Number Theory Exercise

Yuheng Shi

September 2022

This file is my solution to homework problems of the course Algebraic Number Theory I at JHU during Fall 2022. The problems are embedded in the lecture notes, which can be found here: `math.jhu.edu/~iyengar/ANT`. Because the course is in progress, a more complete version can be found here: `https://github.com/YuhengShi1/Math-Writings`.

Ex.2.1.5.(1) Consider a finite extension E of $\mathbb{F}_p$ of degree n where $n \geq 1$. Then $|E| = p^n$. $\forall a \in E, a^{p^n} - a = a^{p^n-1} \cdot a - a = a - a = 0$ since $|E^*| = p^n - 1$. Let $f \in \mathbb{F}_p[x] = x^{p^n} - x$. f is separable because $\gcd(f, f') = \gcd(x^{p^n} - x, -1) = 1$. Thus all elements of E are exactly roots of f, so E is splitting field of f over $\mathbb{F}_p$.
Conversely, for any $n \geq 1$, we can construct a field extension of $\mathbb{F}_p$ of degree n by letting E be the spitting field of f over $\mathbb{F}_p$. It is easy to verify that all the roots of f in E form a field containing $\mathbb{F}_p$. Thus as a set, $E = \{\text{all roots of f}\}$. Because f is separable, $|E| = p^n$. So $[E : \mathbb{F}_p] = n$.
Therefore, all finite extensions of $\mathbb{F}_p$ are splitting fields of $x^{p^n} - x$ over $\mathbb{F}_p$, where $n \geq 1$. By uniqueness of splitting fields, we can denote a field with p^n elements by $\mathbb{F}_{p^n}$. Since a field extension is splitting field extension if and only if it is finite and normal, any finite extension of $\mathbb{F}_p$ is normal. For any finite extension $\mathbb{F}_{p^n}/\mathbb{F}_p$, the minimal polynomial of any element of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ divides $x^{p^n} - x$ which is separable, so the minimal polynomial is separable, so the extension is separable.
(2)Assume $n \geq 1$. Let $\Phi_n(x) \in \mathbb{C}[x]$ be $\prod_{1 \leq m \leq n, (m,n)=1} (x - \zeta_n^m)$. Then $\Phi_n(x) \in \mathbb{Z}[x]$ and $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. To prove $\Phi_n(x) \in \mathbb{Z}[x]$, note $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Indeed,

$$x^n - 1 = \prod_{1 \leq m \leq n} (x - \zeta_n^m) = \prod_{1 \leq d|n} \prod_{1 \leq m \leq d, (m,d)=1} (x - \zeta_d^m) = \prod_{1 \leq d|n} \Phi_d(x)$$

where the second step is true because each factor in the LHS is in the RHS by removing $\gcd(m, n)$ on the exponent of ζ_n^m. Each factor in the RHS is in the LHS by multiplying $\frac{n}{d}$ on denominator and numerator of exponent of ζ_d^m. Each factor on RHS appears only once by elementary arguments. Then we use induction to prove $\Phi_n(x) \in \mathbb{Z}[x]$. The base case is trivial. For any $n > 1$, we have $x^n - 1 = \Phi_n(x) \cdot q(x)$ for some $q(x) \in \mathbb{Z}[x]$ by induction hypothesis. Because $\Phi_n(x)$ is monic, we can apply polynomial division in $\mathbb{Z}[x]$ by dividing $x^n - 1$ with $q(x)$. But this is also the result of polynomial division in $\mathbb{C}[x]$. By uniqueness of results of polynomial division (in $\mathbb{C}[x]$), we see that $\Phi_n(x) \in \mathbb{Z}[x]$. To prove $\Phi_n(x)$ is irreducible over $\mathbb{Q}$, it suffices to prove it is irreducible over $\mathbb{Z}$ by Gauss's Lemma.
FSOC, suppose $\Phi_n(x)$ is reducible. Note all irreducible factors of $\Phi_n(x)$ over $\mathbb{Z}$ collect the roots ζ_n^m where $(n, m) = 1$. Then there exists an irreducible factor $f(x)$ of $Phi_n(x)$ such that $\exists$ prime number p not dividing n and integer m, $f(\zeta_n^m) = 0$ and $f(\zeta_n^{pm}) \neq 0$. Otherwise, pick irreducible factor $h(x)$ which satisfies $h(\zeta_n) = 0$, then $\forall m$ such that $(m, n) = 1$, m is a product of primes not dividing n, so $h(\zeta_n^m) = 0$, then $\Phi_n(x) = h(x)$ is irreducible, contradiction.
Write $\Phi_n(x) = f(x)g(x)$. Because $\Phi_n(x)$ is monic, by Gauss's lemma f and g are primitive. By assumption $f(x)$ is the minimal polynomial of ζ_n^m over ͏" and $g(\zeta_n^{pm}) = 0$, so $f(x)|g(x^p)$ over $\mathbb{Q}$. So $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$. But $g(x^p)$ and $f(x)$ are primitive, so using Gauss's Lemma we actually have $h(x) \in \mathbb{Z}[x]$ (a detailed argument is given in the second to last paragraph of proof of Ex.2.2.9(3)). Working modulo p, we have $\tilde{g}(x^p) = \tilde{f}(x)\tilde{h}(x)$ where the " " represents image of a polynomial in $\mathbb{Z}[x]$ under the canonical map $\mathbb{Z}[x] \to \mathbb{F}_p[x]$. Note $\tilde{g}(x^p) = (\tilde{g})^p$, as we have $(\varphi_1 + \varphi_2)^p = \varphi_1^p + \varphi_2^p$ and $a^p = a \forall\ \varphi_1, \varphi_2 \in \mathbb{F}_p[x], a \in \mathbb{F}_p$.

Because $f(x)$ has leading coefficient ± 1, $\tilde{f}(x)$ is nonzero and nonunit, then $\tilde{f}(x)$ and $\tilde{g}(x)$ share some nontrivial factor $\tilde{l}(x)$, so $(\tilde{l}(x))^2 | \tilde{f}(x)\tilde{g}(x)$, so $\tilde{\Phi}_n(x)$ is inseparable in $\mathbb{F}_p[x]$. On the other hand $\tilde{\Phi}_n(x)$ is a factor of $x^n - 1 \in \mathbb{F}_p[x]$, and $\gcd(x^n - 1, nx^{n-1}) = 1$ by Euclidean algorithm (Note here $nx^{n-1} \neq 0$ because p does not divide n). But from knowledge on separability, this means $x^n - 1$ is separable over $\mathbb{F}_p$, thus is its factor $\tilde{\Phi}_n(x)$. Contradiction. Therefore, $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible. Then $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$. Because $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is splitting field extension of $\Phi_n(x)$, it is a normal extension. It is separable extension because ζ_n is separable over $\mathbb{Q}$. Therefore $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a finite Galois extension of degree $\phi(n)$. Thus $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Furthermore, by our knowledge of simple algebraic extension, elements of $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_n)$ are exactly those maps fixing $\mathbb{Q}$ and sending ζ_n to one root of $\Phi_n(x)$. Define $\phi : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \to (\mathbb{Z}/n\mathbb{Z})^*$ by $\phi(f) = [m]$ where $f(\zeta_n) = \zeta_n^m$. It is straightforward to verify this is a well-defined isomorphism. Thus $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

(3) Let $\alpha = \sqrt{2} + \sqrt{3}$. Obviously $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \leq 4$. Since $f(x) = x^4 - 10x^2 + 1$ kills $\sqrt{2} + \sqrt{3}$, and $f(x)$ is irreducible over $\mathbb{Z}$ (indeed, the four roots of $f(x)$ over $\mathbb{C}$ are $(\pm\sqrt{2} \pm \sqrt{3})$, and the product of any of the factors over $\mathbb{C}$ cannot be in $\mathbb{Z}[x]$ up to multiplication by constants), $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$, so $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Ex.2.1.7. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is separable over $\mathbb{Q}$ because it is finitely generated over $\mathbb{Q}$ by $\sqrt{2}$ and $\sqrt{3}$, and these two elements are separable over $\mathbb{Q}$. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is normal over $\mathbb{Q}$ because it is the splitting field extension of $x^4 - 10x^2 + 1$, as proved in Ex.2.1.5(c). Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is (finite) Galois extension. Define $G := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$, then $|G| = 4$ because the extension is Galois of degree 4. By our knowledge of simple algebraic extension, we can view $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a simple extension over $\mathbb{Q}(\sqrt{3})$, then because the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{3}) = x^2 - 2$ has two distinct roots $\pm\sqrt{2}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\exists$ an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ fixing $\sqrt{3}$ and sending $\sqrt{2}$ to $-\sqrt{2}$. Similarly, $\exists$ an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ fixing $\sqrt{2}$ and sending $\sqrt{3}$ to $-\sqrt{3}$. Composing these two automorphisms gives the last element of G sending $\sqrt{2}$ and $\sqrt{3}$ to their negative value. Thus $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It has three nontrivial proper subgroups. One is generated by $\varphi_{-\sqrt{2}}$, one is generated by $\varphi_{-\sqrt{3}}$, one is generated by $\varphi_{-\sqrt{2}, -\sqrt{3}}$, where the φ's have obvious definition. By Fundamental Theorem of Galois Theory, the subfields fixed by these subgroups are all nontrivial intermediate fields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Thus these fields are $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{6})$.

Ex.2.2.2. Define $f : F[x] \to \mathbb{Z}_{\geq 0}$ by $f(\varphi) = \deg \varphi$. Then $\forall a, b \in F[x]$ where $b \neq 0$, by polynomial division $\exists! q, r \in F[x]$ such that $a = bq + r$ where $0 \leq f(r) < f(b)$ or $r = 0$.

Ex.2.2.5. Let our ring be A. Consider any ascending chain of ideals $(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq ....$ It is easy to verify that $\bigcup_{i=0}^{\infty}(a_i)$ forms an ideal. But A is PID, so this union equals (b) for some $b \in A$. Then $b \in (a_k)$ for some $k \geq 0$. Then $(b) \subseteq (a_k)$. So $\forall n \geq k$, $(b) \subseteq (a_n) \subseteq (b)$. So $(a_n) = (b)$. So the chain stabilizes after (a_k).

Ex2.2.7. In a PID A, irreducibles are primes. Indeed, let $a \in A$ be irreducible, and let $bc \in (a)$ for some $b, c \in A$. Since A is PID, $(a, b) = (e)$ for some $e \in A$. a is irreducible, so $(e) = A$ or $(e) = (a)$. If $(e) = (a)$, then $b \in (a)$, and we are done. So suppose $(e) = A$. Then $\exists x, y \in A$ such that $ax + by = 1$. Multiply both sides by c and using $bc \in (a)$ we see $c \in (a)$. Then the unique factorization into irreducibles (primes) follows.

Ex.2.2.9(1). Let A be our UFD. In any integral domain, any prime p is irreducible. Indeed, if $p = ab$ for some $a, b \in A$, then WLOG assume $a \in (p)$. Then $p = pcb$ for some $c \in A$. A is integral domain and $p \neq 0$, so $1 = cb$ and b is a unit. In particular, when A is UFD, irreducibles are also primes. Indeed, let $a \in A$ be irreducible, and suppose $bc \in (a)$ for some $b, c \in A$. Then $bc = ad$ for some $d \in A$. Since A is UFD, the multiset of irreducible factors (up to associates) must equal on both sides. In particular, $b \in (a)$ or $c \in (a)$.
(2) $\mathbb{Z}$ is PID, so it is UFD by Proposition 2.2.6. We will prove later Ex.2.2.9(3) which implies $\mathbb{Z}[x]$ is UFD as well. The ideal $(2, x) \subseteq \mathbb{Z}[x]$ in not principal. Indeed if $(2, x) = (f)$ for some $f \in \mathbb{Z}[x]$, then because $(2, x)$ is the set of polynomials with even constant part, $\deg f = 0$, otherwise $2 \notin (f)$. Obviously $f \neq \pm 1$. Thus f is an integer with absolute value ≥ 2. But then $x \notin (f)$, contradiction.
(3) We will use Gauss's Lemma in this proof, i.e. over any UFD, $(cont_{fg}) = (cont_f)(cont_g)$ where $cont_f$ means gcd of coefficients of f. First note for an integral domain R, if all irreducibles are primes and a.c.c. (ascending chain condition) holds for principal ideals, then R is UFD. This follows from proof of Proposition 2.2.6 and Ex 2.2.7. (Also, if R is UFD, then irreducibles are primes (by Ex 2.2.9(1))) and a.c.c. holds for principal ideals (since each element factors into a unique collection of finitely many irreducibles)).

Now suppose A is UFD. Take any ascending chain of principal ideals in $A[x]$: $(f_0) \subseteq (f_1) \subseteq (f_2) \subseteq ...$, and FSOC suppose each step is strict inclusion. Then $f_0 = f_1 g$ where g is nonunit. If $\deg g = 0$, then the collection of irreducible factors (up to associates) of leading coefficient of f_1 is a proper subset of the collection of irreducible factors (up to associates) of leading coefficient of f_0. Because the leading coefficient of f_0 has only finitely many irreducible factors, we conclude that $\exists k$ such that $\deg f_k < \deg f_0$. Continue the same argument, we see that $\forall n \geq 0$, $\exists m$ such that $\deg f_m < \deg f_0 - m$, impossible. Therefore, a.c.c. holds for principal ideals of $A[x]$.
Next take any irreducible $f(x) \in A[x]$. Note then f is primitive, i.e. content of f is trivial. Suppose $gh \in (f)$ for some $g, h \in A[x]$. By Gauss's Lemma and its corollary, $f(x)$ is irreducible in $K(A)[x]$ where $K(A)$ is the field of fraction of A. We already showed PID is UFD, and $K(A)[x]$ is PID, and irreducibles are primes in UFD, thus $f(x)$ is a prime element in $K(A)[x]$. Then WLOG $g = f\varphi$ where $\varphi \in K(A)[x]$. Obviously $\exists a \in A$ such that $a\varphi \in A[x]$ (for example, let a be lcm of denominators of coefficients of φ). Then $ag = f \cdot (a\varphi)$. Taking content on both sides, $(a)(cont_g) = (cont_f)(cont_{a\varphi}) = (cont_{a\varphi})$. This tells us that φ must be in $A[x]$ to begin with, otherwise the equation cannot be true. Thus $f|g$ in $A[x]$ and f is prime.
Above all, $A[x]$ is an UFD.

Ex.2.2.11. If $1/3$ is integral over $\mathbb{Z}$, then take the monic polynomial f with integer coefficients which kill $1/3$, say $f = \sum_{i=0}^{n} a_i x^i$ where $a_n = 1$. Then $0 = 3^n f(1/3) = \sum_{i=0}^{n} a_i \cdot 3^{n-i} = 1 + \sum_{i=0}^{n-1} a_i \cdot 3^{n-i}$, but this implies $3|1$, contradiction.
$(1+\sqrt{17})/2$ is integral over $\mathbb{Z}$ because it is a root of the monic polynomial with integer coefficients: $x^2 - x - 4 \in \mathbb{Z}[x]$.

Ex2.2.13(1). $A \subseteq \tilde{A} \subseteq B$, since $\forall a \in A$, a is killed by $x - a \in A[x]$. In particular $1 \in \tilde{A}$. Take any $b_1, b_2 \in \tilde{A}$, we want to prove $b_1 - b_2 \in \tilde{A}$ and $b_1 b_2 \in \tilde{A}$. It suffices to prove any element $x \in A[b_1, b_2]$ is integral over A. Note $A[b_1, b_2]$ is finitely generated as $A[b_1]$-module because $A[b_2]$ is finitely generated as A-module by Lemma 2.2.12. Again by Lemma 2.2.12, $A[b_1]$ is finitely generated as A-module. Call a (finite) set of generators of $A[b_1, b_2]$ over $A[b_1]$ by S_1, and call a (finite) set of generators of $A[b_1]$ over A by S_2, then $S_1 S_2$ is a finite set of generators of $A[b_1, b_2]$ as A-module.
Let $m_1, ..., m_n$ be generators of $A[b_1, b_2]$ as A-module. Then $x \cdot m_i = \sum_{j=1}^{n} a_{ij} m_j$ for some coefficients $(a_{ij})_{1 \leq i,j \leq n}$ in A.

Let M be a n-by-n matrix with coefficients in A where $M_{ij} = a_{ij}$. Then $Mv = xv$ where $v = \begin{pmatrix} m_1 \\ .. \\ .. \\ .. \\ m_n \end{pmatrix}$ and xv uses scalar multiplication where we view $A[b_1, b_2]$ as an $A[x]$-module. Let $f \in A[t]$ be the characteristic polynomial of M. Note f is monic. Then $f(x)v = (f(M))v = 0v = 0$ where the second step is true by Cayley-Hamilton. This means $\forall 1 \leq i \leq n$, $f(x)m_i = 0$, so $f(x)u = 0$ $\forall u \in A[b_1, b_2]$. In particular, $f(x) \cdot 1 = 0$, so x is integral over A.

Remark 1: we have proved that for any ring extension $A \subseteq B$, if B is finitely generated as A-module, then B is integral over A.

Ex.2.2.13(2). The reverse direction follows from the previous remark. The positive direction follows from noticing that any large power of b_i can be replaced by a sum of smaller powers of b_i using a polynomial $p \in A[x]$ which kills b_i.

Ex.2.2.16(1) (This exercise reminds me of the similar result for algebraic field extension.) Take any $c \in C$. Then $p(c) = 0$ for some $p(x) \in B[x]$. Let $b_0, ..., b_{n-1}$ be coefficients of $p(x)$. By Ex.2.2.13(2), $A[b_0, ..., b_{n-1}]$ is finitely generated A-module. Let S_1 be a set of generators. Because c is integral over $A[b_0, ..., b_{n-1}]$, $A[b_0, ..., b_{n-1}, c]$ is finitely generated as $A[b_0, ..., b_{n-1}]$-module. Let S_2 be a set of generators. Then $A[b_0, ..., b_{n-1}, c]$ is finitely generated as A-module by $S_1 S_2$. So by Remark 1, $A[b_0, ..., b_{n-1}, c]$ is integral over A. In particular, c is integral over A, so C is integral over A.
(2) Let $\tilde{\tilde{A}}$ be integral closure of $\tilde{A}$ in B. By part (1), $\tilde{\tilde{A}}$ is integral over A. Thus $\tilde{\tilde{A}} \subseteq \tilde{A}$ by definition of integral closure. So $\tilde{\tilde{A}} = \tilde{A}$.

(3) If $\frac{p}{q} \in \mathbb{Q}$ where p, q are relatively prime is killed by some monic polynomial $f(x) \in \mathbf{Z}[x]$ of degree n, then $q^n f(\frac{p}{q}) = 0$ implies $q|p$, so $q = \pm 1$, so $\frac{p}{q} \in \mathbb{Z}$. So $\mathbb{Z}$ is integrally closed.
(4) The same proof as (3).

Ex.2.3.4 $\frac{1}{2}$, and in fact any rational number which is not integer, because $\mathbb{Z}$ is integrally closed.

Ex.2.3.5 Because K is finite extension of $\mathbb{Q}$, K is algebraic over $\mathbb{Q}$, so $\exists p(x) \in \mathbb{Q}[x]$ monic polynomial such that $p(\alpha) = 0$. Suppose $\deg p = n$. Multiply $p(x)$ by some integer to get $q(x) \in \mathbb{Z}[x]$. We still have $q(\alpha) = 0$. Next we will again multiply $q(x)$ by some integer and remove some power of each coefficient to get a monic polynomial killing $m\alpha$ for some $m > 0$. Denote the leading coefficient of $q(x)$ by a_n, and fix a prime integer p dividing a_n. Denote the power of p in the i-th coefficient of $q(x)$ by $k_{i,p}$. Let $m_p \in \mathbb{Z}_+$ be large enough such that $n|m_p + k_{n,p}$ and $\forall 1 \leq i \leq n-1, i \cdot \frac{m_p + k_{n,p}}{n} \leq k_{i,p} + m_p$. Such m_p obviously exists. Let $s = \prod_{p|a_n} p^{m_p}$, then $(sa_n)^{\frac{1}{n}} \in \mathbb{Z}$ and $(sa_n)^{\frac{1}{n}} \cdot \alpha$ is killed by the monic polynomial we get from $q(x)$ by multiplying s then dividing the i-th coefficient by $(sa_n)^{\frac{i}{n}}$. This polynomial has integer coefficients because of our choice of m_p. Because $\alpha = m\alpha \cdot \frac{1}{m}$, we see $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

Ex.2.3.7 $\forall \alpha, \beta \in K, c_1, c_2 \in F$, $m_{c_1\alpha + c_2\beta} = c_1 m_\alpha + c_2 m_\beta$, so $\operatorname{tr}_{K/F}(c_1\alpha + c_2\beta) = \operatorname{tr}(m_{c_1\alpha+c_2\beta}) = \operatorname{tr}(c_1 m_\alpha + c_2 m_\beta) = c_1 \operatorname{tr}(m_\alpha) + c_2 \operatorname{tr}(m_\beta) = c_1 \operatorname{tr}_{K/F}(\alpha) + c_2 \operatorname{tr}_{K/F}(\beta)$, so $\operatorname{tr}_{K/F} : K \to F$ is an F-linear map. $\forall \alpha, \beta \in K^\times$, $\det_{K/F}(\alpha\beta) = \det(m_{\alpha\beta}) = \det(m_\alpha \circ m_\beta) = \det(m_\alpha)\det(m_\beta) = \det_{K/F}(\alpha)\det_{K/F}(\beta)$. Note $\det_{K/F}(\alpha) \neq 0$ because $\det_{K/F}(\alpha)\det_{K/F}(\alpha^{-1}) = \det_{K/F}(1) = 1$. So $\det_{K/F} : K^\times \to F^\times$ is a group homomorphism.

Ex.2.4.4. By Proposition 2.3.8, $\operatorname{tr}_{K/F}(\alpha_i\alpha_j) = \sum_{\sigma \in \operatorname{Gal}(K/F)} \sigma(\alpha_i)\sigma(\alpha_j)$. Let $M = (\sigma_i(\alpha_j))_{ij}$, then $(M^t M)_{ij} = \sum_{k=1}^n (\sigma_k(\alpha_i))(\sigma_k(\alpha_j)) = \operatorname{tr}_{K/F}(\alpha_i\alpha_j)$. From linear algebra, $\det(M^t) = \det(M)$, so $d(\alpha_1, ..., \alpha_n) = \det(M)^2 = \det(M^t)\det(M) = \det(M^t M) = \det((\operatorname{tr}_{K/F}(\alpha_i\alpha_j))_{i,j})$. If $\alpha_i \in \mathcal{O}_K$, then $\operatorname{tr}_{K/F}(\alpha_i\alpha_j) \in \mathcal{O}_F$ by Corollary 2.3.10, so $d(\alpha_1, ..., \alpha_n) = \det((\operatorname{tr}_{K/F}(\alpha_i\alpha_j))_{i,j}) \in \mathcal{O}_F$, because $\mathcal{O}_F$ is a subring.

Ex.2.4.10. Pick any two integral bases of $\mathcal{O}_K$, $(\alpha_1, .., \alpha_n)$ and $(\beta_1, ..., \beta_n)$. Note $(\alpha)_i$ and $(\beta)_i$ are bases of K over $\mathbb{Q}$ by Ex.2.3.5. Let $M_1 = (\operatorname{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j}$ and $M_2 = (\operatorname{tr}_{K/\mathbb{Q}}(\beta_i\beta_j))_{i,j}$. Let $A = M(\mathrm{id}, (\alpha_1, ..., \alpha_n), (\beta_1, ..., \beta_n))$, i.e. the (i,j)-entry of A is coefficient of β_i in α_j when we write α_j as a linear combination of the β's. Then $M_1 = A^t M_2 A$. To see this, $(A^t M_2)_{i,k} = \operatorname{tr}_{K/\mathbb{Q}}(\alpha_i\beta_k)$ by linearity, so $(A^t M_2 A)_{i,j} = \operatorname{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)$, so $M_1 = A^t M_2 A$. Because $(\alpha)_i$ and $(\beta)_i$ are basis of the free $\mathbb{Z}$-module $\mathcal{O}_K$, A has integer-coefficients. A is invertible, so $\det A \in \mathbb{Z}^\times$, so $\det A = \pm 1$. So $\det M_1 = \det(M_2)(\det A)^2 = \det(M_2)$. So the discriminant of K is well-defined.

Ex.2.4.12. First, $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} \supseteq \{a + b\sqrt{D} | a, b \in \mathbb{Z}\}$, because $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is a subring of $\mathbb{Q}(\sqrt{D})$ containing $\mathbb{Z}$ and $\sqrt{D}$ (as $x^2 - D \in \mathbb{Z}[x]$ kills $\sqrt{D}$). We claim that

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \{a + b\sqrt{D} | a, b \in \mathbb{Z}\} & \text{if } D \equiv 2, 3 \mod 4 \\ \{\frac{a + b\sqrt{D}}{2} | a, b \in \mathbb{Z}, a \equiv b \mod 2\} & \text{if } D \equiv 1 \mod 4 \end{cases} \tag{1}$$

First we verify $\supseteq$ direction. The $\supseteq$ in the first line is true by previous comment. It is easy to verify that the second line of (1) is indeed a subring. To see containment, $x^2 - ax + \frac{a^2 - b^2 D}{4}$ kills $\frac{a + b\sqrt{D}}{2}$ by quadratic formula, and $a^2 - b^2 D \equiv 0 \mod 4$ because a and b have the same parity and $D \equiv 1 \mod 4$. Next we verify $\subseteq$ direction. Suppose a and b are rational numbers and $a + b\sqrt{D}$ is killed by some monic polynomial with integer coefficients $p(x)$. If $a + b\sqrt{D} \in \mathbb{Q}$ then because $\mathbb{Z}$ is integrally closed, $a + b\sqrt{D} \in \mathbb{Z}$ which is contained in the RHS of (1). So assume $a + b\sqrt{D} \notin \mathbb{Z}$, then because $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is a quadratic extension, minimal polynomial of $a + b\sqrt{D}$ over $\mathbb{Q}$ has degree 2, let $q(x)$ be this minimal polynomial. Then $q(x)|p(x)$. Because $p(x) \in \mathbb{Z}$ and both $p(x)$ and $q(x)$ are monic, comparing content by Gauss's Lemma we get $q(x) \in \mathbb{Z}[x]$. Suppose $q(x) = x^2 + c_1 x + c_0$. By quadratic formula, roots of $q(x)$ are $\frac{-c_1 \pm \sqrt{c_1^2 - 4c_0}}{2}$. If $c_1^2 - 4c_0 \equiv 0 \mod 4$, then c_1 is even, so if $c_1^2 - 4c_0 \geq 0$ then roots of $q(x)$ are integers, so $a + b\sqrt{D} \in \mathbb{Z}$ is in the RHS of (1). If $c_1^2 - 4c_0 \equiv 0 \mod 4$ and $c_1^2 - 4c_0 < 0$, then roots of $q(x)$ are of form $a' + b'\sqrt{-1}$ for $a', b' \in \mathbb{Z}$, then $a' + b'\sqrt{-1} = a + b\sqrt{D}$, so compare the real and complex part we have $a = a' \in \mathbb{Z}$ and $b\sqrt{D} = b'\sqrt{-1}$. Taking square on the latter we get $b^2 D = -b'$. But D is square free, so b has to be an integer. So $a + b\sqrt{D}$ is in RHS of (1).

So we are left with the case where $c_1^2 - 4c_0 \equiv 1 \mod 4$, Then $a = \frac{-c_1}{2}$ and $b\sqrt{D} = \pm\frac{\sqrt{c_1^2 - 4c_0}}{2}$. Taking square on the latter equation and suppose $b = \frac{b_1}{b_0}$ where $(b_1, b_0) = 1, b_0 > 0$ we get

$$4b_1^2 D = b_0^2 c_1^2 - 4b_0^2 c_0^2 \tag{2}$$

Then $b_0^2 | 4D$, and D is square free, so $b_0 = 1$ or $b_0 = 2$. If $b_0 = 1$ then $b \in \mathbb{Z}$ and the equation becomes $4b_1^2 D = c_1^2 - 4c_0^2$. Moding both sides by 4 we see c_1 is even, so $a = \frac{-c_1}{2} \in \mathbb{Z}$, so $a + b\sqrt{D}$ is in the RHS of (1). Therefore, assume $b_0 = 2$, and (2) becomes $b_1^2 D = c_1^2 - 4c_0^2$. Also, because $(b_1, b_0) = 1$, b_1 is odd and thus $b_1^2 \equiv 1 \mod 4$. Moding both sides by 4, we get $D \equiv c_1^2 \mod 4$. Now this is impossible if $D \equiv 2, 3 \mod 4$, so we must have $D \equiv 1 \mod 4$, then c_1 is odd. Thus, $a + b\sqrt{D} = \frac{-c_1}{2} + \frac{b_1}{2}\sqrt{D}$ where c_1, b_1 are odd, so $a + b\sqrt{D}$ is in the RHS of (1).
Above all, we have shown that (1) holds. When $D \equiv 2, 3 \mod 4$, an integral basis for $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is $(1, \sqrt{D})$. Because $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is a Galois extension where the only two automorphisms over $\mathbb{Q}$ are identity and the one sending $\sqrt{D}$ to its negative, $d_{\mathbb{Q}(\sqrt{D})} = d(1, \sqrt{D}) = \det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^2 = 4D$. When $D \equiv 1 \mod 4$, it's easy to verify that an integral basis for $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is $(\frac{1+\sqrt{D}}{2}, \frac{1-\sqrt{D}}{2})$. Then $d_{\mathbb{Q}(\sqrt{D})} = d(\frac{1+\sqrt{D}}{2}, \frac{1-\sqrt{D}}{2}) = \det \begin{pmatrix} \frac{1+\sqrt{D}}{2} & \frac{1-\sqrt{D}}{2} \\ \frac{1-\sqrt{D}}{2} & \frac{1+\sqrt{D}}{2} \end{pmatrix}^2 = D$.

Ex.3.1.2. Suppose $7 = \alpha\beta$ for some $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, then $49 = N(7) = N(\alpha)N(\beta)$. So either $N(\alpha) = N(\beta) = 7$ or WLOG $N(\alpha) = 1$. $\forall a + b\sqrt{-5} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, $N(a + b\sqrt{-5}) = a^2 + 5b^2$, which cannot be equal to 7, so $N(\alpha) = 1$. If $\alpha = a + b\sqrt{-5}$ then $a^2 + 5b^2 = 1$, so $a = \pm 1$ and $b = 0$, so α is a unit, so 7 is irreducible. Similarly, suppose $1 \pm 2\sqrt{-5} = \alpha\beta$ for some $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, then $21 = N(1 \pm 2\sqrt{-5}) = N(\alpha)N(\beta)$. As explained before, 7 cannot be the norm of an element in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, so WLOG $N(\alpha) = 1$, then as explain before α is a unit, so $1 \pm 2\sqrt{-5}$ is irreducible.

Ex.3.2.2. (a) Prime ideals of $S = \prod_{i=1}^k R_i$ are of form $\prod_{i=1}^k \mathfrak{p}_i$ where all $\mathfrak{p}_i$ are R_i except one $\mathfrak{p}_i$ which is a prime ideal in R_i. First, it is easy to verify these are prime ideals. Conversely, let P by any prime ideal of S. Let e_i be the element whose i-th entry is 1 and other entries are 0. Then not all e_i can be in P because P is proper. WLOG assume $e_1 \notin P$. Then $\forall x \in \{0\} \times \prod_{i=2}^k R_i$, $e_1 x = 0 \in P$ so $x \in P$, so $\{0\} \times \prod_{i=2}^k R_i \subseteq P$. Let $\pi_1(P)$ denote the projection of P on the first factor. Then $\forall a_1 \in \pi_1(P)$, $\{a_1\} \times \prod_{i=2}^k R_i \subseteq P$, because we can first choose a $(a_1, ..., a_k) \in P$, then add by an element whose first coordinate is 0 to get whatever we want. Finally note that $\pi_1(P) \subseteq R_1$ satisfies all properties of a prime ideal in R_1 except that it may not be proper. But it has to be proper, otherwise $P = S$. So $P = \mathfrak{p}_1 \times \prod_{i=2}^k R_i$ where $\mathfrak{p}_1$ is a prime ideal of R_1. Then the statement of the problem follows.

(b) A field has Krull dimension 0 because the only prime ideal in a field is (0). Any integral domain with dimension 0 is a field, because if there is some nonzero nonunit element, then by Zorn's lemma there is a maximal ideal containing the ideal generated by that element, then because (0) is also a prime ideal, dimension of the integral domain is at least 1, contradiction.

(c) First we show that in a PID R, nonzero prime ideals are maximal ideals. Let $(p) \subset (R)$ be a nonzero prime ideal, and suppose $(a) \supseteq (p)$. Then $p = ab$ for some $b \in R$. Since (p) is prime, either $a \in (p)$ or $b \in (p)$. if $a \in (p)$, then $(a) \subseteq (p)$, so $(a) = (p)$. If $b \in (p)$, then $b = pc$ for some $c \in R$, and we have $p = pac$. Because p is nonzero and R is integral domain, we get $1 = ac$, so a is a unit, so $(a) = R$. Thus we have proved that in a PID, nonzero prime ideals are maximal. Then if R is a PID which is not a field, $\dim R \leq 1$ because if $\mathfrak{p}_1, \mathfrak{p}_2$ are nonzero prime ideals such that $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$, we must have $\mathfrak{p}_1 = \mathfrak{p}_2$. On the other hand, $\dim R \geq 1$ because we can take any nonzero nonunit element a, then by Zorn's lemma there is a maximal ideal $\mathfrak{m}$ containing (a), so $(0) \subset \mathfrak{m}$ is a chain of prime ideals.

Ex.3.2.4. Let R be a finite integral domain. Let $a \in R^\times$, then $\{a^n | n \geq 1\} \subseteq R^\times$ because product of nonzero elements is nonzero in integral domain. Because R is finite, $\exists n, m \geq 1$, $n > m$, such that $a^n = a^m$. Cancelling a^m on both sides we get $a^{n-m} = 1$, so a^{n-m-1} is the inverse of a and a is a unit.

Ex.3.2.6. Let R be a PID which is not a field. Then $\dim R = 1$ because every nonzero prime ideal (such ideal exists because R is not a field and by Zorn's lemma) is maximal (Indeed, if (p) is nonzero prime ideal and $(p) \subseteq (q)$, then $\exists r \in R$, $rq = p \in (p)$, so $r \in (p)$ or $q \in (p)$. $r \in (p)$ implies q is a unit so $q = R$. $q \in (p)$ implies r is a unit so $(q) = (p)$). R is obviously noetherian. R is integrally closed because any PID is UFD and UFD is integrally closed. Thus R is Dedekind domain.

Ex.3.3.3.(1) ($\Longrightarrow$) Pick a generating set $S = \{a_1, ..., a_n\}$. Let $r \in \mathcal{O}$ be the product of denominators of one representative of each a_i, then $ra_i \in \mathcal{O}$ for each i, so $r\mathfrak{a} \subseteq \mathcal{O}$. ($\Longleftarrow$) $\mathcal{O}$ is noetherian, so any $\mathcal{O}$-submodule of $\mathcal{O}$ is finitely generated. Since $r\mathfrak{a}$ is an $\mathcal{O}$-submodule of $\mathcal{O}$, $r\mathfrak{a}$ is finitely generated by some $\{a_1, ..., a_n\} \subseteq \mathcal{O}$ as an $\mathcal{O}$-module. Then $\mathfrak{a}$ is finitely generated by $\{\frac{a_1}{r}, ..., \frac{a_n}{r}\}$ as $\mathcal{O}$-module.
(2) Let I_1, I_2 be two fractional ideals with finite generating sets S_1, S_2. Then I_1, I_2 are $\mathcal{O}$-submodules of K, so $I_1 + I_2$ is an $\mathcal{O}$-submodule of K. $I_1 + I_2$ is obviously generated as $\mathcal{O}$-module by $S_1 \cup S_2$, so sum of two fractional ideals is fractional ideal. By definition of product of fractional ideals, an element of I_1I_2 is a finite sum of products of elements from I_1 and I_2, so I_1I_2 is obviously an $\mathcal{O}$-submodule of K. I_1I_2 is generated by S_1S_2 as an $\mathcal{O}$-module, because $S_1S_2 \subseteq I_1I_2$ and for any $a_1 \in I_1, a_2 \in I_2$, a_i can be written as an $\mathcal{O}$-linear combination of elements from S_i, so a_1a_2 is an $\mathcal{O}$-linear combination of elements from S_1S_2, so any element in I_1I_2 can be written as an $\mathcal{O}$-linear combination of elements from S_1S_2. Therefore, product of two fractional ideals is fractional ideal.

Ex.3.3.7. Take any $a \in (x\mathcal{O} : y\mathcal{O})$, then $a(y\mathcal{O}) \subseteq x\mathcal{O}$. So $\exists r \in \mathcal{O}$, $ay = xr$, so $a = \frac{x}{y}r \in (\frac{x}{y})\mathcal{O}$. Conversely, take any $a \in (\frac{x}{y})\mathcal{O}$. Then $a = \frac{x}{y}r$ for some $r \in \mathcal{O}$, so $ay = xr$. Then $a(y\mathcal{O}) = (ay)\mathcal{O} = (xr)\mathcal{O} \subseteq x\mathcal{O}$ because $r \in \mathcal{O}$. Thus $a \in (x\mathcal{O} : y\mathcal{O})$. The map $x \mapsto x\mathcal{O}$ also preserves multiplication, because $\forall x, y \in K$, elements of $(x\mathcal{O})(y\mathcal{O})$ are finite sum of products of elements from $(x\mathcal{O})$ and $(y\mathcal{O})$, and if $r_1, r_2 \in \mathcal{O}$, then $(xr_1)(yr_2) = (xy)(r_1r_2) \in (xy)\mathcal{O}$, so $(x\mathcal{O})(y\mathcal{O}) \subseteq (xy)\mathcal{O}$. $(x\mathcal{O})(y\mathcal{O}) \supseteq (xy)\mathcal{O}$ is obvious. But the map $x \mapsto x\mathcal{O}$ does not preserve addition. For example, let $\mathcal{O} = \mathbb{Z}$, then $(2+3)\mathbb{Z} = 5\mathbb{Z}$, but $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$.

Ex.3.3.13. The statement is: Any nonzero, nonunit integer can be written uniquely as a product of prime numbers, up to units and permutation. To prove this, first we prove existence. Let X be the set of nonzero, nonunit integers which cannot be written as a product of prime numbers. By the well-ordering principle (this corresponds to noetherian property), we can pick one such integer n with the least absolute value. n itself cannot be a prime number, so there exists some nonunit integer dividing n with smaller absolute value than n. Pick such integer with the least absolute value (we again use well-ordering principle, which replaces Zorn's lemma this time), call it p, then p is a prime number because of our choice. $\frac{n}{p}$ is nonunit and has smaller absolute value than n (this step is easy for $\mathbb{Z}$ but takes much more steps for a general Dedekind domain), so by our choice of n, $\frac{n}{p}$ is a product of prime numbers, then n is a product of prime numbers. Uniqueness follows because if p is prime, then $p|ab$ implies $p|a$ or $p|b$.
For a general PID, this argument does not work, because we do not have a natural "well-ordering principle" for general PID.

Ex.3.3.14.(1) First note that in Dedekind domain $\mathcal{O}$, if $I|J$ where I, J are ideals, then the exponent of each prime ideal in the prime factorization of I is less than or equal to that of J. The argument to prove this is similar to the proof of uniqueness of prime factorization. If $I = \prod_{i=1}^r \mathfrak{p}_i^{v_i}$ and $J = \prod_{i=1}^r \mathfrak{p}_i^{w_i}$, then $\gcd(I, J) = \prod_{i=1}^r \mathfrak{p}_i^{\min(v_i, w_i)}$ satisfies the property that $\gcd(I, J)|I, \gcd(I, J)|J$, and if $\mathfrak{a}$ is any ideal dividing I and J, we have $\mathfrak{a}|\gcd(I, J)$. But $I + J$ satisfies the same property, and it's easy to see that an ideal satisfying such property is unique. So $I + J = \gcd(I, J)$.
Similarly we define $\mathrm{lcm}(I, J) = \prod_{i=1}^r \mathfrak{p}_i^{\max(v_i, w_i)}$, then $\mathrm{lcm}(I, J)$ satisfies the property that $I|\mathrm{lcm}(I, J)$, $J|\mathrm{lcm}(I, J)$, and if $\mathfrak{a}$ is any ideal divided by I and J, we have $\mathrm{lcm}(I, J)|\mathfrak{a}$. It's easy to see that $I \cap J$ satisfies the same property and that an ideal satisfying such property is unique. Therefore $I \cap J = \mathrm{lcm}(I, J)$.

(2) Let I, J, K be nonzero ideals in Dedekind domain $\mathcal{O}$ and $n > 0$. If $\gcd(I, J) = \mathcal{O}$ and $IJ = K^n$, then there exist ideals K_1, K_2 such that $I = K_1^n$, $J = K_2^n$. Proof: Let $\mathfrak{p}$ be any prime ideal dividing K (If no such ideal exists, then $K = \mathcal{O}$ and we can set $K_1 = K_2 = \mathcal{O}$), then the exponent of $\mathfrak{p}$ in the prime factorization of IJ is a multiple of n. Because $\gcd(I, J) = \mathcal{O}$, I and J share no common prime factors, so these copies of $\mathfrak{p}$ all belong to I or J. Repeat this argument for all prime ideals dividing K and we finish the proof.

Ex.3.3.15. By property of fractional ideal, $\exists r \in \mathcal{O}$, $r \neq 0$ such that $r\mathfrak{a} \subseteq \mathcal{O}$. Then $r\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i$ where $\mathfrak{p}_i$ are not necessarily distinct prime ideals. Note $(r)\mathfrak{a} = r\mathfrak{a}$ where (r) is the principle ideal in $\mathcal{O}$ generated by r. Write $(r) = \prod_{i=1}^s \mathfrak{q}_i$ where $\mathfrak{q}_i$ are not necessarily distinct prime ideals, then $\mathfrak{a} \prod_{i=1}^s \mathfrak{q}_i = \prod_{i=1}^r \mathfrak{p}_i$, then $\mathfrak{a} = \frac{\prod_{i=1}^{r} \mathfrak{p}_i}{\prod_{i=1}^{s} \mathfrak{q}_i}$. We assume $\mathfrak{p}_i \neq \mathfrak{q}_j$ for all i, j by cancelling the same ideals on the fraction. Then such expression is unique, because for any two such expressions $\frac{\prod_{i=1}^{r} \mathfrak{p}_i}{\prod_{i=1}^{s} \mathfrak{q}_i} = \frac{\prod_{i=1}^{r'} \mathfrak{p}_i'}{\prod_{i=1}^{s'} \mathfrak{q}_i'}$, we can multiply by the product of their denominators on both sides to get $\prod_{i=1}^{r} \mathfrak{p}_i \prod_{i=1}^{s'} \mathfrak{q}_i' = \prod_{i=1}^{r'} \mathfrak{p}_i' \prod_{i=1}^{s} \mathfrak{q}_i$, then $\mathfrak{p}_1$ contains the RHS, and by property of prime ideals, p_1 equals one ideal on the RHS. Because $\mathfrak{p}_i, \mathfrak{q}_j$ are all distinct, $\mathfrak{p}_1 = \mathfrak{p}_1'$ after some reordering. Then we can cancel $\mathfrak{p}_1$ on both sides. Repeat the same argument, we see $r = r'$, $s = s'$, and $\mathfrak{p}_i = \mathfrak{p}_i'$, $\mathfrak{q}_i = \mathfrak{q}_i'$ for all i.

A proof that a Dedekind domain is UFD if and only if it is a PID: The reverse direction has been proved before and does not need the assumption of Dedekind domain. For the positive direction, let $I \subseteq \mathcal{O}$ be any ideal. Then $I = (a_1, ..., a_m)$ because $\mathcal{O}$ is noetherian. We claim that $I = (\gcd(a_1, ..., a_m))$ (gcd exists because $\mathcal{O}$ is a UFD). Indeed, I is a sum of ideals (a_i), and by Ex.3.3.14, sum of ideals is equal to gcd of these ideals. Using the other definition of gcd of ideals in terms of prime factorizations, we see that $I = (\gcd(a_1, ..., a_m))$.

Ex.4.1.2. Consider the composition $\varphi : \mathbb{Z} \hookrightarrow \mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/I$. Pick any nonzero $a \in I$, then there exists monic $p(x) \in \mathbb{Z}[x]$ such that $p(0) \neq 0$ and $p(a) = 0$. Then $p(0) \in \mathbb{Z} \cap I$, so $\ker \varphi$ is nontrivial. Then $\ker \varphi = (n)$ for some $n > 0$. Then we have an induced injection $\tilde{\varphi} : \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathcal{O}_K/I$. Because $\mathcal{O}_K$ has an integral basis, $\mathcal{O}_K/I$ is a finitely generated $\mathbb{Z}/n\mathbb{Z}$-module. But $\mathbb{Z}/n\mathbb{Z}$ is finite, so $\mathcal{O}_K/I$ is finite.

Ex.4.1.5. First view $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ as an $\mathcal{O}_k$-module, note that the action of $\mathfrak{p} \subseteq \mathcal{O}_k$ on any element of $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ is 0. In another word, using the equivalent definition of module structure, we have a ring homomorphism from $\mathcal{O}_k$ to $\mathrm{End}_{Ab}\mathfrak{p}^a/\mathfrak{p}^{a+1}$ whose kernel contains $\mathfrak{p}$, so we have an induced ring homomorphism from $k_\mathfrak{p}$ to $\mathrm{End}_{Ab}\mathfrak{p}^a/\mathfrak{p}^{a+1}$, so $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ is naturally a $k_\mathfrak{p}$-vector space. Next we show $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ is 1-dimensional. Pick any nonzero $[x] \in \mathfrak{p}^a/\mathfrak{p}^{a+1}$. Then $x \in \mathfrak{p}^a$ and $x \notin \mathfrak{p}^{a+1}$, so the power of $\mathfrak{p}$ in prime factorization of (x) is a. Then $\gcd((x), \mathfrak{p}^{a+1}) = \mathfrak{p}^a$. But we also know $\gcd((x), \mathfrak{p}^{a+1}) = (x) + \mathfrak{p}^{a+1}$, so $(x) + \mathfrak{p}^{a+1} = \mathfrak{p}^a$. Then for any $[y] \in \mathfrak{p}^a/\mathfrak{p}^{a+1}$, $\exists r \in \mathcal{O}_k, p \in \mathfrak{p}^{a+1}$ such that $xr + p = y$. So $(r + \mathfrak{p}) \cdot [x] = [y]$ where the dot means the action of $k_\mathfrak{p}$ on $\mathfrak{p}^a/\mathfrak{p}^{a+1}$. So $[x]$ spans $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ as a $k_\mathfrak{p}$-vector space. So $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ is 1-dimensional $k_\mathfrak{p}$-vector space and $|\mathfrak{p}^a/\mathfrak{p}^{a+1}| = |\mathcal{O}_k/\mathfrak{p}|$.

Ex.4.3.3. First define $\varphi : K \otimes_\mathbb{Q} \mathbb{C} \to \prod_\tau \mathbb{C}$ on pure tensors by $(\alpha \otimes c) \mapsto (\tau(\alpha) \cdot c)_\tau$. This map is bilinear, so it can be extended to the whole $K \otimes_\mathbb{Q} \mathbb{C}$. Because K is n-dimensional $\mathbb{Q}$-vector space, $K \otimes_\mathbb{Q} \mathbb{C}$ is n-dimensional $\mathbb{C}$-vector space, and φ respects multiplication by scalars from $\mathbb{C}$, so φ is a $\mathbb{C}$-linear map. Let $\alpha_1, ..., \alpha_n$ be a basis of K over $\mathbb{Q}$, then $\varphi(\alpha_i \otimes 1) = (\tau_j(\alpha_i))\tau_j$. The $(\tau_j(\alpha_i))$'s form a matrix, and its determinant squared is just the discriminant of $\alpha_1, ..., \alpha_n$, which is nonzero by Fact.2.4.5. Therefore, the vectors $(\varphi(\alpha_i \otimes 1))_i$ are linearly independent. There are n such vectors, and $\prod_\tau \mathbb{C}$ is n-dimensional $\mathbb{C}$-vector space, so φ is surjective. But $K \otimes_\mathbb{Q} \mathbb{C}$ is n-dimensional $\mathbb{C}$-vector space, so φ must be injective. Therefore, $K \otimes_\mathbb{Q} \mathbb{C} \cong \prod_\tau \mathbb{C}$ under φ as $\mathbb{C}$-vector spaces.

Ex.4.3.5.(a)$\langle Fx, Fy \rangle = \sum_\tau (Fx)_\tau \overline{Fy_\tau} = \sum_\tau \overline{x_{\overline{\tau}}}\, \overline{\overline{y_{\overline{\tau}}}} = \overline{\sum_\tau x_{\overline{\tau}} \overline{y_{\overline{\tau}}}} = \overline{\langle x, y \rangle}$
(b) Let $\varphi : K \otimes_\mathbb{Q} \mathbb{C} \to \prod_\tau \mathbb{C}$ be the map in the exercise 4.3.3. Then $\varphi^{-1} \circ F \circ \varphi(\alpha \otimes c) = \varphi^{-1} \circ F(\prod_\tau \tau(\alpha)c) = \varphi^{-1}(\prod_\tau \tau(\alpha)\overline{c}) = (\alpha \otimes \overline{c})$.

Ex.4.3.8. Because $x, y \in K_\mathbb{R}$, $\langle Fx, Fy \rangle = \langle x, y \rangle$. We showed in Ex.4.3.5(a) that $\langle Fx, Fy \rangle = \overline{\langle x, y \rangle}$, so $\langle x, y \rangle = \overline{\langle x, y \rangle}$.

Ex.4.3.10. Elements of $K_\mathbb{R}$ are those $x \in K_\mathbb{C}$ such that for each real embedding τ, x_τ is real, and for each complex embedding τ, $x_{\overline{\tau}} = \overline{x_\tau}$. Obviously for each $\alpha \in K$, $(\tau(\alpha))_\tau$ satisfies this condition.

Ex.4.3.14. Let $\tau_1, ..., \tau_r$ be the real embeddings, let $\tau_{r+1}, ..., \tau_{r+2s}$ be the complex embeddings where for each $1 \leq i \leq s$, τ_{r+i} and τ_{r+s+i} are complex conjugates. Assume the canonical isomorphism φ between $\mathbb{R}^n$ and $K_\mathbb{R}$ uses the coordinates of $K_\mathbb{R}$ indexed by $\tau_1, ..., \tau_{r+s}$. Then $X = \{(x_{\tau_1}, ..., x_{\tau_n}) \in K_\mathbb{R} | \forall 1 \leq i \leq r, -c\tau_i < x_{\tau_i} < c\tau_i, \forall r+1 \leq j \leq r+s, |x_{\tau_j}| < c_{\tau_j}\}$. Then under the canonical isomorphism φ, X is a line of length c_{τ_i} in the first r coordinates, and is a circle of radius $c_{\tau_{r+i}}$ in each consecutive 2 coordinates from the $(r+1)$-th coordinate to the $(r+2s)$-th coordinate. So $\mathrm{vol}_{lebesgue}(X) = (2c_{\tau_1})(2c_{\tau_2})...(2c_{\tau_r})(\pi c_{\tau_{r+1}}^2)...(\pi c_{\tau_{r+s}}^2) = 2^r \pi^s \prod_\tau c_\tau$ as $c_\tau = c_{\overline{\tau}}$. Then $\mathrm{vol}(X) = 2^s \mathrm{vol}_{lebesgue}(X) = 2^{r+s}\pi^s \prod_\tau c_\tau > 2^{r+s}\pi^s (2/\pi)^s \sqrt{|d_K|} N(I) = 2^n \mathrm{vol}(D_I)$.

Ex.4.4.2. If D is squarefree, then we know $d_{\mathbb{Q}(\sqrt{D})} = D$ if $D \equiv 1 \mod 4$ and $d_{\mathbb{Q}(\sqrt{D})} = 4D$ if $D \equiv 2, 3 \mod 4$. If $D > 0$, then $s = 0$, so we want $C_{\mathbb{Q}(\sqrt{D})} = \sqrt{|d_{\mathbb{Q}(\sqrt{D})}|} < 2$, so we want $|d_{\mathbb{Q}(\sqrt{D})}| < 4$, and the only possibility is $D = 1$. If $D < 0$, then $s = 1$, so we want $C_{\mathbb{Q}(\sqrt{D})} = (\frac{2}{\pi})\sqrt{|d_{\mathbb{Q}(\sqrt{D})}|} < 2$, so we want $|d_{\mathbb{Q}(\sqrt{D})}| < \pi^2$. $9 < \pi^2 < 10$, so the possibilities are $D = -1, -2, -3, -7$.
Therefore, when D is squarefree, $C_{\mathbb{Q}(\sqrt{D})} < 2$ if and only if $D = 1, -1, -2, -3$, or -7. In these cases, each class of fractional ideals in $\mathrm{Cl}_{\mathbb{Q}(\sqrt{D})}$ contains an ideal with absolute norm less than 2. Then the norm has to be 1, so the ideal is $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. So each fractional ideal is principal, and $h_{\mathbb{Q}(\sqrt{D})} = 1$.

Ex.4.4.6. Let $K = \mathbb{Q}(\sqrt{D})$ where $D \neq 1$ and D is squarefree integer.
When $D > 1$ and $D \equiv 1 \mod 4$, we have $s = 0$ and $d_K = D$, so $C'_K = \frac{1}{2}\sqrt{D} < 2$, so $D < 16$ and we get $D = 5, 13$.
When $D > 1$ and $D \equiv 2, 3 \mod 4$, we have $s = 0$ and $d_K = 4D$, so $C'_K = \frac{1}{2}\sqrt{4D} < 2$, so $D < 4$ and we get $D = 2, 3$.
When $D < 0$ and $D \equiv 1 \mod 4$, we have $s = 1$ and $d_K = D$, so $C'_K = \frac{1}{2}\frac{4}{\pi}\sqrt{-D} < 2$, so $D \geq -9$ and we get $D = -3, -7$.
When $D < 0$ and $D \equiv 2, 3 \mod 4$, we have $s = 1$ and $d_K = 4D$, so $C'_K = \frac{1}{2}\frac{4}{\pi}\sqrt{-4D} < 2$, so $D > -\frac{\pi^2}{4}$ and we get $D = -1, -2$.
Above all, $K = \mathbb{Q}(\sqrt{D})$ where $D = 2, 3, 5, 13, -1, -2, -3$, or -7. We see that using C'_K instead of C_K, we find more quadratic field with class number 1.

Ex.5.1.1. $1 \in \mathcal{O}_L$, so $\mathfrak{p}\mathcal{O}_L \supseteq \mathfrak{p}$ is nonzero. Then we prove $\mathfrak{p}\mathcal{O}_L$ is proper. Because Cl_K is finite, for any fractional ideal of $\mathcal{O}_K$, its certain power becomes principal fractional ideal. In particular, there exists $n \geq 1$ such that $\mathfrak{p}^n = a\mathcal{O}_K$ for some $a \in \mathcal{O}_K$. Obviously $a \neq 0$. Note that $(\mathfrak{p}\mathcal{O}_L)^n = \mathfrak{p}^n\mathcal{O}_L = (a\mathcal{O}_K)\mathcal{O}_L = a\mathcal{O}_L$. On one hand, we have $N(a\mathcal{O}_L) = N_{L/\mathbb{Q}}(a) = N_{K/\mathbb{Q}}(a)^{[L:K]} = N(a\mathcal{O}_K)^{[L:K]} > 1$ where the second step is true because $a \in K$, so we can consider determinant of $m_a : L \to L$ using a basis of $L/\mathbb{Q}$ consisting of $[L : K]$ "copies" of a fixed basis of $K/\mathbb{Q}$, each "copy" consisting of the basis of $K/\mathbb{Q}$ multiplied by a certain element from a basis of L/K. On the other hand, $N((\mathfrak{p}\mathcal{O}_L)^n) = N(\mathfrak{p}\mathcal{O}_L)^n$, so we must have $N(\mathfrak{p}\mathcal{O}_L) > 1$. That is, $\mathfrak{p}\mathcal{O}_L$ is proper.

Ex.5.1.3. $\dim \mathcal{O}_K = 1$, so $\mathfrak{p}$ is maximal, so $\mathcal{O}_K/\mathfrak{p}$ is a field, so $\mathcal{O}_L/\mathfrak{q}$ is a $\mathcal{O}_K/\mathfrak{p}$-vector space. As an $\mathcal{O}_K/\mathfrak{p}$-vector space, $\mathcal{O}_L/\mathfrak{q}$ is generated by classes of elements from a set of integral basis of $\mathcal{O}_L$, which is finite. So $\mathcal{O}_L/\mathfrak{q}$ is a finite dimensional $\mathcal{O}_K/\mathfrak{p}$-vector space. [Another way to see this is we know that $\mathcal{O}_L/\mathfrak{q}$ is a finite set. So $\mathcal{O}_L/\mathfrak{q}$ has to be a finite dimensional F-vector space for any base field F.]

Ex.5.1.6. First, restriction of nonzero prime ideals gives prime ideals, because inverse image of prime ideal under a ring homomorphism is prime ideal. Also, such prime ideal is nonzero, because it must contain some nonzero integer, for example by proof of Theorem 3.2.3.
Next, note that $\mathfrak{q}$ is the only prime ideal in $\mathcal{O}_L$ whose prime factorization in $\mathcal{O}_M$ has $\mathfrak{m}$. Indeed, if $\mathfrak{q}'$ is another prime ideal in $\mathcal{O}_L$ whose prime factorization in $\mathcal{O}_M$ contains $\mathfrak{m}$, then $\mathfrak{m} \supseteq \mathfrak{q}'$, so $\mathfrak{q} = \mathfrak{m} \cap \mathcal{O}_L \supseteq \mathfrak{q}'$, so $\mathfrak{q} = \mathfrak{q}'$ since $\dim \mathcal{O}_L = 1$.
We have $\mathfrak{p}\mathcal{O}_M = (\mathfrak{p}\mathcal{O}_L)\mathcal{O}_M$. Using the previous observation to count the exponent of $\mathfrak{m}$ on both sides gives $e_{\mathfrak{m}/\mathfrak{p}} = e_{\mathfrak{m}/\mathfrak{q}}e_{\mathfrak{q}/\mathfrak{p}}$.
We have field extensions $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q} \hookrightarrow \mathcal{O}_M/\mathfrak{m}$, so $[\mathcal{O}_M/\mathfrak{m} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_M/\mathfrak{m} : \mathcal{O}_L/\mathfrak{q}][\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$ by knowledge of field extensions. Thus $f_{\mathfrak{m}/\mathfrak{p}} = f_{\mathfrak{m}/\mathfrak{q}}f_{\mathfrak{q}/\mathfrak{p}}$.

Ex.5.1.8. First we note that K is indeed the fractional field of $\mathcal{O}_K$, because for any $a \in K$, $\exists n > 0$ such that $na \in \mathcal{O}_K$, then $a \in K(\mathcal{O}_K)$ (this denotes fractional field of $\mathcal{O}_K$) by multiplying n^{-1} to na. Conversely, the fractional field of $\mathcal{O}_K$ can be embedded in K by the universal property of fractional field.
Next, assume for some i, $a_i \neq 0$, then the $\mathcal{O}_K$-submodule of K generated by $a_1, ..., a_m$, denoted by $(a_1, ..., a_m)$, is nonzero, so it has an inverse (which is also a fractional ideal) denoted by $(a_1, ..., a_m)^{-1}$ such that $(a_1, ..., a_m)(a_1, ..., a_m)^{-1} = \mathcal{O}_K$. There must be some element $c \in (a_1, ..., a_m)^{-1}$ such that $ca_j \notin \mathfrak{p}$ for some j. Otherwise, because $(a_1, ..., a_m)(a_1, ..., a_m)^{-1}$ is an $\mathcal{O}_K$-module generated by elements of form $(\sum_{i=1}^m r_i a_i)c$ where $r_i \in \mathcal{O}_K$ and $c \in (a_1, ..., a_m)^{-1}$, we see $(a_1, ..., a_m)(a_1, ..., a_m)^{-1} \subseteq \mathfrak{p}$, contradiction. So $\exists c \in (a_1, ..., a_m)^{-1}$ such that $ca_j \notin \mathfrak{p}$ for some j. Furthermore, $\forall i$, $ca_i \in \mathcal{O}_K$ because

$(a_1,...,a_m)(a_1,...,a_m)^{-1} = \mathcal{O}_K$.

Ex.5.2.3. First we verify C_α is an ideal of $\mathcal{O}_L$. $\forall x, y \in C_\alpha$, $\forall c \in \mathcal{O}_L$, $(x-y)c = xc - yc \in \mathcal{O}_K[\alpha]$. $\forall x \in C_\alpha, r \in \mathcal{O}_L$, $rx\mathcal{O}_L = x(r\mathcal{O}_L) \subseteq x\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$. So C_α is an ideal of $\mathcal{O}_L$. $C_\alpha \subseteq \mathcal{O}_K[\alpha]$ because $\forall x \in C_\alpha$, $x = x \cdot 1 \in x\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$. Let I be any ideal of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\alpha]$. Then $\forall c \in I$, $c\mathcal{O}_L \subseteq I \subseteq \mathcal{O}_K[\alpha]$, so $c \in C_\alpha$. So $I \subseteq C_\alpha$, and we see C_α is the largest ideal of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\alpha]$.

Ex.5.2.10. First assume $D \equiv 2,3 \mod 4$. Then by a previous exercise we know $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$. The minimal polynomial of $\sqrt{D}$ over $\mathbb{Q}$ is $q = x^2 - D$. View q as a polynomial in $\mathbb{F}_p[x]$, then q is reducible if and only if D is a square mod p. When D is not a square mod p, by Theorem 5.2.5, $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, with inertia degree 2. When D is a square mod p, say $a^2 \equiv D \mod p$, then $x^2 - D = (x+a)(x-a)$ over $\mathbb{F}_p$. If $p|D$, then $p|a$, so $x^2 - D = x^2$, so $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (p, \sqrt{D})^2$ is the factorization into prime ideals, with inertia degree 1. If $p \nmid D$ and $p = 2$, then $x^2 - D = (x+1)^2$, so $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (p, \sqrt{D}+1)^2$ is the factorization into prime ideals, with inertia degree 1. If $p \nmid D$ and $p \neq 2$, then $a \neq -a \mod p$, so $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (p, \sqrt{D}+a)(p, \sqrt{D}-a)$ is the factorization into prime ideals, both with inertia degree 1.
Then assume $D \equiv 1 \mod 4$. Then by a previous exercise we know $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. The minimal polynomial of $\frac{1+\sqrt{D}}{2}$ over $\mathbb{Q}$ is $q = x^2 - x + \frac{1-D}{4}$. View q as a polynomial in $\mathbb{F}_p[x]$, then q is reducible if and only if $x^2 - x + \frac{1-D}{4}$ has a root over $\mathbb{F}_p$ if and only if D is the square of an odd integer mod p. Thus, if D is not the square of an odd integer mod p, $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, with inertia degree 2. If D is the square of an odd integer mod p, say $(2a-1)^2 \equiv D \mod p$, then over $\mathbb{F}_p$, $x^2 - x + \frac{1-D}{4} = (x-a)(x+a-1)$. If $p|D$, then $x^2 - x + \frac{1-D}{4} = (x-a)^2$, so $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (p, \frac{1+\sqrt{D}}{2} - a)^2$ is the factorization into prime ideals, with inertia degree 1. If $p \nmid D$, then $x - a$ and $x + a - 1$ are distinct irreducible polynomials over $\mathbb{F}_p$, so $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (p, \frac{1+\sqrt{D}}{2} - a)(p, \frac{1+\sqrt{D}}{2} + a - 1)$ is the factorization into prime ideals, with inertia degree 1.

so $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = (p, \frac{1+\sqrt{D}}{2} - a)(p, \frac{1+\sqrt{D}}{2} + a - 1)$ is the factorization into prime ideals, and inertia degree of both prime ideals over p is 1.

Ex.5.3.2. (1)Elements of $\sigma(\mathfrak{ab})$ have form $\sum_i \sigma(a_i)\sigma(b_i)$ where $a_i \in \mathfrak{a}, b_i \in \mathfrak{b}$, which are exactly elements of $\sigma(\mathfrak{a})\sigma(\mathfrak{b})$.
(2) $\sigma(\mathfrak{q})$ is indeed an ideal of $\mathcal{O}_L$: it is contained in $\mathcal{O}_L$ because $\sigma(\mathcal{O}_L) = \mathcal{O}_L$; it is obvious that $\sigma(\mathfrak{q})$ is a subgroup under addition; $\forall r \in \mathcal{O}_L, \forall q \in \mathfrak{q}$, $r\sigma(q) = \sigma(\sigma^{-1}(r)q) \in \sigma(\mathfrak{q})$ because $\sigma^{-1}(r) \in \mathcal{O}_L$. $\sigma(\mathfrak{q})$ is proper in $\mathcal{O}_L$ because if $\sigma(\mathfrak{q}) = \mathcal{O}_L$, then $\mathfrak{q} = \sigma^{-1}(\sigma(\mathfrak{q})) = \sigma^{-1}(\mathcal{O}_L) = \mathcal{O}_L$. Finally if $a, b \in \mathcal{O}_L$ and $ab \in \sigma(\mathfrak{q})$, then $\sigma^{-1}(a)\sigma^{-1}(b) \in \mathfrak{q}$, so $\sigma^{-1}(a) \in \mathfrak{q}$ or $\sigma^{-1}(b) \in \mathfrak{q}$, so $a \in \sigma(\mathfrak{q})$ or $b \in \sigma(\mathfrak{q})$. So $\sigma(\mathfrak{q})$ is a prime ideal of $\mathcal{O}_L$.
(3) If $\mathfrak{q}|\mathfrak{p}\mathcal{O}_L$, then $\sigma(\mathfrak{q}) \supseteq \sigma(\mathfrak{p}\mathcal{O}_L)$. Any element of $\mathfrak{p}\mathcal{O}_L$ can be written as $\sum_i p_i r_i$ where $p_i \in \mathfrak{p}$, $r_i \in \mathcal{O}_L$, and $\sigma(\sum_i p_i r_i) = \sum_i p_i \sigma(r_i) \in \mathfrak{p}\mathcal{O}_L$ because σ fixes K, so $\sigma(\mathfrak{p}\mathcal{O}_L) \subseteq \mathfrak{p}\mathcal{O}_L$. Applying the same argument using σ^{-1} shows $\mathfrak{p}\mathcal{O}_L \subseteq \sigma(\mathfrak{p}\mathcal{O}_L)$, so $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$. So $\sigma(\mathfrak{q}) \supseteq \mathfrak{p}\mathcal{O}_L$.
(4) Already showed in part (3).
(5) The identity of $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ obviously fixes $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ be the only nonidentity element. By part(3), $\sigma(\mathfrak{p}_1) = \mathfrak{p}_1$ or $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$. If $\sigma(\mathfrak{p}_1) = \mathfrak{p}_1$, then $\mathfrak{p}_1 \subseteq \mathbb{Q}$ because $\mathfrak{p}_1$ is fixed by the whole Galois group. But this is impossible because $\mathfrak{p}_1 \supseteq 2\mathcal{O}_{\mathbb{Q}(\sqrt{D})} \ni 2\sqrt{D}$. So $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$. Similarly, $\sigma(\mathfrak{p}_2) = \mathfrak{p}_1$.

Ex.5.3.8. Let S denote the set of all prime ideals on $\mathcal{O}_L$ dividing $\mathfrak{p}\mathcal{O}_K$. We know that G acts on S transitively, and for a fixed $\mathfrak{q} \in S$, $D_\mathfrak{q}$ is the stabilizer subgroup of G fixing $\mathfrak{q}$. Pick any $\mathfrak{q}_1, \mathfrak{q}_2 \in S$, then there exists $\sigma \in G$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. By group theory, we know $\sigma D_{\mathfrak{q}_1}\sigma^{-1} = D_{\mathfrak{q}_2}$. Also by group theory (Orbit-Stabilizer Theorem), we have G-set isomorphism $\frac{G}{D_\mathfrak{q}} \cong S$ for any $\mathfrak{q} \in S$ ($\frac{G}{D_\mathfrak{q}}$ is not necessarily a group, but is a set of left cosets of $D_\mathfrak{q}$ in G with the natural left action of G). So $[G : D_\mathfrak{q}] = |S| = g_\mathfrak{p}$, and $|D_\mathfrak{q}| = \frac{|G|}{g_\mathfrak{p}} = \frac{n}{g_\mathfrak{p}} = e_\mathfrak{p} f_\mathfrak{p}$.

Ex.5.3.13. First, some calculation of degree of field extension. By Galois theory, $[G : I_\mathfrak{q}] = [L^{I_\mathfrak{q}} : K]$, and we know $|I_\mathfrak{q}| = e_\mathfrak{p}$, so $[L^{I_\mathfrak{q}} : K] = f_\mathfrak{p} g_\mathfrak{p}$. By the same argument, $[L^{D_\mathfrak{q}} : K] = g_\mathfrak{p}$ so $[L^{I_\mathfrak{q}} : L^{D_\mathfrak{q}}] = f_\mathfrak{p}$. And $[L : L^{I_\mathfrak{q}}] = [L : K]/[L^{I_\mathfrak{q}} : K] = e_\mathfrak{p}$.
Let $\mathfrak{q}'' := \mathfrak{q} \cap \mathcal{O}_{L^{I_\mathfrak{q}}}$. We prove $k_\mathfrak{q} = k_{\mathfrak{q}''}$. The decomposition subgroup of $\mathrm{Gal}(L/L^{I_\mathfrak{q}})$ at $\mathfrak{q}$ is $\mathrm{Gal}(L/L^{I_\mathfrak{q}}) = I_\mathfrak{q}$ itself, because $I_\mathfrak{q} \subseteq D_\mathfrak{q}$. By Theorem 5.3.10 we have surjection $I_\mathfrak{q} \to \mathrm{Gal}(k_\mathfrak{q}/k_{\mathfrak{q}''})$. The kernel of this map is also $I_\mathfrak{q}$, because $\forall \sigma \in I_\mathfrak{q}, \forall \overline{a} \in k_\mathfrak{q}$, $\overline{\sigma}(\overline{a}) = \overline{a}$. So we have $|\mathrm{Gal}(k_\mathfrak{q}/k_{\mathfrak{q}''})| = 1$, so $k_\mathfrak{q} = k_{\mathfrak{q}''}$ and $f_{\mathfrak{q}/\mathfrak{q}''} = 1$.

Note $\mathfrak{q}$ is the only prime dividing $\mathfrak{q}''\mathcal{O}_L$ because the action of $\mathrm{Gal}(L/L^{I_\mathfrak{q}})$ on the set of primes dividing $\mathfrak{q}''\mathcal{O}_L$ is transitive and all elements of $\mathrm{Gal}(L/L^{I_\mathfrak{q}})$ fix $\mathfrak{q}$. Then apply the degree counting formula to $L/L^{I_\mathfrak{q}}$ to get $e_\mathfrak{p} = e_{\mathfrak{q}/\mathfrak{q}''}f_{\mathfrak{q}/\mathfrak{q}''} = e_{\mathfrak{q}/\mathfrak{q}''}$. So $\mathfrak{q}''$ is totally ramified with ramification index $e_\mathfrak{p}$. And this directly implies $e_{\mathfrak{q}''/\mathfrak{q}'} = 1$ because $e_\mathfrak{p} = e_{\mathfrak{q}/\mathfrak{q}''}e_{\mathfrak{q}''/\mathfrak{q}'}$.
Next, note $L^{I_\mathfrak{q}}/L^{D_\mathfrak{q}}$ is Galois because $I_\mathfrak{q}$ is normal in $D_\mathfrak{q}$ (since it is a kernel). Apply degree counting formula to $L^{I_\mathfrak{q}}/L^{D_\mathfrak{q}}$ we get $f_\mathfrak{p} = e_{\mathfrak{q}''/\mathfrak{q}'}f_{\mathfrak{q}''/\mathfrak{q}'}g_{\mathfrak{q}'} = f_{\mathfrak{q}''/\mathfrak{q}'}g_{\mathfrak{q}'}$. By previous paragraph, $f_\mathfrak{p} = f_{\mathfrak{q}''/\mathfrak{q}'}$. So we see $g_{\mathfrak{q}'} = 1$, so $\mathfrak{q}''$ is the only prime dividing $\mathfrak{q}'\mathcal{O}_{L^{I_\mathfrak{q}}}$. We also know $e_{\mathfrak{q}''/\mathfrak{q}'} = 1$, so $\mathfrak{q}'\mathcal{O}_{L^{I_\mathfrak{q}}} = \mathfrak{q}''$. Thus we see that $\mathfrak{q}'$ is inert in $\mathcal{O}_{L^{I_\mathfrak{q}}}$ with inertia degree $f_\mathfrak{p}$.

Ex.5.4.2. Under the isomorphism, we have $\overline{\sigma_\mathfrak{q}}(\overline{x}) = (\overline{x})^{\# k_\mathfrak{p}}$ for any $\overline{x} \in k_\mathfrak{q}$, so $\sigma_\mathfrak{q}(x) \equiv x^{\# k_\mathfrak{p}} \mod \mathfrak{q}$ for any $x \in \mathcal{O}_L$. For uniqueness, suppose $\tau \in D_\mathfrak{q}$ also satisfies $\tau(x) \equiv x^{\# k_\mathfrak{p}} \mod \mathfrak{q}$ for all $x \in \mathcal{O}_L$. Then $\overline{\tau}(\overline{x}) = (\overline{x})^{\# k_\mathfrak{p}}$ for all $\overline{x} \in k_\mathfrak{q}$, so $\overline{\tau} = \overline{\sigma_\mathfrak{q}}$. Under the isomorphism, $\tau = \sigma_\mathfrak{q}$.

Ex.5.4.6. First note that by Ex.5.2.10, when $p \nmid d_{\mathbb{Q}(\sqrt{D})}$, $(p) \subset \mathbb{Z}$ is unramified in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, and $p\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is product of two distinct prime ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, both with inertia degree 1. Then $|\mathrm{Gal}(k_\mathfrak{q}/k_{(p)})| = [k_\mathfrak{q} : k_{(p)}] = f_{\mathfrak{q}/(p)} = 1$, so $D_\mathfrak{q}$ is the trivial subgroup of $\mathrm{Gal}(L/K)$. So $(\frac{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}{(p)}) = \mathrm{id}_L$.

Ex.6.1.3.(1) We first verify that the relation introduced in Definition 6.1.1. is equivalence relation. It is obvious that the relation is reflexive and symmetric. To prove transitivity, suppose $(a_1, s_1) \sim (a_2, s_2)$ and $(a_2, s_2) \sim (a_3, s_3)$. Then exists $s', s'' \in S$ such that $s'(a_1s_2 - a_2s_1) = 0$ and $s''(a_2s_3 - a_3s_2) = 0$. Multiply the first equation by $s''s_3$, multiply the second equation by $s's_1$, then add these two equations together we have $s's''s_2s_3a_1 - s''s's_1s_2a_3 = s's''s_2(a_1s_3 - a_3s_1) = 0$, so $(a_1, s_1) \sim (a_3, s_3)$. So "$\sim$" is an equivalence relation. We define addition and multiplication in $S^{-1}A$ by $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1s_2+a_2s_1}{s_1s_2}$ and $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}$. Then we verify this is well defined. For addition, suppose $\frac{a_1}{s_1} = \frac{a_1'}{s_1'}$, then there exists $s \in S$ such that $s(a_1s_1' - a_1's_1) = 0$, then $s((a_1s_2 + a_2s_1)s_1's_2 - (a_1's_2 + a_2s_1')s_1s_2) = 0$ by some calculation, so addition is well defined. Similarly we can verify multiplication is well defined. Let the multiplicative identity be $\frac{1}{1}$ and additive identity be $\frac{0}{1}$, then it is obvious that $S^{-1}A$ satisfies axioms of a commutative ring. The map from A to $S^{-1}A$ given by $a \mapsto \frac{a}{1}$ is obviously a ring homomorphism.
(2) If $0 \in S$, then for any $\frac{a}{s} \in S^{-1}A$, because $0(a \cdot 1 - 0 \cdot s) = 0$, $\frac{a}{s} = \frac{0}{1}$. So $S^{-1}A = 0$. Conversely if $S^{-1}A = 0$, then $\frac{0}{1} = \frac{1}{1}$, so there exists $s \in S$, $s = s(0 \cdot 1 - 1 \cdot 1) = 0$.
(3) If $\frac{a_1}{s_1} = \frac{a_2}{s_2}$, then there exists $u \in S$ such that $u(a_1s_2 - a_2s_1) = 0$. Since we assume $0 \notin S$, $u \neq 0$. And A is integral domain, so $a_1s_2 - a_2s_1 = 0$, so we can take $u = 1$. The canonical map $A \to S^{-1}A$ is injective, because if $\frac{a}{1} = \frac{0}{1}$ for some $a \in A$, then by our previous observation $a \cdot 1 - 0 \cdot 1 = 0$, so $a = 0$, so the kernel is trivial, so the map is injective.
(4) We have $\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{s} \cdot \frac{s}{1} = \frac{s}{s} = \frac{1}{1}$ where the last step is true because $1(s \cdot 1 - 1 \cdot s) = 0$, so $\frac{s}{1}$ is a unit.

Ex.6.1.5(1) If such a map $\tilde{\varphi}$ exists, then $\tilde{\varphi}(\frac{a}{s}) = \tilde{\varphi}(\frac{a}{1}) \cdot \tilde{\varphi}(\frac{1}{s}) = \tilde{\varphi}(\frac{a}{1}) \cdot \tilde{\varphi}(\frac{s}{1})^{-1} = \varphi(a)\varphi(s)^{-1}$. Note $\varphi(s)$ is invertible by assumption. So we have uniqueness. This function $\tilde{\varphi}$ is well defined, because if $\frac{a}{s} = \frac{a'}{s'}$ then there exists $s'' \in S$ such that $s''(as' - a's) = 0$. Apply φ we have $\varphi(s'')\varphi(as' - a's) = 0$. But $\varphi(s'')$ is a unit, so we can multiply by its inverse to get $\varphi(as' - a's) = 0$. Then $\varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1}$, so $\tilde{\varphi}$ is well defined. It is easy to verify that $\tilde{\varphi}$ is a ring homomorphism that makes the diagram commute. So we have existence.
(2) Let S_1 be the set of prime ideals of A contained in $A \setminus S$. Let S_2 be the set of prime ideals of $S^{-1}A$. Let $f : S_1 \to S_2$ be the function introduced in problem statement. We first verify f is well defined. Pick any $\mathfrak{p} \in S_1$, Then $f(\mathfrak{p})$ is a proper subset of $S^{-1}A$, because if $\frac{1}{1} = \frac{p}{s}$ for some $p \in \mathfrak{p}, s \in S$, then there exists $s' \in S$ such that $s'(p - s) = 0$, so $s' \in \mathfrak{p}$ or $s \in \mathfrak{p}$, impossible since $\mathfrak{p} \cap S = \emptyset$. It is straightforward to see that $f(\mathfrak{p})$ is an ideal of $S^{-1}A$. To see it is prime ideal, suppose $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{p}{s_3} \in f(\mathfrak{p})$, then there exists $s \in S$ such that $s(a_1a_2s_3 - ps_1s_2) = 0$. Because $\mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \emptyset$, $a_1 \in \mathfrak{p}$ or $a_2 \in \mathfrak{p}$, so $\frac{a_1}{s_1} \in f(\mathfrak{p})$ or $\frac{a_2}{s_2} \in f(\mathfrak{p})$, so $f(\mathfrak{p})$ is prime ideal. Conversely, let $g : S_2 \to S_1$ be $g(\mathfrak{q}) = \iota^{-1}(\mathfrak{q})$ where ι is the canonical map from A to $S^{-1}A$. Because inverse image of prime ideal is still prime ideal, we only need to verify $g(\mathfrak{q}) \cap S = \emptyset$. FSOC, suppose $p \in g(\mathfrak{q} \cap S)$, then $\frac{p}{1} \in \mathfrak{q}$. But $\frac{p}{1}$ is a unit in $S^{-1}A$ because $p \in S$, so $\mathfrak{q} = S^{-1}A$. Contradiction with $\mathfrak{q}$ being a proper subset of $S^{-1}A$. So $g(\mathfrak{q}) \cap S = \emptyset$, so $g(\mathfrak{q}) \in S_1$. It is straightforward to verify that $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$.

Ex.6.2.7. Pick any $a, b \in K^\times$, then $a = u_1\pi^{n_1}$ and $b = u_2\pi^{n_2}$ where u_1, u_2 are units in A and $n_1, n_2 \in \mathbb{Z}$. Then $v(ab) = v(u_1u_2\pi^{n_1+n_2}) = n_1 + n_2 = v(a) + v(b)$.

Ex.6.2.10. First we note that $A_\mathfrak{p}$ can be naturally embedded into K, and we are taking intersection of all $A_\mathfrak{p}$ viewed as subrings of K. Because $A \subseteq A_\mathfrak{p}$ for all $\mathfrak{p}$, $A \subseteq \bigcap_\mathfrak{p} A_\mathfrak{p}$. For the reverse direction, take $x \in \bigcap_\mathfrak{p} A_\mathfrak{p}$, let $\mathfrak{a} = \{a \in A | ax \in A\}$. Then $\mathfrak{a}$ is an ideal of A because A is a subring of K. $\mathfrak{a}$ must be proper, otherwise by Zorn's Lemma there exists a maximal ideal $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then by assumption $x = \frac{a}{s}$ where $a \in A, s \notin \mathfrak{p}$. But $sx = a \in A$ so $s \in \mathfrak{a} \subseteq \mathfrak{p}$, contradiction. So $\mathfrak{a} = A$. In particular, $1 \in \mathfrak{a}$, so $x \in A$.
Remark: More generally, this shows that any integral domain is equal to intersection of its localizations at every maximal ideal.

Ex.6.3.2. First, $|1|{=}|1^2| = |1|^2$ and $|1| \neq 0$, so $|1| = 1$. If $|\cdot|$ is nonarchimedean, then $\forall n \in \mathbb{N}$, $n \neq 0$, $|n| \leq |1| = 1$ by the property of being nonarchimedean. $|0| = 0$. So $\{|n| : n \in \mathbb{N}\}$ is bounded. For the other direction, suppose $\{|n| : n \in \mathbb{N}\}$ is bounded by $M > 0$. FSOC, suppose $|\cdot|$ is archimedean, then there exists $x, y \in K$ such that $|x + y| > \max\{|x|, |y|\}$. This implies $x \neq 0, y \neq 0$. WLOG, suppose $|x| \geq |y|$. Then $|1 + \frac{y}{x}| > \max\{1, |\frac{y}{x}|\}$ where $|\frac{y}{x}| \leq 1$. Let $u = \frac{y}{x}$. For any $n > 1$, $n \in \mathbb{Z}$, we have $|1 + u|^n = |(1 + u)^n| = |\sum_{i=0}^{n} \binom{n}{i} u^i| \leq (n + 1)M$. But $|1 + u| > 1$, so the LHS is exponential growth, while the RHS is linear growth, so the inequality is impossible for some n. So $|\cdot|$ has to be nonarchimedean.

Ex.6.3.8. First, $A_{|\cdot|}$ is a subring of K. For any $a, b \in A_{|\cdot|}$, $|a - b| \leq \max\{|a|, |b|\} \leq 1$, so $a - b \in A_{|\cdot|}$. $|ab| = |a||b| \leq 1$, so $ab \in A_{|\cdot|}$. $|1| = 1$, so $1 \in A_{|\cdot|}$. So $A_{|\cdot|}$ is a subring of K.
K is an integral domain, so $A_{|\cdot|}$ is an integral domain. If $x \in A_{|\cdot|}$ is a unit, then $|x^{-1}| \leq 1$, so $|x| \geq 1$. $|x| \leq 1$ because $x \in A_{|\cdot|}$. So $|x| = 1$. Conversely, if $x \in K$ and $|x| = 1$, then $|x^{-1}| = 1$, so $x^{-1} \in A_{|\cdot|}$, so x is a unit in $A_{|\cdot|}$. So $A^\times_{|\cdot|}$ is the unit group of $A_{|\cdot|}$.
It is quick to verify that $\mathfrak{m}_{|\cdot|}$ is a proper ideal of $A_{|\cdot|}$. Because $A_{|\cdot|} \setminus \mathfrak{m}_{|\cdot|} = A^\times_{|\cdot|}$, $\mathfrak{m}_{|\cdot|}$ is the unique maximal ideal of $A_{|\cdot|}$.
It remains to show that $A_{|\cdot|}$ is PID. Let $I \subseteq A_{|\cdot|}$ be a nontrivial ideal. By assumption, image of the group homomorphism $|\cdot| : K^\times \to \mathbb{R}_{>0}$ is isomorphic to $\mathbb{Z}$, so $|K^\times|$ is free group on one element, so we can pick $u \in I$ such that u has the biggest norm in I. Then for any $v \in I$, we have $v = vu^{-1}u$ where $|vu^{-1}| = \frac{|v|}{|u|} \leq 1$, so $vu^{-1} \in A_{|\cdot|}$, so $v \in (u)$. So $I = (u)$ is principally generated.

Ex.6.5.2. The forward direction is true for any norm on a field: $\forall \epsilon > 0$, $\exists N$ such that $\forall m, n \geq N$, $|a_n - a_m| < \epsilon$, and in particular $|a_n - a_{n+1}| < \epsilon$. The reverse direction is true for any nonarchimedean norm: $\forall \epsilon > 0$, $\exists N$ such that $\forall n \geq N$, $|a_{n+1} - a_n| < \epsilon$. Then for all $n, m \geq N$, assume $n \leq m$, $|a_m - a_n| = |\sum_{i=n}^{i=m-1}(a_{i+1} - a_i)| \leq \max_{n \leq i \leq m-1} |a_{i+1} - a_i| < \epsilon$, so (a_n) is Cauchy.

Ex.6.6.2. Take any $f, g \in R[x]$. Suppose $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$. $(af + bg)' = af' + bg'$ is straightforward to see. To see $(fg)' = f'g + fg'$, it suffices to see $(fg)'$ and $f'g + fg'$ have the same coefficients at degree k where k is arbitrary. The k-th coefficient for $(fg)'$ is $(k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}$. The k-th coefficient for $f'g + fg'$ is $\sum_{i=0}^{k}((i+1)a_{i+1}b_{k-i} + a_i(k-i+1)b_{k-i+1}) = \sum_{i=1}^{k+1} i a_i b_{k-i+1} + \sum_{i=0}^{k} a_i(k-i+1)b_{k-i+1} = (k+1)a_{k+1}b_0 + (k+1)\sum_{i=1}^{k} a_i b_{k-i+1} + (k+1)a_0 b_{k+1} = (k+1)\sum_{i=0}^{k+1} a_i b_{k+1-i}$. So $(fg)' = f'g + fg'$.
For $(f \circ g)' = (f' \circ g)g'$, note that If (f_1, g) and (f_2, g) are pairs satisfying this equation, then $((f_1 f_2) \circ g)' = ((f_1 \circ g)(f_2 \circ g))' = (f_1 \circ g)(f_2 \circ g)' + (f_1 \circ g)'(f_2 \circ g) = (f_1 \circ g)(f_2' \circ g)g' + (f_1' \circ g)g'(f_2 \circ g) = ((f_1 f_2' + f_1' f_2) \circ g)g' = ((f_1 f_2)' \circ g)g'$, so $(f_1 f_2, g)$ is also a pair satisfying this equation. It is also easy to see that (x, g) is a pair satisfying this equation. Also note that $(\_ \circ g)'$ and $(\_' \circ g)g'$ are R-linear endomorphisms of $R[x]$. Combining all these observations, we conclude $(f \circ g)' = (f' \circ g)g'$ for any pair (f, g).

Ex.6.6.3. Let $h(x) = f(x) - f(a) - f'(a)(x - a)$. It suffices to prove $(x - a)^2 | h(x)$. First we have $h(a) = 0$, so $(x - a) | h(x)$, say $h(x) = (x - a)g(x)$ for some $g(x) \in R[x]$. We also have $(x - a)g'(x) + g(x) = h'(x) = f'(x) - f'(a)$, then evaluating at a on both sides gives $g(a) = 0$, so $(x - a) | g(x)$. Thus $(x - a)^2 | h(x)$ and we are done.

Ex.6.6.6. Assume $a_0 \in A$ such that $|f(a_0)| < |f'(a_0)|^2$. Then $|f(a_0)| < 1$ so $f(a_0) \in \mathfrak{m}$. Note $|f'(a_0)| > 0$ so we can divide by $f'(a_0)$. Assume $|f(a_0)| > 0$. Recursively define a_n in the same way as in the proof of Lemma.6.6.5. Inductively we show the following for all $n \geq 0$:
(a) $|f(a_{n+1})| < |f(a_n)|$

(b) $|f'(a_{n+1})| = |f'(a_n)|$, in particular $f'(a_{n+1}) \neq 0$, so we can divide by $f'(a_{n+1})$
(c) $|f(a_{n+1})| < |f'(a_{n+1})|^2$.
When $n = 0$, by Taylor expansion we have the following:

$$f(a_1) = f(a_0) - f'(a_0)\frac{f(a_0)}{f'(a_0)} + g(a_1)(\frac{f(a_0)}{f'(a_0)})^2 = g(a_1)(\frac{f(a_0)}{f'(a_0)})^2 \tag{3}$$

$$f'(a_1) = f'(a_0) - f''(a_0)\frac{f(a_0)}{f'(a_0)} + h(a_1)(\frac{f(a_0)}{f'(a_0)})^2 \tag{4}$$

where $g, h \in A[x]$. By (3) we have $|f(a_1)| \leq \frac{|f(a_0)|^2}{|f'(a_0)|^2} < |f(a_0)|$ because $|f(a_0)| < |f'(a_0)|^2$. Applying the ultrametric property to (4) we have $|f'(a_1)| = |f'(a_0)|$. Finally, using (a) and (b) we have $|f(a_1)| < |f(a_0)| < |f'(a_0)|^2 = |f'(a_1)|^2$.
If $\exists n$ such that $f(a_n) = 0$ then we are done ($a_n \in A$ because for each $k < n$, $|\frac{f(a_k)}{f'(a_k)}| < 1$). Otherwise we show by induction that (a),(b),(c) hold for all n. The arguments are very similar to the base case $n = 0$, so I will omit them here.
Because for each n, $a_{n+1} - a_n = -\frac{f(a_n)}{f'(a_n)}$ and $|\frac{f(a_n)}{f'(a_n)}| < |f'(a_n)| \leq 1$, $a_{n+1} - a_n \in \mathfrak{m}$, so $a_n - a_0 \in \mathfrak{m}$ for all n. $|a_{n+1} - a_n| = |\frac{f(a_n)}{f'(a_n)}| = \frac{|f(a_n)|}{|f'(a_0)|}$, and $|f(a_n)|$ is a strictly decreasing sequence, and $|\cdot|$ is a discrete norm, so we have $\lim_{n\to\infty} |a_{n+1} - a_n| = 0$, so (a_n) is a Cauchy sequence. A is complete DVR, so $a_n \to a$ for some $a \in A$. Then $f(a) = \lim_{n\to\infty} f(a_n) = 0$. Also $|a - a_0| = \lim_{n\to\infty} |a_n - a_0| < 1$, so $\overline{a} = \overline{a_0}$ in k.

Next we prove the lift is unique. Suppose $\overline{a_1} = \overline{a_2} \in k$ is a simple root of $\overline{f}$ and $f(a_1) = f(a_2) = 0$. FSOC, suppose $a_1 \neq a_2$, then $f(x) = (x - a_1)(x - a_2)g(x)$ for some $g(x) \in A[x]$, and $f'(x) = (x - a_1)(x - a_2)g'(x) + ((x - a_1) + (x - a_2))g(x)$, so $f'(a_1) = (a_1 - a_2)g(a_1)$. Because $a_1 - a_2 \in \mathfrak{m}$, $|a_1 - a_2| < 1$ so $|f'(a_1)| < 1$. But $\overline{a_1}$ is a simple root of $\overline{f}$, so $|f'(a_1)| = 1$. Contradiction. So $a_1 = a_2$.

Ex.6.6.8. First, by knowledge of elementary number theory we know the quadratic congruence equation $x^2 \equiv 7 \mod 27$ has exactly two solutions since $(7, 27) = 1$. We note $1 \in \mathbb{F}_3$ solves $x^2 - 7 \in \mathbb{F}_3$. Let $a_0 = 1 \in \mathbb{Z}_3$, then $v(f(a_0)) = v(-6) = 1$, so by the comment after Ex.6.6.6 we have $f(a_n) \equiv 0 \mod \pi^{2^n}$, so in particular $f(a_2) \equiv 0 \mod \pi^4$, so quotienting by $(\pi)^4$ we have $f(a_2) = 0$ in $\mathbb{Z}/81\mathbb{Z}$. Calculation shows $a_1 = 4$ and $a_2 = \frac{23}{8}$. Since $\frac{23}{8} \equiv 13 \mod 81$, we conclude $13^2 - 7 \equiv 0 \mod 81$. Then $13^2 - 7 \equiv 0 \mod 27$. By elementary number theory, the other root is $27 - 13 = 14$. So the two roots are 13 and 14.

Ex.6.7.9. Suppose $|\cdot|$ is trivial on $\mathbb{Q}$. Then the induced topology on $\mathbb{Q}$ is discrete. $\mathbb{Q}$ is also closed in K because if $(a_n) \subseteq \mathbb{Q}$ is a convergent sequence in K, then it is also Cauchy, so $\exists N > 0$ such that $\forall n \geq N$, $|a_n - a_N| < 1$. But $a_n - a_N \in \mathbb{Q}$, so $|a_n - a_N| = 0$, so $a_n = a_N$, so $a_n \to a_N \in \mathbb{Q}$. So $\mathbb{Q}$ is closed in K. Because the norm is trivial, $\mathbb{Q} \subseteq B_1(0)$ where $B_1(0)$ denotes the closed ball of radius 1 centered at 0. By lemma 6.7.4, $B_1(0)$ is compact. Closed subset of compact set is compact, so $\mathbb{Q}$ is compact. But any discrete, compact set must be finite, by definition of compactness. Contradiction. So $|\cdot|$ is non-trivial on $\mathbb{Q}$.

Ex.7.1.1. $N_{L/K} : L \to K$ is multiplicative because determinant is multiplicative, so $\forall x, y \in L$, $|xy|_L = |N_{L/K}(xy)|_K^{1/n} = |N_{L/K}(x)N_{L/K}(y)|_K^{1/n} = |N_{L/K}(x)|_K^{1/n}|N_{L/K}(y)|_K^{1/n} = |x|_L|y|_L$. Obviously $|0|_L = 0$. Conversely if $|x|_L = 0$ for some $x \in L$, then the linear map $m_x : L \to L$ given by $\alpha \mapsto x\alpha$ has zero determinant, so it is not injective, so $x\alpha = 0$ for some $\alpha \in L - \{0\}$, so $x = 0$. Last, we want to show $|x + y|_L \leq |x|_L + |y|_L$. This is true if either $x = 0$ or $y = 0$. So suppose x and y are nonzero, and WLOG assume $|x|_L \leq |y|_L$. Then $|x + y|_L = |y|_L|1 + \frac{x}{y}|_L$ and $|x|_L + |y|_L = |y|_L(1 + |\frac{x}{y}|_L)$, so it suffices to prove $|1 + x|_L \leq 1 + |x|_L$ for $|x|_L \leq 1$. By theorem 7.1.4(3) (proof of this part of the theorem does not use $|\cdot|_L$ satisfies triangle inequality, so we are not in circular argument), $|x|_L \leq 1$ if and only if x is in the integral closure of $\mathcal{O}_K$ in L, so $1 + x$ is in the integral closure of $\mathcal{O}_K$ in L, so $|1 + x|_L \leq 1 \leq 1 + |x|_L$.

Ex.7.1.5. First, it is easy to verify that $||\cdot||$ is indeed a norm on V. Let $(v_n)_{n\geq 1}$ be a Cauchy sequence in V. For each fixed i, denote the i-th component of v_n be v_{ni}, then the sequence $(v_{ni})_{n\geq 1}$ is Cauchy sequence in K, by definition of $||\cdot||$. K is complete, so $v_{ni} \to w_i$ for some $w_i \in K$. Then $v_n \to (w_1, ..., w_n)$ because for each fixed m, $||v_m - (w_1, ..., w_n)|| = \max_{i=1,...,n} |v_{mi} - w_i|$ can be bounded by choosing large enough m. So V is complete under $||\cdot||$. To conclude part (2) of the theorem, we note L is a finite dimensional vector space over K, K is a local field, and $|\cdot|_L$ is a norm on L as a K-vector space. By Lemma 7.1.3, the sup norm and $|\cdot|_L$ induces the same topology on L,

Ex.7.1.6. Choose $p \in \mathfrak{p}$ such that $(p)\mathcal{O}_E = \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}\mathfrak{q}_1 ... \mathfrak{q}_n$ where each $\mathfrak{q}_i$ is distinct from $\mathfrak{q}$. Such p exists, otherwise the exponent of $\mathfrak{q}$ in $\mathfrak{p}\mathcal{O}_E$ is greater than $e_{\mathfrak{q}/\mathfrak{p}}$. Note $p \notin \mathfrak{p}^2$. We claim $\frac{p}{1}$ is a generator of the maximal ideal of $\mathcal{O}_{F,\mathfrak{p}}$. Indeed, pick any generator of the maximal ideal of $\mathcal{O}_{F,\mathfrak{p}}$, $\frac{p'}{s}$, then because $\mathcal{O}_{F,\mathfrak{p}}$ is a DVR, $\frac{p}{1} = \frac{a'}{s'}(\frac{p'}{s})^n$ for some $n \geq 0$, $a' \notin \mathfrak{p}$. Then $ps's^n = a'p'^n$. Then because $p \notin \mathfrak{p}^2$ and $a' \notin \mathfrak{p}$, we must have $n = 1$. But this means in $\mathcal{O}_{F,\mathfrak{p}}$, $\frac{p}{1}$ and $\frac{p'}{s}$ only differ by multiplication of a unit. So $\frac{p}{1}$ generates the maximal ideal of $\mathcal{O}_{F,\mathfrak{p}}$.
Let $\frac{q}{1}$ be a generator of maximal ideal of $\mathcal{O}_{E,\mathfrak{q}}$. Then $q \in \mathfrak{q} - \mathfrak{q}^2$. By the universal property of localization, there is natural embedding $\iota : \mathcal{O}_{F,\mathfrak{p}} \to \mathcal{O}_{E,\mathfrak{q}}$, and we have $\frac{p}{1} = \iota(\frac{p}{1}) = \frac{a}{s}(\frac{q}{1})^n$ where $\frac{a}{s}$ is a unit in $\mathcal{O}_{E,\mathfrak{q}}$ (thus $a \notin \mathfrak{q}$) and $n \geq 0$. Then $ps = aq^n$. Consideration of exponent of $\mathfrak{q}$ in the ideal generated by both sides of this equation gives $e_{\mathfrak{q}/\mathfrak{p}} = n$. Now because F is fractional field of the DVR $\mathcal{O}_{F,\mathfrak{p}}$, each nonzero element of F can be written as $a(\frac{p}{1})^n$ where $n \in \mathbb{Z}$, a is a unit of $\mathcal{O}_{F,\mathfrak{p}}$. It is easy to verify that $\iota(a)$ is a unit in $\mathcal{O}_{E,\mathfrak{q}}$. So after extending definition of ι to $\iota : F \to E$, we get $\iota(a(\frac{p}{1})^n) = u(\frac{q}{1})^{ne_{\mathfrak{q}/\mathfrak{p}}}$ where u is some unit in $\mathcal{O}_{E,\mathfrak{q}}$. So we see that the effect of ι is to raise the valuation of an element in F by $e_{\mathfrak{q}/\mathfrak{p}}$ times. Because large valuation corresponds to small norm, we see that Cauchy sequences in F become (after inclusion in E) Cauchy sequences in E. Therefore natural inclusion gives the induced field extension $E_\mathfrak{q}/F_\mathfrak{p}$. Clearly, this extension induces natural inclusion $\tilde{\iota} : \mathcal{O}_{F_\mathfrak{p}} \to \mathcal{O}_{E_\mathfrak{q}}$.
By a previous exercise, we know that the maximal ideal of $\mathcal{O}_{F_\mathfrak{p}}$ is generated by any element with biggest norm smaller than 1. $[(\frac{p}{1}, \frac{p}{1}, ...)] \in \mathcal{O}_{F_\mathfrak{p}}$ is one such element. Similarly, $[(\frac{q}{1}, \frac{q}{1}, ...)] \in \mathcal{O}_{E_\mathfrak{q}}$ is generator of the maximal ideal. Because $\iota(\frac{p}{1}) = u(\frac{q}{1})^{e_{\mathfrak{q}/\mathfrak{p}}}$ where $u \in \mathcal{O}_{E,\mathfrak{q}}^\times$, $\tilde{\iota}([(\frac{p}{1}, \frac{p}{1}, ...)]) = [(\iota(\frac{p}{1}), \iota(\frac{p}{1}), ...)] = [(u, u, ...)] \cdot [(\frac{q}{1}, \frac{q}{1}, ...)]^{e_{\mathfrak{q}/\mathfrak{p}}}$. On the other hand, $\tilde{\iota}([(\frac{p}{1}, \frac{p}{1}, ...)]) = v[(\frac{q}{1}, \frac{q}{1}, ...)]^{e_{E_\mathfrak{q}/F_\mathfrak{p}}}$ for some $v \in \mathcal{O}_{E_\mathfrak{q}}^\times$. Because units in $\mathcal{O}_{E_\mathfrak{q}}$ have norm 1, comparing norms in the previous two equations gives $e_{\mathfrak{q}/\mathfrak{p}} = e_{E_\mathfrak{q}/F_\mathfrak{p}}$.

Ex.7.2.5. To prove $K(\zeta_m)/K$ is unramified, I will mimic the proof of proposition 7.2.4. Let $L = K(\zeta_m)$.

First, $\overline{\zeta_m} \in k_L$ is a primitive m-th root of unity, because if it is not, then $\overline{\zeta_m}$ is killed by $f = x^n - 1 \in k_L[x]$ for some $n|m$ where $n < m$. Then $p \nmid n$, so $f' = nx^{n-1}$ is nonzero, and since $\gcd(f', f) = 1$, f is separable. So by Hansel's Lemma, there exists $\alpha \in \mathcal{O}_L$ such that $\alpha^n = 1$ and $\overline{\alpha} = \overline{\zeta_m}$. But $\alpha^m = 1$, so $\overline{\alpha}^m = \overline{\zeta_m}^m = 1$. Because $x^m - 1 \in k_L[x]$ is separable, by uniqueness of lift in Hansel's Lemma, $\alpha = \zeta_m$. This contradicts ζ_m being a primitive m-th root of unity. So $\overline{\zeta_m} \in k_L$ is a primitive m-th root of unity. So $k_L \supseteq k_K(\overline{\zeta_m}) \supseteq k_K$.

Next, I will prove $[k_K(\overline{\zeta_m}) : k_K] = [L : K]$. Take $g = x^m - 1 \in \mathcal{O}_K[x]$. We again note that $\overline{g} = x^m - 1 \in k_K[x]$ is separable. By Hansel's Lemma, this implies that if $g = g_1 ... g_s$ where the g_i's are irreducible and monic, then each $\overline{g_i}$ is irreducible and monic. $g(\zeta_m) = 0$, so g_i is minimal polynomial of ζ_m over K for some i. Also $\overline{g_i}(\overline{\zeta_m}) = 0$ so $\overline{g_i}$ is minimal polynomial of $\overline{\zeta_m} \in k_L$ over k_K. Then $[L : K] = \deg g_i = \deg \overline{g_i} = [k_K(\overline{\zeta_m}) : k_K]$.

Because $[L : K] = e_{L/K}[k_L : k_K]$, we must have $e_{L/K} = 1$ and $[k_L : k_K] = [L : K]$. This proves $K(\zeta_m)/K$ is unramified. By proposition 7.2.4, we know $K(\zeta_m) = K(\zeta_{q^n-1})$ for some n, and $n = [K(\zeta_m) : K]$. Therefore $n = [k_K(\overline{\zeta_m}) : k_K] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ where α is a primitive m-th root of unity. Then $\alpha^{q^n-1} = 1$, so $m|q^n - 1$. Let d be the smallest positive integer such that $m|q^d - 1$. Then $n = d$. Otherwise, $n > d$, and we have $\mathbb{F}_{q^n} \supset \mathbb{F}_{q^d} \supseteq \mathbb{F}_q(\alpha) \supseteq \mathbb{F}_q$, because $\mathbb{F}_{q^d}$ is the splitting field extension of $h(x) = x^{q^d} - x$ over $\mathbb{F}_q$, and $h(\alpha) = 0$. Thus $n = d$. So n is the order of q in $(\mathbb{Z}/m\mathbb{Z})^\times$ as a group under multiplication. Note $q \in (\mathbb{Z}/m\mathbb{Z})^\times$ because $(q, m) = 1$.

Ex.7.4.4. ($\Longrightarrow$) Suppose R is DVR. Then R is noetherian because R is PID. R is a local ring because R has a unique maximal ideal by assumption. Furthermore, this maximal ideal is nonzero by assumption, so R cannot be a field (otherwise the only maximal ideal is 0). The maximal ideal of R is principal ideal because R is PID.
($\Longleftarrow$) Because R is local, it has a unique maximal ideal. This maximal ideal is nonzero, otherwise R is a field by Zorn's Lemma. Denote the maximal ideal of R by $\mathfrak{m} = (m)$. We have $\cap_{i=1}^\infty \mathfrak{m}^i = 0$. Otherwise, pick nonzero $a_0 \in \cap_{i=1}^\infty \mathfrak{m}^i$. Because $a_0 \in (m)$, there exists $a_1 \in R$ such that $a_0 = ma_1$. We have $(a_0) \subsetneq (a_1)$, because if $(a_0) = (a_1)$, then $a_1 = ua_0$ for some $u \in R^*$, then $a_0 = mua_0$, so $(1 - mu)a_0 = 0$. $1 - mu \in R^*$, so $a_0 = 0$, contradiction. So $(a_0) \subsetneq (a_1)$.

Also, $a_0 = m^2b$ for some $b \in R$, so $m(mb - a_1) = 0$. $mb - a_1$ cannot be a unit, so $a_1 \in \mathfrak{m}$. Write $a_1 = mc_1$

for some $c_1 \in R$, $a_0 = m^3 c_2$ for some $c_2 \in R$, then $m^2(mc_2 - c_1) = 0$, so $c_1 \in \mathfrak{m}$, so $a_1 \in \mathfrak{m}^2$. Continue such argument, we see $a_1 \in \cap_{i=1}^{\infty} \mathfrak{m}^i$. Thus we can find a_2 such that $(a_1) \subsetneq (a_2)$, and $a_2 \in \cap_{i=1}^{\infty} \mathfrak{m}^i$. Then we can find $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$, which contradicts R being noetherian. Thus $\cap_{i=1}^{\infty} \mathfrak{m}^i = 0$.

Therefore, for any nonzero proper ideal I, there exists $n > 0$ such that $I \subseteq \mathfrak{m}^n$ and $I \nsubseteq \mathfrak{m}^{n+1}$. This implies $\exists i \in I$ such that $i = m^n u$ where $u \in R^*$. So $I = \mathfrak{m}^n$ is principal. So R is PID, and R is furthermore DVR.

Ex.7.4.6. Since L/K is totally ramified, for any $a \in K$ we have $v_L(a) = n \cdot v_K(a)$. Suppose $p_{\pi_L} = x^n + \sum_{i=0}^{n-1} a_i x^i$ where $a_i \in K$. Then $\sum_{i=0}^{n=1} a_i \pi_L^i = -\pi_L^n$. We note $v_L(a_i \pi_L^i) \neq v_L(a_j \pi_L^j)$ for all $i \neq j$ because they are different modulo n. Thus $n = v_L(\sum_{i=0}^{n=1} a_i \pi_L^i) = \min_i\{v_L(a_i \pi_L^i)\} = \min_i\{n \cdot v_K(a_i) + i\}$, so $v_K(a_i) \geq 1$, so $a_i \in (\pi_K)$ for all i. Next, FSOC assume $v_K(a_0) \geq 2$, then $v_L(a_0) \geq 2n$, then $\infty = v_L(0) = v_L(\pi_L^n + \sum_{i=0}^{n-1} a_i \pi_L^i) = n$, contradiction. So $v_K(a_0) = 1$ and p_{π_L} is Eisenstein.

Ex.7.4.8. ($\Longrightarrow$) Pick any π_K and π_L, we have $\pi_L^n \cdot u = \pi_K$ for some $u \in \mathcal{O}_L^\times$. Since $f_{L/K} = 1$, we have $\mathcal{O}_K/(\pi_K) \cong \mathcal{O}_L/(\pi_L)$, so there exists $u' \in \mathcal{O}_K^\times$ such that $u' \equiv u \mod \pi_L$, then $uu'^{-1} \equiv 1 \mod \pi_L$. Consider $f(x) = x^n - uu'^{-1} \in \mathcal{O}_L[x]$. Modulo π_L, we get $\overline{f}(x) = x^n - 1 \in \mathcal{O}_L/(\pi_L)[x]$. $\gcd(\overline{f}, \overline{f}') = \gcd(x^n - 1, nx^{n-1}) = 1$ because $p \nmid n$. Then $\overline{f}$ is separable, so 1 is a simple root of $\overline{f}$, so by Hensel's Lemma f has a root $r \in \mathcal{O}_L^\times$. Then we have $(\pi_L \cdot r)^n = \pi_L^n \cdot uu'^{-1} = \pi_K \cdot u'^{-1}$. From proof of Proposition 7.4.5, we know L is generated over K by any uniformizer of L, so $L = K(\pi_L \cdot r) = K((\pi_K \cdot u'^{-1})^{1/n})$ where $\pi_K \cdot u'^{-1}$ is a uniformizer of K.

($\Longleftarrow$) Let $a = \pi_K^{1/n}$, then $|a|_L = |\pi_K|_L^{1/n}$. We also have $|\pi_L|_L = |\pi_K|_L^{1/e_{L/K}}$, so we must have $e_{L/K} = n$, otherwise $e_{L/K} < n$, then $|a|_L > |\pi_L|_L$, contradicting with π_L having the largest norm less than 1 in $\mathcal{O}_L$. It remains to prove $p \nmid n$, which I don't know how to prove.

Ex.7.7.1. Let $|\cdot|$ be any norm on $\overline{\mathbb{Q}_p}$ extending the norm on $\mathbb{Q}_p$. $\forall \alpha \in \mathbb{Q}_p$, $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ is finite extension. By Theorem 7.1.4, we must have $|\alpha| = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_{\mathbb{Q}_p}^{[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]^{-1}}$, so the norm $|\cdot|$, if exists, is unique. It remains to verify that $|\alpha| = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_{\mathbb{Q}_p}^{[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]^{-1}}$ defines a norm on $\overline{\mathbb{Q}}_p$.

For any finite extension $L/\mathbb{Q}_p$, denote the unique norm on L extending the norm on $\mathbb{Q}_p$ by $|\cdot|_L$. We note that for any finite extensions $L/K/\mathbb{Q}_p$ and $\alpha \in K$, $N_{L/\mathbb{Q}_p}(\alpha) = (N_{K/\mathbb{Q}_p}(\alpha))^{[L:K]}$, which can be seen by considering a basis of L over $\mathbb{Q}_p$ from "mixing" a basis of L over K and a basis of K over $\mathbb{Q}_p$. Thus $|\alpha|_L = |\alpha|_K$. Thus for any $\alpha, \beta \in \overline{\mathbb{Q}}_p$, $|\alpha\beta| = |\alpha\beta|_{\mathbb{Q}_p(\alpha\beta)} = |\alpha\beta|_{\mathbb{Q}_p(\alpha,\beta)} = |\alpha|_{\mathbb{Q}_p(\alpha,\beta)} \cdot |\beta|_{\mathbb{Q}_p(\alpha,\beta)} = |\alpha|_{\mathbb{Q}_p(\alpha)} \cdot |\beta|_{\mathbb{Q}_p(\beta)} = |\alpha| \cdot |\beta|$, and $|\alpha + \beta| = |\alpha + \beta|_{\mathbb{Q}_p(\alpha+\beta)} = |\alpha + \beta|_{\mathbb{Q}_p(\alpha,\beta)} \leq \max\{|\alpha|_{\mathbb{Q}_p(\alpha,\beta)}, |\beta|_{\mathbb{Q}_p(\alpha,\beta)}\} = \max\{|\alpha|_{\mathbb{Q}_p(\alpha)}, |\beta|_{\mathbb{Q}_p(\beta)}\} = \max\{|\alpha|, |\beta|\}$. Thus $|\cdot|$ is a nonarchimedean norm on $\overline{\mathbb{Q}}_p$.

Ex.8.0.2. First we show EH/F is Galois extension. Since H/F is finite $H = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in H$. Then $EH = E(\alpha_1, \ldots, \alpha_n)$. Since $\alpha_1, \ldots, \alpha_n \in EH$ are algebraic and separable over E (because they are algebraic and separable over F), EH/E is finite and separable. Since E/F is finite and separable, EH/F is finite and separable. Next consider any embedding $\sigma : EH \to \overline{F}$. Then $\sigma(EH) = \sigma(E)\sigma(H) = EH$ where the last step is true because E/F and H/F are normal. Therefore EH/F is normal. Thus EH/F is Galois.

To see EH/F is abelian, let $G = \mathrm{Gal}(EH/F)$, $N_1 = \mathrm{Gal}(EH/E), N_2 = \mathrm{Gal}(EH/H)$. we note $\frac{G}{N1} = \mathrm{Gal}(E/F)$ is abelian group, and $\frac{G}{N_2} = \mathrm{Gal}(H/F)$ is abelian group. Let $\varphi : G \to \frac{G}{N_1} \times \frac{G}{N_2}$ be the canonical map. Then $\frac{G}{\ker \varphi} \cong \operatorname{im} \varphi$ is abelian group. But $\ker \varphi = N_1 \cap N_2 = e$, the trivial group, so G is abelian.