1. (a) We first show by induction that for each $n \geq 1$, there are unique elements $a_0, \dots, a_{n-1} \in X$ such that $x - \sum_{i=0}^{n-1} a_i \pi^i \in (\pi^n)$. The case $n = 1$ is just the definition of X. For the induction step, we can write (by induction) $x - \sum_{i=0}^{n-1} a_i \pi^i = \pi^n y$ for some $y \in A$; and we can write $y = a_n + \pi z$ for some element $a_n \in X$, giving an expression $x = \sum_{i=0}^{n} a_i \pi^i + \pi^{n+1} z$. If we have another such expression $x = \sum_{i=0}^{n} b_i \pi^i + \pi^{n+1} z'$, then the induction hypothesis shows that $a_i = b_i$ for each $i = 0, \dots, n-1$. We can then divide by π^n to conclude that $a_n - b_n \in (\pi)$, hence $a_n = b_n$ (by definition of X).

   To say that A is complete means that the natural map $f : A \to \varprojlim_{n \geq 1} A/(\pi^n)$ is an isomorphism. We can define an element of the inverse limit by $(\sum_{i=0}^{n-1} a_i \pi^i \bmod (\pi^n))_{n \geq 1}$. This is equal to $f(x)$, showing that x has an expression of the given form. The expression is unique because f is injective.

   (b) Suppose that $x = \sum_{i=0}^{\infty} a_i p^i$ has an eventually periodic p-adic expansion. We must show that x is rational. After subtracting an integer from x and dividing by a power of p, we can assume that the p-adic expansion is periodic: there exists an integer $k \geq 1$ such that $a_i = a_{i+k}$ for all $i \geq 0$. Thus we can write

$$x = (a_0 + a_1 p + \dots a_{k-1} p^{k-1})(1 + p^k + p^{2k} + \dots).$$

   We therefore just need to show that $\sum_{i=0}^{\infty} p^{ik}$ is rational. It equals $1/(1 - p^k)$, so this is true.

   (c) Suppose that $x = \sum_{i=0}^{\infty} a_i \pi^i$ has an eventually periodic π-adic expansion, where $\pi = \sqrt{p}$. We want to show that $x \in \mathbb{Q}(\sqrt{p})$. We can again assume that there exists $k \geq 1$ such that $a_i = a_{i+k}$ for all $i \geq 0$. We can moreover assume that $k = 2r$ is even (otherwise replace k by $2k$). Then we can write

$$\begin{aligned} x &= (a_0 + a_1 \pi + \dots a_{k-1} \pi^{k-1})(1 + \pi^k + \pi^{2k} + \dots) \\ &= (a_0 + a_1 \pi + \dots a_{k-1} \pi^{k-1})(1 + p^r + p^{2r} + \dots), \end{aligned}$$

   showing that indeed $x \in \mathbb{Q}(\sqrt{p})$.

2. (a) Let $f(X) = X^n + a_1 X^{n-1} + \dots + a_n \in K[X]$ be a monic polynomial such that $f(0) \neq 0$, and let $v_K : K^\times \to \mathbb{Z}$ be the valuation. The Newton polygon $N_K(f)$ is defined to be the lower convex hull of the points $(i, v_K(a_i))$ for those $i = 0, \dots, n$ such that $a_i \neq 0$.

Let $\lambda_1 < \lambda_2 < \cdots < \lambda_k$ be the slopes of $N_K(f)$, and let m_i be the multiplicity of λ_i. Then there exists a unique factorisation $f(X) = \prod_{i=1}^k g_i(X)$ in $K[X]$ such that $g_i(X) \in K[X]$ is a monic polynomial of degree m_i and $N_K(g_i))$ has a single segment of slope λ_i.

(b) Let $f(X) \in \mathbb{Q}[X]$ be a monic irreducible polynomial, and let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(X)$. Let p be a prime and factorise $f(X) = \prod_{i=1}^r f_i(X)$ in $\mathbb{Q}_p[X]$, where each $f_i(X) \in \mathbb{Q}_p[X]$ is monic and irreducible. Then there is a bijection between the set of prime ideals $P \subset \mathcal{O}_K$ lying above (p) and the set of irreducible factors $f_i(X)$ of $f(X)$ in $\mathbb{Q}_p$ with the following property: if P and $f_i(X)$ correspond under this bijection, then $f_i(X)$ is the minimal polynomial of $\alpha \in K_P$ over $\mathbb{Q}_p$.

(c) Now let $f(X) = X^4 + 6X^2 - 48$. We have $6 = 2 \times 3$ and $48 = 2^4 \times 3$ so $N_{\mathbb{Q}_3}(f)$ has a single segment of slope $1/4$, while $N_{\mathbb{Q}_2}(f)$ has two segments of slope $1/2$ and $3/2$, each slope occurring with multiplicity 2. By Eisenstein's criterion at the prime 3, $f(X)$ is irreducible.

Let $L/\mathbb{Q}$ be the splitting field of $f(X)$. Let $\alpha, \beta \in L$ be the roots of $X^2 + 6X - 48$, $E = \mathbb{Q}(\alpha, \beta)$. Thus $E/\mathbb{Q}$ is a quadratic subfield of $L/\mathbb{Q}$ and $L = E(\sqrt{\alpha}, \sqrt{\beta})$. If we let $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/E)$, then there is a surjective homomorphism $G \to \mathrm{Gal}(E/\mathbb{Q})$ with kernel H. Viewing G as a subgroup of S_4 via its action by permutation of $\{\sqrt{\alpha}, -\sqrt{\alpha}, \sqrt{\beta}, -\sqrt{\beta}\}$, we see that H is contained in the subgroup generated by the transpositions (12) and (34); in particular, it has cardinality at most 4.

We claim that H has cardinality 4, so G has order 8. There are several different ways to do this. Here is one using the prime 3. Let $P \subset \mathcal{O}_L$ be a prime ideal lying above 3, and let $R = P \cap K$, where $K = \mathbb{Q}(\sqrt{\alpha})$. Then $L_P/\mathbb{Q}_3$ is a Galois extension containing K_P. Since $f(X)$ is Eisenstein at 3, the degree 4 extension $K_R/\mathbb{Q}_3$ is totally ramified of degree 4. This shows that the extension $L_P/\mathbb{Q}_3$ is tamely ramified, of ramification index divisible by 4. We proved in lectures that if M_1/M_2 is a Galois tamely ramified extension of degree n then the residue field k_{M_2} contains the n^{th} roots of unity. Therefore we see that the maximal unramified subextension $L_{P,0}$ of L_P must have degree 2, so that the cardinality of $k_{L_{P,0}}^\times$ is divisible by 4.

We deduce that $L_P/\mathbb{Q}_3$ is Galois of degree 8, that $\mathrm{Gal}(L_P/\mathbb{Q}_3) = \mathrm{Gal}(L/\mathbb{Q})$, and that P is the unique prime ideal of $\mathcal{O}_L$ lying above

3. In particular, G has cardinality 8.

3. (a) Let $f(X,Y) = aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]$ be positive definite binary quadratic form. We say that $f(X,Y)$ is reduced if $c \geq a \geq |b|$, and $b \geq 0$ if either of these inequalities are equalities.

   Now let K be an imaginary quadratic field, viewed a subfield of $\mathbb{C}$; we take the convention that squareroots of negative numbers have positive imaginary part. We will prove that there is a bijection between the ideal class group of $\mathcal{O}_K$ and the set of reduced positive definite binary quadratic forms of discriminant $\operatorname{disc} \mathcal{O}_K$. We prove this in two stages. We first show that there is a bijection between the ideal class group and the set of $\mathrm{SL}_2(\mathbb{Z})$-orbits of binary quadratic forms of this discriminant. We then show that each $\mathrm{SL}_2(\mathbb{Z})$-orbit contains a unique representative which is reduced.

   Let $D = \operatorname{disc} \mathcal{O}_K$. We know that $K = \mathbb{Q}(\sqrt{D})$. To construct the bijection, we associate to any positive definite binary quadratic form of discriminant D the fractional ideal $I = \mathbb{Z} \oplus \mathbb{Z}\beta$, where $\beta = (-b + \sqrt{D})/2a$ is the unique root of $f(X,1)$. We need to check that I is invariant under multiplication by I. We then need to check that if we replace $f(X,Y)$ by an equivalent form (under the action of $\mathrm{SL}_2(\mathbb{Z})$, then we replace I by another fractional ideal which nevertheless lies in the same ideal class.

   [For the rest of the proof, see Theorem 5.13 and Corollary 5.16 in the online notes.]

   (b) Now let $K = \mathbb{Q}(\sqrt{-6})$, so that $\operatorname{disc} \mathcal{O}_K = D = -24$. To calculate the cardinality of the ideal class group of K, we enumerate the reduced positive definite binary quadratic forms $f(X,Y) = aX^2 + bXY + cY^2$ of discriminant D. They all satisfy $|b| \leq \sqrt{24/3}$, hence $|b| \leq 2$. We see that the only possibilities are $X^2 + 6Y^2$ and $2X^2 + 3Y^2$.

   Thus the Hilbert class field H of $K = \mathbb{Q}(\sqrt{-6})$ is an everywhere unramified quadratic extension. To show $H = K(\sqrt{2})$, we just need to show $K(\sqrt{2})/K$ is everywhere unramified. The polynomial $X^2 - 2$ has discriminant prime to 2, so $K(\sqrt{2})/K$ is unramified at the prime ideals of $\mathcal{O}_K$ not lying above 2. We can also represent $K(\sqrt{-3}) = K(\zeta_3)$. The minimal polynomial $X^2 - X + 1$ of ζ_3 has discriminant prime to 3, so $K(\sqrt{2})/K$ is unramified at the prime ideals of $\mathcal{O}_K$ not lying above 3. Taking these statements together now shows that indeed $K(\sqrt{2})$ is the Hilbert class field of K.

4. The first polynomial divides $X^7 - X$, which we know to have 7 roots

in $\mathbb{Z}_7$ (which are all distinct modulo 7; the simple version of Hensel's lemma applies). For the second polynomial $f(X) = X^2 + 2X + 4$, we find $f(2X) = 4(X^2 + X + 1)$. The polynomial in brackets has no roots in $\mathbb{F}_2$, hence a fortiori in $\mathbb{Z}_2$ (and Hensel's lemma is not really required). The polynomial $g(X) = 3X^3 + X + 3$ satisfies $9g(X/3) = X^3 + 3X + 27 = h(X)$, say. We will apply Hensel's lemma to $h(X)$. We have $h(0) = 27$, $h'(0) = 3$; the strong version of Hensel's lemma applies to tell us that there is a unique root $\alpha \in \mathbb{Z}_3$ of $h(X)$ satisfying $v_3(\alpha) > v_3(h'(0)) = 1$.

We wish to know if $h(X)$ has any other roots in $\mathbb{Z}_3$. Looking mod 3, we see that any other root β of $h(X)$ in $\mathbb{Z}_3$ must lie in $3\mathbb{Z}_3$. We know that (by uniqueness of α) it must lie in $3\mathbb{Z}_3 - 9\mathbb{Z}_3$. However any such β satisfies $v_3(h(\beta)) = v_3(3\beta) = 2$, by the ultrametric triangle inequality, so cannot be a root.

5. (a) We recall the definition of our homomorphisms. Let $A_L \subset L$ denote the valuation ring. If $t \in G = G_0$, then $t(\pi_L) = a_t\pi_L$ for some $a_t \in A_L^\times$. The map $G_0/G_1 \to k_L^\times$ sends t to a_t mod (π), or equivalently to $t(\pi_L)/\pi_L$ mod (π). If π'_L is another choice of uniformizer, then we can write $\pi'_L = u\pi_L$ for some $u \in A_L^\times$, and then $t(\pi'_L)/\pi'_L = t(u)/u \cdot t(\pi_L)/\pi_L$. Since the extension L/K is totally ramified, G acts trivially on k_L, and hence $t(u) \equiv u$ mod (π). This shows that $\theta_0(t) = t(\pi_L)/\pi_L$ mod $(\pi_L) \in k_L^\times$ is independent of the choice of uniformizer.

   (b) If $i \geq 1$ and $t \in G_i$, then $t(\pi_L) = \pi_L + a_t\pi_L^{i+1}$ for some $a_t \in A_L$, and the map $G_i \to k_L$ sends t to a_t mod (π_L). Since $a_t = (t(\pi_L)/\pi_L - 1)/\pi_L^i$, this gives the claimed formula.

   Another way to express this is to set $U_L^i = \ker(A_L^\times \to (A_L/(\pi_L^i))^\times) = 1 + \pi^i A_L$, for any $i \geq 1$. There is a group isomorphism $f_i : U_L^i/U_L^{i+1} \to (\pi_L^i)/(\pi_L^{i+1})$ given by $x \mapsto x - 1$. If $t \in G_i$ then $t(\pi_L)/\pi_L \in U_L^i$, and $\theta_i(t) = f_i(t(\pi_L)/\pi_L)$. To see that θ_i is independent of choices, it is enough to show that $t(u\pi_L)/u\pi_L \equiv t(\pi_L)/\pi_L$ mod (π_L^{i+1}). Equivalently, that $t(u)/u \equiv 1$ mod (π_L^{i+1}). This is true because $t \in G_i$.

   This also shows why our original homomorphism does depend on our choice of uniformizer. Any such choice gives an isomorphism $g_{\pi_L} : (\pi_L^i)/(\pi_L^{i+1}) \to k_L$, $y \mapsto y/\pi_L^i$ mod (π_L), and our original homomorphism is $g_{\pi_L} \circ \theta_i$. We see that $g_{u\pi_L}(y) = u^{-i}g_{\pi_L}$, so if $u^i \not\equiv 1$ mod (π_L) and G_i/G_{i+1} is non-trivial then the homomorphisms $G_i \to k_L$ corresponding to the choices π_L and $u\pi_L$ of uniformizer are not equal.

(c) We want to show that if $s \in G_0$ and $t \in G_i$, then $\theta_i(sts^{-1}) = \theta_0(s)^i \theta_i(t)$. We calculate

$$\theta_i(sts^{-1}) = s(ts^{-1}(\pi_L)/s^{-1}(\pi_L) - 1) \bmod (\pi_L^{i+1}).$$

We have shown that θ_i is independent of the choice of uniformizer, so we can compute using the uniformizer $s^{-1}(\pi_L)$; we get $\theta_i(sts^{-1}) = s(\theta_i(t))$, where s is acting now on the group $(\pi_L^i)/(\pi_L^{i+1})$. To get the desired formula, we must show that the action of s on $(\pi_L^i)/(\pi_L^{i+1})$ (a 1-dimensional k_L-vector space equals multiplication by $\theta_0(s)^i$. In other words, that if $a \in A_L$ then $s(a\pi_L^i) \equiv \theta_0(s)^i a\pi_L^i \bmod (\pi_L^{i+1})$. Dividing through by $a\pi_L^i$, this is equivalent to the identity $s(a\pi_L^i)/a\pi_L^i \bmod (\pi_L) = \theta_0(s)^i$, which follows immediately from the definition of θ_0.

6. We assume $n \geq 3$, so $L \neq \mathbb{Q}$ and L/K is a quadratic extension. We recall that the Hilbert class field H/K is the maximal abelian unramified extension of K in which every real embedding of K remains real; moreover, $[H : K] = h_K$ (by class field theory). The extension HL/L is abelian and everywhere unramified; moreover, L has no real embeddings. It follows that HL is contained inside the Hilbert class field of L, which has degree h_L.

   By the tower law, we have $[HL : L][L : K] = [HL : H][H : K]$. We have $[L : K] = 2$. We have $[HL : H] \leq 2$, with equality if and only if $HL \neq H$. However, HL does not embed in $\mathbb{R}$ while H does, so we have $[HL : H] = 2$ and hence $[HL : L] = [H : K] = h_K$. Since HL is contained in the Hilbert class field of L, we deduce that h_K divides h_L.

7. We set $K = \mathbb{Q}(i)$, $L = K(\alpha)$ where $\alpha^4 = 2$. Thus L is the splitting field over $\mathbb{Q}$ of the polynomial $X^4 - 2$. We observe that $L/\mathbb{Q}$ is unramified outside 2, so L/K is unramified away from the unique prime ideal $P = (1 + i)$ of $\mathcal{O}_K$ lying above 2.

   The extension L/K is abelian of degree dividing 4. We will show that it has degree 4. Let Q denote a prime ideal of $\mathcal{O}_L$ lying above P. We will show that in fact L_Q/K_P is totally ramified of degree 4.

   Let $\sqrt{2} = \alpha^2$. We first recall that the extension $E = K_P(\sqrt{2})$ is a totally ramified quadratic extension of K_P of degree 2, with uniformizer $1 + \frac{1+i}{\sqrt{2}}$ (we have studied this extension in lectures). We consider the element

$\pi = 1 + \frac{1+i+\sqrt{2}}{\alpha^3}$. We compute

$$\pi^2 = 1 + \frac{1+i}{\sqrt{2}} + (1+\alpha)(1+i) + \alpha^3.$$

Since $1 + \frac{1+i}{\sqrt{2}}$ has strictly smaller valuation than $(1+i)$ and α^3, we see that π^2 has the same valuation as a uniformizer of E. This is possible only if L_Q/E is a ramified quadratic extension and π is a uniformizer of L_Q.

To compute the conductor of the extension L/K, we will compute the ramification groups of the extension L_Q/K_P. Let $G = \mathrm{Gal}(L_Q/K_P)$. It is cyclic of degree 4, generated by the element τ with $\tau(\alpha) = i\alpha$. We thus compute

$$\tau(\pi) - \pi = -\alpha(1 + \frac{1+i}{\sqrt{2}}),$$

hence $v_{L_Q}(\tau(\pi) - \pi) = 4$, and $\tau^2(\pi) - \pi = 2(1-\pi)$, hence $v_{L_Q}(\tau^2(\pi) - \pi) = 8$. We conclude that the lower ramification groups satisfy $G_0 = G_1 = G_2 = G_3$, $G_4 = \cdots = G_7 = \{1, \tau^2\}$, $G_8 = \{1\}$. It follows that the upper ramification groups are given by $G^0 = G^1 = G^2 = G^3$, $G^4 = G^5 = \{1, \tau\}$, $G^6 = \{1\}$. In particular, the conductor of the abelian extension L/K is the ideal P^6.

By class field theory, there is a surjection $\phi_{L/K} \to H(P^6) \to \mathrm{Gal}(L/K)$. We now describe the group $H(P^6)$ and its subgroup $\ker \phi_{L/K}$. The ideal class group of K is trivial, so we know that $H(P^6)$ is isomorphic to the quotient of the group $(\mathcal{O}_K/P^6)^\times$ by the subgroup generated by $\{\pm 1, \pm i\}$. We see that $H(P^6)$ has cardinality $2^5/2^2 = 8$, and therefore that $\ker \phi_{L/K}$ has order 2.

We therefore just need to identify a non-trivial element of $\ker \phi_{L/K}$. To do this, we calculate Frobenius elements. The prime 3 is inert in K, so $3\mathcal{O}_K$ is prime. Let R be a prime ideal of $\mathcal{O}_L$ lying above 3. Then $\mathrm{Frob}_{3\mathcal{O}_K}$ acts on $\mathcal{O}_L/R$ by $\alpha \mapsto \alpha^9 = 4\alpha \equiv \alpha \bmod R$. It follows that $\mathrm{Frob}_{3\mathcal{O}_K} = 1$ and $3 \bmod P^6$ generates $\ker \phi_{L/K}$.