s$$
$$g(x) = b_0 + b_1x + ... + b_{t-1}x^{t-1} + b_tx^t$$

   for some $s, t \geq 0$ and non-zero coefficients $a_s \in R$ and $b_t \in R$. The product is then:

$$f(x)g(x) = a_0b_0 + ... + a_sb_tx^{s+t} = 0.$$

   It follows that $a_sb_t = 0$. However, R is an integral domain and so this implies that at least one of a_s and b_t is zero, which is a contradiction.

   Assume that the result is true for $n = k \geq 1$. We now prove the result for $n = k + 1$. Let $f(x_1, x_2, ..., x_{k+1})g(x_1, x_2, ..., x_{k+1}) = 0$ for non-zero $f(x_1, x_2, ..., x_{k+1}) \in R[x_1, x_2, ..., x_{k+1}]$ and $g(x_1, x_2, ..., x_{k+1}) \in R[x_1, x_2, ..., x_{k+1}]$.

   We may write:

$$f(x_1, x_2, ..., x_{k+1}) = f_0(x_1, x_2, ..., x_k) + f_1(x_1, x_2, ..., x_k)x_{k+1} + ... + f_s(x_1, x_2, ..., x_k)x_{k+1}^s$$
$$g(x_1, x_2, ..., x_{k+1}) = g_0(x_1, x_2, ..., x_k) + g_1(x_1, x_2, ..., x_k)x_{k+1} + ... + g_t(x_1, x_2, ..., x_k)x_{k+1}^t$$

   for some $s, t \geq 0$ and non-zero coefficients $f_s(x_1, x_2, ..., x_k) \in R[x_1, x_2, ..., x_k]$ and $g_t(x_1, x_2, ..., x_k) \in R[x_1, x_2, ..., x_k]$. The product is then:

$$f(x_1, x_2, ..., x_{k+1})g(x_1, x_2, ..., x_{k+1}) = f_0(x_1, x_2, ..., x_k)g_0(x_1, x_2, ..., x_k) + ...$$
$$+ f_s(x_1, x_2, ..., x_k)g_t(x_1, x_2, ..., x_k)x_{k+1}^{s+t} = 0.$$

   It follows that $f_s(x_1, x_2, ..., x_k)g_t(x_1, x_2, ..., x_k) = 0$. However, $R[x_1, x_2, ..., x_k]$ is an integral domain by assumption and so at least one of these polynomials is zero, which is a contradiction. By induction, the claim is true for all $n \geq 1$.

8. Note that if $a \in R^\times$ and $b \in R^\times$ then a^{-1} and b^{-1} exist in $R^\times$. It follows that:

$$(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) = 1$$

   so that $ab \in R^\times$.

Associativity follows from the fact that R is a ring (any counter-example to associativity under multiplication in $R^\times$ would give such a counter-example in R).

The set $R^\times$ has identity element 1, since $1 \cdot r = r \cdot 1 = r$ for every $r \in R^\times$ (and $1 \in R^\times$ since $1 \cdot 1 = 1$).

Every $r \in R^\times$ has an inverse under multiplication by definition, namely r^{-1}.

It follows that $R^\times$ is a group. It is abelian since R is a commutative ring.

9. (a) We first show that $\langle x \rangle$ is an additive subgroup of R. Let $a, b \in \langle x \rangle$. Then $a = cx$ and $b = dx$ for some $c, d \in R$. It follows that $a - b = cx - dx = (c - d)x \in \langle x \rangle$, since $c - d \in R$.

   Now we show closure under multiplication by elements of R. Take $r \in R$. Then $ra = r(cx) = (rc)x \in \langle x \rangle$, since $rc \in R$. This finishes the proof that $\langle x \rangle$ is an ideal of R.

   (b) Suppose that $y|x$. Then $x = ry$ for some $r \in R$. It follows that

$$\langle x \rangle = \{\gamma x \,|\, \gamma \in R\} = \{\gamma(ry) \,|\, \gamma \in R\} = \{(\gamma r)y \,|\, \gamma \in R\} \subseteq \{\gamma' y \,|\, \gamma' \in R\} = \langle y \rangle.$$

   Suppose that $\langle x \rangle \subseteq \langle y \rangle$. Then $x \in \langle y \rangle$, so that $x = ry$ for some $r \in R$. Thus $y|x$.

   (c) If $y|x$ and $x|y$ then by (b) we have that $\langle x \rangle \subseteq \langle y \rangle$ and $\langle y \rangle \subseteq \langle x \rangle$. This implies that $\langle x \rangle = \langle y \rangle$.

   Suppose now that $\langle x \rangle = \langle y \rangle$. Then $y|x$ and $x|y$, which implies that $x = ry$ and $y = sx$ for some $r, s \in R$. It follows that $x = r(sx) = (rs)x$, so that $x(1 - rs) = 0$. Since R is an integral domain we have that $x = 0$ or $rs = 1$. In the first case we have that $x = y = 0$ and so $x = uy$ for **any** unit $u \in R$. In the second case we have that $x = ry$ and $r \in R^\times$, so that once again the two generators differ by a unit. This proves the claim.

10. This is similar to Exercise 9(a). We first show that $\langle \beta_1, \beta_2, ..., \beta_n \rangle$ is an additive subgroup of R. Let $a, \in \langle \beta_1, \beta_2, ..., \beta_n \rangle$. Then $a = c_1\beta_1 + c_2\beta_2 + ... + c_n\beta_n$ and $b = d_1\beta_1 + d_2\beta_2 + ... + d_n\beta_n$ for some coefficients $c_1, c_2, ..., c_n, d_1, d_2, ..., d_n \in R$. It follows that $a - b = (c_1 - d_1)\beta_1 + (c_2 - d_2)\beta_2 + ... + (c_n - d_n)\beta_n \in R$, since $c_i - d_i \in R$ for each i.

    Now we show closure under multiplication by elements of R. Take $r \in R$. Then $ra = r(c_1\beta_1 + c_2\beta_2 + ... + c_n\beta_n) = (rc_1)\beta_1 + (rc_2)\beta_2 + ... + (rc_n)\beta_n \in R$, since $rc_i \in R$ for each i. This finishes the proof that $\langle \beta_1, \beta_2, ..., \beta_n \rangle$ is an ideal of R.

11. **Claim 1:** Condition 1 implies condition 3. Suppose that there exists a chain of ideals

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

    that does not stabilise. Pick any ideal I_{n_1} in the chain. Since the chain doesn't stabilise, there must exist an ideal I_{n_2} for some $n_2 > n_1$ that strictly contains I_{n_1}.

    Again, since the chain doesn't stabilise, there must exist an ideal I_{n_3} for some $n_3 > n_2$ that strictly contains I_{n_2}.

    If we keep doing this then the collection of ideals $\{I_{n_1}, I_{n_2}, ...\}$ is non-empty and has no maximal element under inclusion. This proves the contrapositive of the claim.

Claim 2: Condition 3 implies condition 1. Suppose there exists a non-empty collection of ideals of R with no maximal element (under inclusion). Pick any ideal I_{n_1} from this collection.

Since I_{n_1} is not maximal there must exist an ideal I_{n_2} for some $n_2 > n_1$ such that I_{n_2} strictly contains I_{n_1}.

Since I_{n_2} is not maximal there must exist an ideal I_{n_3} for some $n_3 > n_2$ such that I_{n_3} strictly contains I_{n_2}.

Continuing in this fashion we find a chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ that does not stabilise. This proves the contrapositive of the claim.

Claim 3: Condition 2 implies condition 3. Suppose that there exists a chain of ideals

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

that does not stabilise. Consider the ideal $I = \cup_n I_n$. This is finitely generated by assumption, so that $I = \langle a_1, a_2, ..., a_m \rangle$ with each $a_i \in R$.

We know that each element a_i must lie in I_{n_i} for some index $n_i \geq 1$. It follows that $\langle a_1, a_2, ..., a_m \rangle \subseteq I_n$ where $n = \max(n_1, n_2, ..., n_m)$. This implies that $I_n = I_{n+1} = I_{n+2} = ...$, contradicting the assumption that the chain of ideals doesn't stabilise.

Claim 4: Condition 3 implies condition 2. Suppose that there exists an ideal I which is not finitely generated. Pick $a_1 \in I$. Since $\langle a_1 \rangle \subseteq I$ is not equal to I, there must exist $a_2 \in I \backslash \langle a_1 \rangle$.

Since $\langle a_1, a_2 \rangle \subseteq I$ cannot equal I, there must exist $a_3 \in I \backslash \langle a_1, a_2 \rangle$.

Since $\langle a_1, a_2, a_3 \rangle \subseteq I$ cannot equal I, there must exist $a_4 \in I \backslash \langle a_1, a_2, a_3 \rangle$.

Continuing in this fashion we make a chain of ideals:

$$\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_3 \rangle \subseteq \langle a_1, a_2, a_3, a_4 \rangle \subseteq ...$$

since we're assuming that every chain of ideals stabilises, we must have that $\langle a_1, a_2, ..., a_n \rangle = \langle a_1, a_2, ..., a_{n+k} \rangle$ for some $n, k \geq 1$. This contradicts the fact that $a_{n+1} \notin \langle a_1, a_2, ..., a_n \rangle$.

12. Pick some non-zero $\alpha \in I$ and label the embeddings $K \hookrightarrow \mathbb{C}$ by $\sigma_1, \sigma_2, ..., \sigma_d$. Then $N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)...\sigma_d(\alpha) \in \mathbb{Z} \backslash \{0\}$, since $\alpha \in I \subseteq \mathcal{O}_K$ is non-zero. We know that at least one term in this product is α, and we may reorder the embeddings σ_i so that $\sigma_1(\alpha) = \alpha$.

We claim that $x = \sigma_2(\alpha)\sigma_3(\alpha)...\sigma_d(\alpha) \in \mathcal{O}_K$, so that $N(\alpha) = \alpha x \in I$ (since $\alpha \in I$ and I is an ideal). To prove the claim note first that each $\sigma_i(\alpha)$ is an algebraic integer (since each is a conjugate of α, and so is a root of $m_\alpha(x)$, which is monic with integer coefficients). It follows that the product x is also an algebraic integer. Since $x = \frac{N(\alpha)}{\alpha} \in K$, we see that $x \in \mathcal{O}_K$ follows.

Now we know that $N(\alpha) \in I$ we can show that the quotient ring $\mathcal{O}_K / I$ is finite as follows. Choose $\beta_1, \beta_2, ..., \beta_d \in \mathcal{O}_K$ such that $\mathcal{O}_K = \{a_1\beta_1 + a_2\beta_2 + ... + a_d\beta_d \,|\, a_1, a_2, ..., a_d \in \mathbb{Z}\}$ (we have proved that this is possible in the notes). Note that since $N(\alpha) \in I$, $\beta_i \in \mathcal{O}_K$ and I is an ideal of $\mathcal{O}_K$, we have that $N(\alpha)\beta_i \in I$ for each i. Thus, given an arbitrary coset $[c_1\beta_1 + c_2\beta_2 + ... + c_d\beta_d] \in \mathcal{O}_K$, we may subtract a suitable multiple of $[0] = [N(\alpha)\beta_i] \in \mathcal{O}_K / I$ for each i to "reduce" our coset representative to one satisfying $c_i \in \{0, 1, ..., |N(\alpha)| - 1\}$ for each i. Since there are only finitely many such elements (at most $|N(\alpha)|^d$) we must have that $\mathcal{O}_K / I$ is a finite ring.