1. Let $\alpha = \frac{1+\sqrt{8}}{2}$, then $2\alpha - 1 = \sqrt{8}$;

Square both sides and get $4\alpha^2 - 4\alpha - 7 = 0$.

So the minimal polynomial of α over $\mathbb{Q}$ is $4x^2 - 4x - 7$, which is not monic. So α is not integral over $\mathbb{Z}$.

2. In the ring $\overline{\mathbb{Z}}$ we have the ascending chain of ideals

$$(2) \subseteq (2^{\frac{1}{2}}) \subseteq \cdots \subseteq (2^{\frac{1}{2^n}}) \subseteq \cdots$$

which is not stationary. Hence $\overline{\mathbb{Z}}$ is not noetherian.

3. Let B be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$.

As $\sqrt{d}$ is integral / $\mathbb{Z}$, we have $\mathbb{Z}[\sqrt{d}] \subseteq B$. If in addition $d \equiv 1\ (4)$, then $\frac{1+\sqrt{d}}{2}$ is integral / $\mathbb{Z}$ (indeed, $\frac{1+\sqrt{d}}{2}$ is a root of $X^2 - X + \frac{1-d}{4}$, which lies in $\mathbb{Z}[X]$ since $\frac{1-d}{4} \in \mathbb{Z}$).

So $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq B$ if $d \equiv 1\ (4)$

Now let $\alpha \in B$. Then α is a root of a monic polynomial $X^2 + bX + c \in \mathbb{Z}[X]$.

So $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2} \in \mathbb{Q}(\sqrt{d}) \Rightarrow b^2 - 4c = k^2 d$ for some $k \in \mathbb{Z}$.

(i) $d \equiv 1\ (4)$ & $k \equiv 1\ (4)$: Then $b^2 \equiv 1\ (4)$, so $2 \nmid b$

Then $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. If $dk^2 \not\equiv 1\ (4)$, then $k^2 \equiv 0\ (4)$ (since squares are $\equiv 0$ or $1\ (4)$), hence $2 \mid b$, $4 \mid (b^2 - 4c)$, so $\alpha \in \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

(ii) $d \not\equiv 1\ (4)$ & $k^2 \equiv 1\ (4)$: Since $b^2 \equiv k^2 d\ (4)$, we must then have $d \equiv 0\ (4)$. But d was squarefree, so this cannot happen.

(iii) $d \not\equiv 1\ (4)$, $k^2 \equiv 0\ (4)$: Then $b^2 \equiv 0\ (4)$, so $2 \mid b$, $4 \mid (b^2 - 4c)$

$\Rightarrow \alpha \in \mathbb{Z}[\sqrt{d}]$.

4. First, note that (x) is not a prime ideal in A, since $z, w \notin (x)$ but $zw = xy \in (x)$. Hence x is not a prime element. Similarly for y, z and w.

We show that x is irreducible. A similar proof can be used also for y, z and w.

Suppose that $x = fg \in A$, and let $F, G \in k[X, Y, Z, W]$ be representatives for f resp g.

Write $F = \sum_{i=1}^{s} F_i$, $G = \sum_{i=1}^{t} G_i$, where the F_i & G_i's are homogeneous of degree i. We may assume that no term F_i, G_i is divisible by $XY - ZW$. Then we have:

$$\begin{aligned} X &= FG + C(XY - ZW) \\ &= \left(\sum_{1}^{s} F_i\right)\left(\sum_{1}^{t} G_i\right) + C(XY - ZW) \\ &= \left(\sum_{\substack{i<s, \\ j<t}} F_i G_j\right) + F_s G_t + C(XY - ZW) \qquad (*) \end{aligned}$$

Assume $s+t \geq 1$. Then the homogeneous part of $(*)$ of degree $s+t$ must vanish, i.e.,

$$F_s G_t + C_{s+t-2}(XY - ZW) = 0$$

But then either F_s or G_t has $XY - ZW$ as a factor. ↯

Hence either f or g must be a unit, so x is irreducible.

5. Let $1, \sqrt{d}$ be a basis for $K = \mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$.

Then $T_\alpha(1) = a + b\sqrt{d}$, $T_\alpha(\sqrt{d}) = bd + a\sqrt{d}$.

So the matrix of T_α is $\begin{pmatrix} a & b \\ bd & a \end{pmatrix}$,

yielding $T_{L/\mathbb{Q}}(\alpha) = 2a$, $N_{L/\mathbb{Q}}(\alpha) = a^2 - d b^2$.

6. First, note that if u is a unit in the ring of integers $\mathcal{O}_K$ for some number field K, then $N(u) = \pm 1$.

Indeed, suppose that $uv = 1$ for some $v \in \mathcal{O}_K$.

Then $N(uv) = N(u)\,N(v) = N(1) = 1$, and since the norm of an algebraic integer lies in $\mathbb{Z}$, this means that $N(u)$ is a unit in $\mathbb{Z}$, hence $\in \{\pm 1\} = \mathbb{Z}^*$.

a) Suppose that $2 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

Then $N(2) = 4 = N(\alpha)\,N(\beta)$. If neither α nor β is a unit in $\mathbb{Z}[\sqrt{-5}]$, then $N(\alpha) = N(\beta) = 2$.

Say $\alpha = x + \sqrt{-5}\,y$. Then $N(\alpha) = x^2 + 5y^2 = 2$.

But this equation has no integer solutions.

Hence α or β must be a unit.

Similarly for the other elements.

b) If for example $2 = u(1+\sqrt{-5})$ for a unit $u \in \mathbb{Z}[\sqrt{-5}]^*$,

then $N(2) = 4 = N(u)\,N(1+\sqrt{-5}) = \pm 6$,

which is nonsense.

Similarly for the other cases.

7. Let $K = \mathbb{F}_p(X)$, $L = \mathbb{F}_p(X^{1/p})$.

Let us show that $\mathrm{Tr}_{L/K}(\alpha) = 0 \quad \forall \alpha \in L$, which shows that $(1,-) = 0$, and hence that the form $(-,-)$ is degenerate.

Let $1, X^{\frac{1}{p}}, \dots, X^{\frac{p-1}{p}}$ be a basis for L/K, and let $\alpha = a_{p-1} X^{\frac{p-1}{p}} + \cdots + a_1 X^{\frac{1}{p}} + a_0$ be any element of L.

Then the matrix of T_α has only a_0 along its diagonal, hence $\mathrm{Tr}_{L/K}(\alpha) = p a_0 = 0$.

8. a) Since

$$\mathrm{Tr}(\alpha_i \alpha_j) = \sum_k \sigma_k(\alpha_i \alpha_j)$$

$$= \sum_k \sigma_k(\alpha_i)\,\sigma_k(\alpha_j) = \left(\sigma_k(\alpha_i)\right)^t_{i,k} \left(\sigma_k(\alpha_j)\right)_{j,k}$$

we have $d(\alpha_1, \dots, \alpha_n) = \det\left(\mathrm{Tr}(\alpha_i \alpha_j)\right) = \det\left(\sigma_i(\alpha_j)\right)^2$.

b) We have

$$\det(\sigma_i \alpha_j) = \sum_{\tau \in S_n} \mathrm{sgn}(\tau)\, \sigma_{\tau(1)}(\alpha_1) \cdots \sigma_{\tau(n)}(\alpha_n)$$

$$= \sum_{\tau \text{ even}} \sigma_{\tau(1)}(\alpha_1) \cdots \sigma_{\tau(n)}(\alpha_n) - \sum_{\tau \text{ odd}} \sigma_{\tau(1)}(\alpha_1) \cdots \sigma_{\tau(n)}(\alpha_n)$$

$$= P - N,$$

so $d_K = (P-N)^2 = (P+N)^2 - 4PN$. Since squares are $\equiv 0$ or $1 \bmod 4$, it suffices to show that $P+N$ and PN are integers.

Let τ be any element of the absolute Galois group of K over $\mathbb{Q}$. Then either $\tau(N) = N$ or $\tau(N) = P$ & $\tau(P) = N$. Either way, $P+N$ and PN are fixed, so $P+N, PN \in \mathbb{Q}$. Since $P+N$, PN are integral, $P+N, PN \in \mathbb{Z}$.

9. a) We get

$$d(1, \alpha, \cdots, \alpha^{n-1}) = (\mathcal{O}_K : \mathbb{Z}[\alpha])^2 d_K ,$$

so if $d(1, \alpha, \cdots, \alpha^{n-1})$ is squarefree, then $(\mathcal{O}_K : \mathbb{Z}[\alpha]) = 1$, hence $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

b) Note that f is irreducible over $\mathbb{Q}$, for if α was a rational root, then α would be an integer dividing -1.

We have $d(1, \alpha, \alpha^2) =$ discriminant of f

$$= -31,$$

which is squarefree, hence $\mathcal{O}_K = \mathbb{Z}[\alpha]$ by a).

10. Suppose that $\mathcal{O}$ is a Dedekind ring that is also a UFD. Let $\mathfrak{a} \subseteq \mathcal{O}$ be an ideal.

Since $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}}$, it suffices to show that all prime ideals of $\mathcal{O}$ are principal.

Let $\mathfrak{p}$ be a prime ideal $\neq 0$ of $\mathcal{O}$, and let $x \in \mathfrak{p} \setminus \{0\}$ be a nonzero element.

Then x factors uniquely into a product of prime elements

$$x = u p_1^{e_1} \cdots p_r^{e_r} , \text{ since } \mathcal{O} \text{ is UFD.}$$

Then $\mathfrak{p} \supseteq (p_i)$ for some i, and since (p_i) is a prime ideal, it follows that $\mathfrak{p} = (p_i)$.

11. Recall that a local, noetherian integral domain of Krull dimension 1 is a DVR $\iff$ it is integrally closed.
(e.g., Prop. 9.2. in Atiyah - Macdonald)
Hence the result follows from the fact that an integral domain A is integrally closed $\iff$ A_m is integrally closed $\forall$ maximal ideals m of A.

12. a) Let $\mathfrak{p} = (2, 1+\sqrt{-d})$. Then $\mathfrak{p}$ is prime, since

$$\mathcal{O}_K/\mathfrak{p} \cong \frac{\mathbb{Z}[x]}{(x^2+d, 2, 1+x)} \cong \mathbb{F}_2.$$

Now compute

$$\mathfrak{p}^2 = (2, 1+\sqrt{-d})^2 = (4, 2(1+\sqrt{-d}), 2\sqrt{-d}+1-d).$$

Since d is odd and $d \not\equiv 3 \ (4)$, we have $d \equiv 1 \ (4)$, so $1-d = 4n$ for some $n \in \mathbb{Z}$.
Then

$$\mathfrak{p}^2 = (4, 2(1+\sqrt{-d}), 2(\sqrt{-d}+2n)) \subseteq (2).$$

Moreover, $2 - 2\sqrt{-d} - (2\sqrt{-d}+4n) = 2-4n \in \mathfrak{p}^2$,
and since $4 \in \mathfrak{p}^2$, $2-4n+4n = 2 \in \mathfrak{p}^2$ also.
Hence $\mathfrak{p}^2 = (2)$.

b) Suppose $\mathfrak{p} = (x)$. Then in particular $2 = \alpha x$,
for some $\alpha \in \mathbb{Z}[\sqrt{-d}]$. Now α cannot be a unit,
hence $N(2) = 4 = N(\alpha)N(x)$ yields $N(x) = 2$.
Write $x = a + b\sqrt{-d}$, $a, b \in \mathbb{Z}$.
Then $a^2 + d b^2 = 2$, which is impossible since $d > 1$.

3. a) Write $(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$, $(y) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mu_{\mathfrak{p}}}$

Then $(xy) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}+\mu_{\mathfrak{p}}}$,

hence $\operatorname{ord}_{\mathfrak{p}}(xy) = \operatorname{ord}_{\mathfrak{p}}(x) + \operatorname{ord}_{\mathfrak{p}}(y)$.

For the second property, let us localize in order to consider one prime at a time.

Since $\mathcal{O}$ is Dedekind, $\mathcal{O}_{\mathfrak{p}}$ is a DVR, so $\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = (\pi)$ for a uniformizer π.

Write $x\mathcal{O}_{\mathfrak{p}} = \mathfrak{p}^{\nu}\mathcal{O}_{\mathfrak{p}} = (\pi^{\nu})$,

$y\mathcal{O}_{\mathfrak{p}} = \mathfrak{p}^{\mu}\mathcal{O}_{\mathfrak{p}} = (\pi^{\mu})$

Thus $x = u\pi^{\nu}$, $y = v\pi^{\mu}$ for $u, v \in \mathcal{O}_{\mathfrak{p}}^{*}$.

We may assume $\mu \leq \nu$.

Then $x + y = u\pi^{\nu} + v\pi^{\mu}$

$$= \underbrace{(uv^{-1}\pi^{\nu-\mu} + 1)}_{\in \mathcal{O}_{\mathfrak{p}}^{*}} v\pi^{\mu},$$

hence $\operatorname{ord}_{\mathfrak{p}}(x+y) \geq \min\{\operatorname{ord}_{\mathfrak{p}}(x), \operatorname{ord}_{\mathfrak{p}}(y)\}$.

b) Writing $a = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$, $b = \prod_{\mathfrak{p}} \mathfrak{p}^{\mu_{\mathfrak{p}}}$,

the statement follows immediately.

(8)

14. a) For each i, pick an element $\xi_i \neq 0$ in

$$\mathfrak{p}_i^{\nu_i}/\mathfrak{p}_i^{\nu_i+1} \subseteq \mathcal{O}/\mathfrak{p}_i^{\nu_i+1}.$$

Since $\varphi : \mathcal{O} \longrightarrow \prod_i \mathcal{O}/\mathfrak{p}_i^{\nu_i+1}$

$$a \longmapsto (a \bmod \mathfrak{p}_i^{\nu_i+1})_i$$

is surjective, there is an $a \in \mathcal{O}$ such that $\varphi(a) = (\xi_i)_i$. This means that, for all i, $a \in \mathfrak{p}_i^{\nu_i}$, but $a \notin \mathfrak{p}_i^{\nu_i+1}$.

But this says precisely that $\operatorname{ord}_{\mathfrak{p}_i}(a) = \nu_i$.

b) With $\alpha = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$. By a), there is an element $a \in \mathcal{O}$ such that $\operatorname{ord}_{\mathfrak{p}_i}(a) = \nu_i \quad \forall\, i = 1, \dots, r$.

But we want $\operatorname{ord}_{\mathfrak{q}}(a) = 0$ for all $\mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_r$.

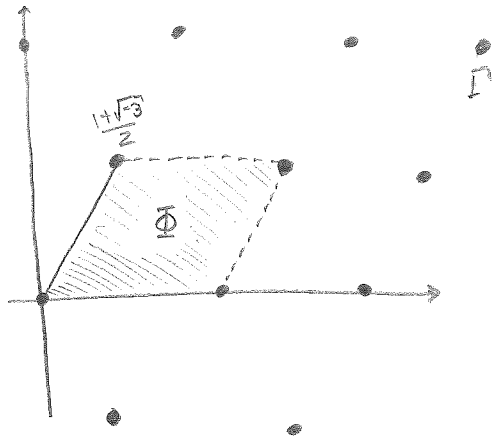
To fix this, let $b \in \mathcal{O}$ be such that

$$\operatorname{ord}_{\mathfrak{q}}(b) = \begin{cases} \nu_i, & \mathfrak{q} = \mathfrak{p}_i \text{ for some } i = 1, \dots, r \\ 0, & \mathfrak{q} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \text{ but} \\ & \operatorname{ord}_{\mathfrak{q}}(a) > 0. \end{cases}$$

Since there are only finitely many $\mathfrak{q}$ s.t. $\operatorname{ord}_{\mathfrak{q}}(a) > 0$, this makes sense.

But then $\operatorname{ord}_{\mathfrak{q}}(a,b) = \operatorname{ord}_{\mathfrak{q}}(\alpha)$ for all primes $\mathfrak{q}$, so $\alpha = (a,b)$.

15. a)



$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi)$
$= \frac{\sqrt{3}}{2}$

b) $u = 2 - \sqrt{3} \Rightarrow N(u) = 4 - 3 = 1$, so u is a unit in $\mathbb{Z}[\sqrt{3}]$.

Let $u_n = (2-\sqrt{3})^n \in \mathbb{Z}[\sqrt{3}]$. Since $|u| < 1$, $\lim_{n\to\infty} u_n = 0$.

So $0 \in R$ is an accumulation point.

c) Any subgroup of R is either cyclic or dense.

By b), $\mathbb{Z}[\sqrt{3}]$ cannot be cyclic.

(In fact, $\mathbb{Z}[\alpha]$ is dense in R for any irrational $\alpha \in R$.)