1. a) We recall that the expression $\frac{a}{q}$ (in $Q = \mathrm{Frac}(A)$) denotes the equivalence class of $(a, q) \in A \times (A \smallsetminus \mathfrak{p})$ for the relation given by

$$\frac{a}{q} = \{(a', q') \in A \times (A \smallsetminus \mathfrak{p}) \colon aq' = a'q\}.$$

The addition and multiplication of equivalence classes are given by the formulae

$$\frac{a}{q} + \frac{a'}{q'} = \frac{aq' + a'q}{qq'},$$
$$\frac{a}{q} \cdot \frac{a'}{q'} = \frac{aa'}{qq'}.$$

One checks that $\frac{0}{1}$ and $\frac{1}{1}$ are the additive and multiplicative units in Q respectively and that both elements are contained in $A_\mathfrak{p}$. Moreover, the formulae show that additive inverses, sums, and products of elements in $A_\mathfrak{p}$ (taken in Q) admit representatives in $A_\mathfrak{p}$ since $qq' \in \mathfrak{p} \implies q \in \mathfrak{p} \vee q' \in \mathfrak{p}$ and thus $A_\mathfrak{p}$ is a subring of Q.
For completeness, we recall that A identifies with a subring of $A_\mathfrak{p}$ via the map $i \colon a \mapsto \frac{a}{1}$. We skip the verification that this is a ring homomorphism and only point out that i is injective since $\frac{a}{1} = \frac{0}{1}$ if and only if $a = a \cdot \cdot 1 = 0 \cdot 1 = 0$.

b) Since both $\mathfrak{a}_\mathfrak{p}$ and A are A-modules, so is $\mathfrak{a} = \mathfrak{a}_\mathfrak{p} \cap A$ and hence $\mathfrak{a}$ is an ideal in A. It is clear that $\mathfrak{a}.A_\mathfrak{p} \subseteq \mathfrak{a}_\mathfrak{p}$. So suppose that $\frac{a}{q} \in \mathfrak{a}_\mathfrak{p}$ with $a \in A$ and $q \in A \smallsetminus \mathfrak{p}$. Then $A \ni \frac{a}{1} = \frac{q}{1} \cdot \frac{a}{q} \in \mathfrak{a}_p$, i.e., $\frac{a}{1} \in \mathfrak{a}$. Since $\frac{1}{q} \in A_\mathfrak{p}$, we find that

$$\frac{a}{q} = \frac{a}{1} \cdot \frac{1}{q} \in \mathfrak{a}.A_\mathfrak{p}$$

and, since $\frac{a}{q}$ was arbitrary, we therefore find that $\mathfrak{a}_\mathfrak{p} \subseteq \mathfrak{a}.A_\mathfrak{p}$ as desired.
Remark: The argument above shows that

$$\mathfrak{a}_\mathfrak{p} = \left\{\frac{a}{q} \colon a \in \mathfrak{a}, q \in A \smallsetminus \{\mathfrak{p}\}\right\}.$$

This is true more generally for extensions of ideals, i.e., let $\mathfrak{b} \lhd A$ be an ideal and let $\mathfrak{b}_\mathfrak{p} = \mathfrak{b}.A_\mathfrak{p}$. We claim that

$$\mathfrak{b}_\mathfrak{p} = \left\{\frac{b}{q} \colon b \in \mathfrak{b}, q \in A \smallsetminus \mathfrak{p}\right\}.$$

To this end let $x \in \mathfrak{b}_\mathfrak{p}$ arbitrary. By definition, there exist $b_1, \ldots, b_r \in \mathfrak{b}$, $a_1, \ldots, a_r \in A$, and $q_1, \ldots, q_r \in A \smallsetminus \mathfrak{p}$ such that

$$x = \sum_{i=1}^{r} \frac{b_i}{1} \cdot \frac{a_i}{q_i} = \sum_{i=1}^{r} \frac{a_i b_i}{q_i}$$
$$= \frac{a_1 b_1 + \cdots + a_r b_r}{q_1 \cdots q_r}.$$

Since $\mathfrak{p}$ is prime, we have that $q_1 \cdots q_r \in A \smallsetminus \mathfrak{p}$. Since $\mathfrak{b}$ is an ideal, we have that $a_1 b_1 + \cdots + a_r b_r \in \mathfrak{b}$. Therefore, the claim follows.

c) Since $\mathfrak{q}$ is coprime to $\mathfrak{p}$, we know that $\mathfrak{q} \cap (A \smallsetminus \mathfrak{p})$ is non-empty. Let q be contained in the latter intersection, then

$$\frac{1}{1} = \frac{q}{1} \cdot \frac{1}{q} \in \mathfrak{q}.A_{\mathfrak{p}}$$

and, hence, the claim.

d) Note that $\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p}.A_{\mathfrak{p}}$ is a proper ideal in $A_{\mathfrak{p}}$. Indeed, if $\frac{1}{1} \in \mathfrak{p}.A_{\mathfrak{p}}$, by the description of the extension proven earlier, there exist $p \in \mathfrak{p}$ and $q \in A \smallsetminus \mathfrak{p}$ such that $\frac{1}{1} = \frac{p}{q}$, i.e., $q \in \mathfrak{p}$, which is absurd.
Let $\mathfrak{a}_{\mathfrak{p}}$ be a proper non-zero ideal and let $\mathfrak{a} = \mathfrak{a}_{\mathfrak{p}} \cap A$. Then $\mathfrak{a}$ is a proper ideal in A since $1 \notin \mathfrak{a}$ and, moreover, $\mathfrak{a} \neq \{0\}$ since clearing the denominator of any non-zero element in $\mathfrak{a}_{\mathfrak{p}}$ yields a non-zero element in $\mathfrak{a}$.
Since A is Dedekind, we can write $\mathfrak{a} = \mathfrak{p}^v \mathfrak{q}$, where $\mathfrak{q}$ is coprime to $\mathfrak{p}$. We claim that for any two ideals $\mathfrak{b}_1, \mathfrak{b}_2 \lhd A$ we have

$$(\mathfrak{b}_1 \cdot \mathfrak{b}_2).A_{\mathfrak{p}} = (\mathfrak{b}_1.A_{\mathfrak{p}}) \cdot (\mathfrak{b}_1.A_{\mathfrak{p}}).$$

Let $x \in (\mathfrak{b}_1 \cdot \mathfrak{b}_2).A_{\mathfrak{p}}$, i.e., using the description of extensions proven before, there are $b_1^{(j)}, \ldots, b_r^{(j)} \in \mathfrak{b}_j$ and $q \in A \smallsetminus \mathfrak{p}$ such that

$$x = \frac{b_1^{(1)} b_1^{(2)} + \cdots + b_r^{(1)} b_r^{(2)}}{q} = \sum_{i=1}^{r} \frac{b_i^{(1)}}{1} \cdot \frac{b_i^{(2)}}{q} \in (\mathfrak{b}_1.A_{\mathfrak{p}}) \cdot (\mathfrak{b}_2.A_{\mathfrak{p}}).$$

On the other hand, let $b^{(j)} \in \mathfrak{b}_j$ and $q_1, q_2 \in A \smallsetminus \mathfrak{p}$, then

$$\frac{b^{(1)}}{q_1} \cdot \frac{b^{(2)}}{q_2} = \frac{b^{(1)} b^{(2)}}{q_1 q_2} \in (\mathfrak{b}_1 \cdot \mathfrak{b}_2).A_{\mathfrak{p}}.$$

In particular, using the description of extension of ideals discussed above, elements in $(\mathfrak{b}_1.A_{\mathfrak{p}}) \cdot (\mathfrak{b}_2.A_{\mathfrak{p}})$ are finite sums of elements in $(\mathfrak{b}_1 \cdot \mathfrak{b}_2).A_{\mathfrak{p}}$ and, hence, $(\mathfrak{b}_1.A_{\mathfrak{p}}) \cdot (\mathfrak{b}_2.A_{\mathfrak{p}}) \subseteq (\mathfrak{b}_1 \cdot \mathfrak{b}_2).A_{\mathfrak{p}}$.
Using the claim, we know that

$$\mathfrak{a}_{\mathfrak{p}} = (\mathfrak{p}^v.A_{\mathfrak{p}}) \cdot (\mathfrak{q}.A_{\mathfrak{p}}) = (\mathfrak{p}.A_{\mathfrak{p}})^v = \mathfrak{m}_{\mathfrak{p}}^v$$

since $\mathfrak{q}$ was coprime to $\mathfrak{p}$.

e) Let x as in the hint and let $x.A_{\mathfrak{p}}$ be the ideal generated by x. Since $x \in \mathfrak{p}$, we know that $x.A_{\mathfrak{p}} \subseteq \mathfrak{m}_{\mathfrak{p}}$. We claim that $x.A_{\mathfrak{p}}$ is not contained in $\mathfrak{m}_{\mathfrak{p}}^2$. To this end, it suffices to show that $x \notin \mathfrak{m}_{\mathfrak{p}}^2 = \mathfrak{p}^2.A_{\mathfrak{p}}$. Assume otherwise, then the explicit description of extensions implies that there exist $a \in \mathfrak{p}^2$ and $q \in A \smallsetminus \mathfrak{p}$ such that $a = qx$ and, in particular, $qx \in \mathfrak{p}^2$. In particular, we have that $(qx).A = (q.A) \cdot (x.A) \subseteq \mathfrak{p}^2$. By assumption, we know that $x.A = \mathfrak{p}\mathfrak{q}$ for $\mathfrak{q}$ coprime to $\mathfrak{p}$ and, hence,

$$\mathfrak{p} = \mathfrak{p}^{-1} \cdot \mathfrak{p}^2 \supset \mathfrak{p}^{-1} \cdot (q.A) \cdot (x.A) = (q.A) \cdot \mathfrak{q}$$

implies that $q.A \subseteq \mathfrak{p}$ and, in particular, $q \in \mathfrak{p}$, which is absurd.

f) Let $\pi \colon A_{\mathfrak{p}} \twoheadrightarrow A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ denote the canonical projection and let $i_{\mathfrak{p}} = \pi \circ i$, where $i \colon A \to A_{\mathfrak{p}}$ is the embedding described earlier. Let $a \in \ker i_{\mathfrak{p}}$. Since $\ker \pi = \mathfrak{m}_{\mathfrak{p}}$, this means that $i(a) = \frac{a}{1} \in \mathfrak{m}_{\mathfrak{p}}$ and, by the explicit description of extensions of ideals, there are $p \in \mathfrak{p}$ and $q \in A \smallsetminus \mathfrak{p}$ such that $p = qa$. Since $\mathfrak{p}$ is prime, it follows that $a \in \mathfrak{p}$ and, therefore, $\ker i_{\mathfrak{p}} \subseteq \mathfrak{p}$. On the other hand, for any $a \in \mathfrak{p}$, we have that $i(a) \in \mathfrak{p}.A_{\mathfrak{p}}$ and, thus, $\ker i_{\mathfrak{p}} = \mathfrak{p}$. By the firs isomorphism theorem, it only remains to prove that $i_{\mathfrak{p}}$ is surjective. To this end, let $x \in A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ and let

$a \in A$ and $q \in A \smallsetminus \mathfrak{p}$ such that $x = \frac{a}{q} + \mathfrak{m}_\mathfrak{p}$. Since A is Dedekind, $\mathfrak{p}$ is maximal and, hence, there exists $q' in A \smallsetminus \mathfrak{p}$ such that $r = qq' - 1 \in \mathfrak{p}$. Let $a' = aq'$, then

$$i_\mathfrak{p}(a') - x = \frac{qa' - a}{q} + \mathfrak{m}_\mathfrak{p} = \frac{r}{q} + \mathfrak{m}_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}$$

and, thus, $i_\mathfrak{p}(a') = x$. This proves surjectivity.

2. Let $d = [K\colon \mathbb{Q}]$ and let $n = d!$. Let S_n denote the group of permutations of a set of cardinality n and let $A_n \lhd S_n$ denote the subgroup of even permutations. We will denote by $\operatorname{sgn}(\tau) \in \{\pm 1\}$ the signature of the permutation $\tau \in S_n$. Then

$$\det(\sigma_j \omega_i) = \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \prod_{i=1}^{d} \sigma_{\tau(j)}\omega_i = \underbrace{\sum_{\tau \in A_n} \prod_{i=1}^{d} \sigma_{\tau(j)}\omega_i}_{=:P} - \underbrace{\sum_{\tau \in S_n \smallsetminus A_n} \prod_{i=1}^{d} \sigma_{\tau(j)}\omega_i}_{=:N} .$$

Let $1 \leqslant i, j \leqslant d$ arbitrary. Since ω_i is an algebraic integer, there exists a monic polynomial $R \in \mathbb{Z}[X]$ such that

$$R(\sigma_j \omega_i) = \sigma_j R(\omega_i) = 0$$

and, hence, σ_j is an algebraic integer. Since products and sums of algebraic integers are algebraic integers, it follows that P and N are algebraic integers. Next we show that $P + N, PN \in \mathbb{Q}$. Since $\mathbb{Z}$ is integrally closed, this will imply that $P + N, PN \in \mathbb{Z}$ and, therefore

$$\Delta_K = (P+N)^2 - 4PN \equiv (P+N)^2 \mod 4$$

and, since squares have residue 0 or 1 mod 4, the claim follows.

In order to see that $P + N$ and PN are rational, let $L \subseteq \mathbb{C}$ be the Galois closure of K, which is the field generated by all the roots of the minimal polynomial of a generator of K over $\mathbb{Q}$. We fix an embedding $\sigma_1 \colon K \to \mathbb{C}$ and identify K with its image in L under σ_1. In particular, from now on we will assume that $\operatorname{Hom}_\mathbb{Q}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_d\}$ with $\sigma_1 = \operatorname{id}_K$. We claim the map $\operatorname{Gal}(L/\mathbb{Q}) \to \operatorname{Hom}_\mathbb{Q}(K, \mathbb{C})$ is surjective and, in particular, every element in $\operatorname{Gal}(L/\mathbb{Q})$ is the extension of an embedding of K in $\mathbb{C}$. To this end, let $\sigma \in \operatorname{Hom}_\mathbb{Q}(K, \mathbb{C})$ arbitrary. Let $\alpha \in K$ such that $K = \mathbb{Q}[\alpha]$. We claim that $\sigma(\alpha) \in L$. Then $\sigma(\alpha) \in L$, since $\sigma(\alpha)$ is a root of the minimal polynomial of α over $\mathbb{Q}$ and since $[\times \alpha]_{L/\mathbb{Q}}$ is diagonalizable over L with eigenvalues equal to the roots of the minimal polynomial of α over $\mathbb{Q}$ (this requires a proof which was sketched in class). It follows that $\sigma(K) \subseteq L$ for all $\sigma \in \operatorname{Hom}_\mathbb{Q}(K, \mathbb{C})$. Given $\sigma \in \operatorname{Hom}_\mathbb{Q}(K, \mathbb{C})$, let $\beta \in L$ such that $L = \sigma(K)[\beta]$. The elements of $\operatorname{Gal}(L/K)$ permute β among the roots of the minimal polynomial of β over $\sigma(K)$ and, hence, σ admits exactly $[L\colon \sigma(K)] = [L\colon K]$ extensions to L.

As a corollary, we obtain that for all $\tilde{\sigma} \in \operatorname{Gal}(L/\mathbb{Q})$ we have that

$$\{\tilde{\sigma} \circ \sigma \colon \sigma \in \operatorname{Hom}_\mathbb{Q}(K/\mathbb{C})\} = \operatorname{Hom}_\mathbb{Q}(K, \mathbb{C}).$$

Indeed, suppose σ and σ' are in $\operatorname{Hom}_\mathbb{Q}(K, \mathbb{C})$ and $\tilde{\sigma} \circ \sigma = \tilde{\sigma} \circ \sigma'$, then invertibility of $\tilde{\sigma}$ yields $\sigma = \sigma'$. Hence the map $\sigma \mapsto \tilde{\sigma} \circ \sigma$ is a permutation of $\operatorname{Hom}_\mathbb{Q}(K, \mathbb{C})$.

In order to see that $P+N \in \mathbb{Q}$, note that for all $\tilde{\sigma} \in \mathrm{Gal}(L/\mathbb{Q})$

$$\begin{aligned}\tilde{\sigma}(P+N) &= \sum_{\tau \in A_n} \prod_{i=1}^{d} (\tilde{\sigma} \circ \sigma_{\tau(i)})(\omega_i) + \sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{n} (\tilde{\sigma} \circ \sigma_{\tau(i)})(\omega_i) \\ &= \sum_{\tau \in S_n} \prod_{i=1}^{d} (\tilde{\sigma} \circ \sigma_{\tau(i)})(\omega_i) = \sum_{\tau \in S_n} \prod_{i=1}^{d} \sigma_{\tau(i)}(\omega_i) \\ &= \sum_{\tau \in A_n} \prod_{i=1}^{d} \sigma_{\tau(i)}(\omega_i) + \sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{d} \sigma_{\tau(i)}(\omega_i) = P+N.\end{aligned}$$

Since $\tilde{\sigma} \in \mathrm{Gal}(L/\mathbb{Q})$ was arbitrary, it follows that $P+N \in L^{\mathrm{Gal}(L/\mathbb{Q})} = \mathbb{Q}$.

In order to see that $PN \in \mathbb{Q}$, we use a slightly different argument (which also works for $P+N$). The claim is that for every $\tilde{\sigma} \in \mathrm{Gal}(L/\mathbb{Q})$ we have

$$\big(\tilde{\sigma}(P) = P \wedge \tilde{\sigma}(N) = N\big) \vee \big(\tilde{\sigma}(P) = N \wedge \tilde{\sigma}(N) = P\big).$$

To this end, we note that, since $\mathrm{Gal}(L/\mathbb{Q})$ acts by permutations on $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, for every $\tilde{\sigma} \in \mathrm{Gal}(L/\mathbb{Q})$ there exists $\tilde{\tau} \in S_n$ such that

$$\forall 1 \leqslant i \leqslant [K\colon \mathbb{Q}] \quad \tilde{\sigma} \circ \sigma_i = \sigma_{\tilde{\tau}(i)}.$$

In particular,

$$\forall 1 \leqslant i \leqslant [K\colon \mathbb{Q}] \forall \tau \in S_n \quad \tilde{\sigma} \circ \sigma_{\tau(i)} = \sigma_{(\tilde{\tau} \circ \tau)(i)}.$$

If $\tilde{\tau}$ is an even permutation, since the sign $\mathrm{sgn}\colon S_n \to \{\pm 1\}$ mapping a permutation to its parity is a homomorphism, we find that $\tilde{\tau} \circ \tau \in A_n$ if and only if $\tau \in A_n$, i.e., composition with $\tilde{\tau}$ corresponds to a permutation on A_n and on $S_n \setminus A_n$. In particular

$$\begin{aligned}\tilde{\sigma}(PN) = \tilde{\sigma}(P)\tilde{\sigma}(N) &= \left(\sum_{\tau \in A_n} \prod_{i=1}^{d} (\tilde{\sigma} \circ \sigma_{\tau(i)})(\omega_i)\right)\left(\sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{d} (\tilde{\sigma} \circ \sigma_{\tau(i)})(\omega_i)\right) \\ &= \left(\sum_{\tau \in A_n} \prod_{i=1}^{d} \sigma_{(\tilde{\tau} \circ \tau)(i)}(\omega_i)\right)\left(\sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{d} \sigma_{(\tilde{\tau} \circ \tau)(i)}(\omega_i)\right) \\ &= \left(\sum_{\tau \in A_n} \prod_{i=1}^{d} \sigma_{\tau(i)}(\omega_i)\right)\left(\sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{d} \sigma_{\tau(i)}(\omega_i)\right) = PN.\end{aligned}$$

If $\tilde{\tau}$ is an odd permutation, we find that $\tilde{\tau} \circ \tau \in A_n$ if and only if $\tau \in S_n \setminus A_n$, i.e., $\tilde{\tau}$ bijectively maps A_n to $S_n \setminus A_n$ and vice versa. In particular

$$\begin{aligned}\tilde{\sigma}(PN) = \tilde{\sigma}(P)\tilde{\sigma}(N) &= \left(\sum_{\tau \in A_n} \prod_{i=1}^{d} (\tilde{\sigma} \circ \sigma_{\tau(i)})(\omega_i)\right)\left(\sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{d} (\tilde{\sigma} \circ \sigma_{\tau(i)})(\omega_i)\right) \\ &= \left(\sum_{\tau \in A_n} \prod_{i=1}^{d} \sigma_{(\tilde{\tau} \circ \tau)(i)}(\omega_i)\right)\left(\sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{d} \sigma_{(\tilde{\tau} \circ \tau)(i)}(\omega_i)\right) \\ &= \left(\sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{d} \sigma_{\tau(i)}(\omega_i)\right)\left(\sum_{\tau \in A_n} \prod_{i=1}^{d} \sigma_{\tau(i)}(\omega_i)\right) = NP = PN.\end{aligned}$$

Since $\tilde{\sigma}$ was arbitrary, we again find that $PN \in L^{\mathrm{Gal}(L/\mathbb{Q})} = \mathbb{Q}$. This completes the proof.

3.