§2.5. Let $\alpha = \sqrt[3]{2}$, $K = \mathbb{Q}(\alpha)$ and $m = (O_K : \mathbb{Z}[\alpha])$. Then we need to show that $m = 1$. The discriminant gives

$$d(1, \alpha, \alpha^2) = -4 \cdot 27 = m^2 d_K.$$ 

It suffices to show that $2, 3 \not| m$. We first show that $2 \not| m$. If $2 | m$, then there exists $\xi \in O_K$, $\xi \not\in \mathbb{Z}[\alpha]$ but $2 \xi \in \mathbb{Z}[\alpha]$. Write

$$2 \xi = b_0 + b_1 \alpha + b_2 \alpha^2$$

and take the minimal $j$ such that $2 \not| b_j$. Then

$$\frac{b_j}{2} \alpha^j + \cdots + \frac{b_2}{2} \alpha^2 = \xi - \left( \frac{b_0}{2} + \cdots + \frac{b_{j-1}}{2} \alpha^{j-1} \right) \in O_K.$$ 

Multiplying by $\alpha^2 - j \in O_K$, it is clear that

$$\frac{b_j}{2} \alpha^2 + \cdots + \frac{b_2}{2} \alpha^{4-j} \in O_K.$$ 

Since $\alpha^3 = 2$, we have $\alpha^n/2 \in O_K$ for any $n \geq 3$. It follows that

$$\frac{b_j}{2} \alpha^2 \in O_K.$$ 

Taking norm from $O_K$ to $\mathbb{Z}$ gives that

$$\frac{b_j^3}{8} \cdot 4 = \frac{b_j^3}{2} \in \mathbb{Z}.$$ 

But $2 \not| b_j$, a contradiction. Therefore $2 \not| m$.

The general result of this argument is that, if $\alpha$ is a root of an Eisenstein polynomial for a prime $p$ and $K = \mathbb{Q}(\alpha)$, then $p \not| (O_K : \mathbb{Z}[\alpha])$.

Now apply this result for $\beta = \alpha - 2$. The minimal polynomial of $\beta$ is $(x + 2)^3 - 2 = x^3 + 6x^2 + 12x + 6$, which is an Eisenstein polynomial for the prime 3. Since $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and $\mathbb{Z}[\alpha] = \mathbb{Z}[\beta]$, we obtain that $3 \not| (O_K : \mathbb{Z}[\beta]) = m$, which finishes the proof. $\square$

For §3 we shall only give solutions of §3.1-§3.8.

§3.1. Since $-7 \equiv 1 \mod 4$, the ring of integers of $\mathbb{Q}(\sqrt{-7})$ is $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Then we have the decomposition

$$33 + 11\sqrt{-7} = 2 \cdot 11 \cdot \frac{3 + \sqrt{-7}}{2} = \frac{1 + \sqrt{-7}}{2} \cdot \frac{1 - \sqrt{-7}}{2} \cdot (2 + \sqrt{-7})(2 - \sqrt{-7}) \cdot \frac{3 + \sqrt{-7}}{2}$$

$$= \frac{1 + \sqrt{-7}}{2} \left( \frac{-1 + \sqrt{-7}}{2} \right)^3 (2 + \sqrt{-7})(2 + \sqrt{-7}).$$
Applying the norm map from $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ to $\mathbb{Z}$, it is not hard to see that all the factors in the last product are irreducible.

§3.2. The ring of integers of $\mathbb{Q}(\sqrt{-47})$ is $\mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$. The only nontrivial part of this exercise is to show that $\frac{13+\sqrt{-47}}{2}$ are irreducible. Suppose that

$$\frac{13 + \sqrt{-47}}{2} = (a + b\sqrt{-47})(c + d\sqrt{-47})$$

where $a, b$ are either both integers or both half-integers. Taking norms give that

$$54 = (a^2 + 47b^2)(c^2 + 47d^2).$$

Then $b$ and $d$ cannot be both nonzero (otherwise $54 \geq 47^2/4$ which is false). Hence we may assume that $d = 0$ and $c$ is an integer. Thus

$$54 = (a^2 + 47b^2)c^2,$$

which implies that $c^2 = 1, 4$ or $9$. It is easy to rule out the possibilities $c^2 = 4$ or $9$. Therefore $c = \pm 1$, which shows that $\frac{13+\sqrt{-47}}{2}$ is irreducible.

§3.3* This problem should appear a bit later. Let $K = \mathbb{Q}(\sqrt{d})$. Since $p \nmid d_K$, $p$ does not ramify in $K$ (Chapter III (2.12)). In this case it means $p\mathcal{O}$ is not a square of a prime ideal of $\mathcal{O}_K$. Then the exercise really says $p\mathcal{O} = p_1p_2$ is a product of two distinct prime ideals if and only if $x^2 \equiv d \mod p$ has a solution. It follows from the fact that if $p\mathcal{O}$ factors as above then $p_2 = \sigma(p_1)$, where $\sigma$ is the nontrivial element of Gal($K/\mathbb{Q}$).

§3.4. Following the hint, assume that there are only finitely many prime ideals $p_1, \ldots, p_r$. Choose $\pi_i \in p_i \setminus p_i^2$. If $a = p_1^{v_1} \cdots p_r^{v_r} \neq 0$ is an ideal, by the Chinese remainder theorem there is $a$ such that $a \equiv \pi_i^{v_i} \mod p_i^{v_i+1}$. Then $a = (a)$ is principal.

§3.5. By the Chinese remainder theorem we may assume that $a = p^n$ is a prime power. Then the only proper ideals of $\mathcal{O}/a$ are $p^i/p^n$, $i = 1, \ldots, n-1$. Take $\pi \in p \setminus p^2$. If we write $(\pi) = p \prod_{q \neq p} q^{n_q}$, then

$$(\pi^i + p^n) = p^i(\prod_{q \neq p} q^{n_q + p^{n-i}}) = p^i.$$ 

It follows that $p^i/p^n = (\pi^i \mod p^n)$ is principal.

§3.6. Let $a$ be a nonzero ideal. Take any $0 \neq x \in a$. By §3.5, $\mathcal{O}/(x)$ is a PID, hence $a/(x)$ is generated by $y + (x)$ for some $y \in a$. It follows that $a$ is generated by $x$ and $y$.

§3.7. Following the hint, the proof of Lemma 3.4 shows that $(0)$ is a product of prime ideals $p_1 \cdots p_r$. Consider the chain

$$R \supset p_1 \supset p_1p_2 \supset \cdots p_1 \cdots p_r = (0).$$

Then each quotient $p_1 \cdots p_{i-1}/p_1 \cdots p_i$
is a finite dimensional vector space over the field $R/p_i$. Therefore the above chain can be refined to into a composition series, from which the descending chain condition follows.

Remark: if a Noetherian ring satisfies the descending chain condition, it is called an Artinian ring. □

§3.8. Write $m = \prod_{i=1}^{r} p_i^{\nu_i}$. We may express a fractional ideal as $a = \prod_{i=1}^{s} p_i^{\mu_i}$, where $s \geq r$. By the Chinese remainder theorem we can find $a \in K^\times$ such that

$$(a) = \prod_{i=1}^{s} p_i^{-\mu_i} \prod_{q \neq p_1, \ldots, p_s} q^{\nu_q}$$

where $\nu_q \geq 0$ for any $q \neq p_1, \ldots, p_s$. Then

$$a \cdot (a) = \prod_{q \neq p_1, \ldots, p_s} q^{\nu_q}$$

is an integral ideal prime to $m$. □

§4.3. Erratum: it should be required that the integers $m_i$ are not all zero in the conclusion.

Let $\Gamma$ be the image of $\mathbb{Z}^n$ under the linear map $\mathbb{R}^n \to \mathbb{R}^n$, $x \mapsto Ax$. Then it is a lattice of $\mathbb{R}^n$ whose volume is $|\det A|$. Let $X$ be the centrally symmetric convex subset

$\{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_i| < c_i\}$

of $\mathbb{R}^n$. Then its volume is $2^n \prod_i c_i$. Therefore

$$\text{vol}(X) > 2^n \text{vol}(\Gamma)$$

and by Minkowski’s lattice point theorem $X$ contains a nonzero lattice point of $\Gamma$, which is the required assertion. □