Solutions for exercises, Algebra I (Commutative Algebra) – Week 10

Exercise 49. (Associated primes, 4 points)

1. Let $\mathfrak{p} \in \mathrm{Ass}(N)$; there is a $n \in N$, such that $\mathrm{Ann}(n) = \mathfrak{p}$; since $n \in M$, we get $\mathfrak{p} \in \mathrm{Ass}(M)$ i.e. $\mathrm{Ass}(N) \subset \mathrm{Ass}(M)$.
   Now, let $\mathfrak{p} \in \mathrm{Ass}(M)$ and $m \in M$ such that $\mathrm{Ann}(m) = \mathfrak{p}$. If $\overline{m} = 0 \in M/N$, then $m \in N$ and we get $\mathfrak{p} \in \mathrm{Ass}(N)$. Otherwise, $\overline{m} \neq 0 \in M/N$ and $\forall a \in \mathfrak{p}$, $a\overline{m} = \overline{am} = \overline{0}$ so $\mathfrak{p} \subset \mathrm{Ann}(\overline{m})$. Conversely if $\mathrm{Ann}(\overline{m}) = \mathfrak{p}$, then $\mathfrak{p} \in \mathrm{Ass}(M/N)$. Otherwise, consider $a \in \mathrm{Ann}(\overline{m})\backslash\mathfrak{p}$ then $a\overline{m} = 0 \in M/N$ i.e. $am \in N$; a direct calculation shows that $\mathfrak{p} \subset \mathrm{Ann}(am)$. Now if $b \in \mathrm{Ann}(am)$, $bam = 0 \in M$ thus $ba \in \mathrm{Ann}(m) = \mathfrak{p}$; but since $a \notin \mathfrak{p}$, $b \in \mathfrak{p}$ i.e. $\mathfrak{p} = \mathrm{Ann}(\underbrace{am}_{\in N})$; thus $\mathfrak{p} \in \mathrm{Ass}(N)$ i.e. $\mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$.

2. Let $\mathfrak{p} \in \mathrm{Ass}(M)$ and consider $m \in M$ such that $\mathrm{Ann}(m) = \mathfrak{p}$. If $\frac{m}{1} = 0 \in M_\mathfrak{p}$, there is a $a \notin \mathfrak{p}$, such that $am = 0 \in M$ i.e. $a \in \mathrm{Ann}(m) = \mathfrak{p}$. Contradiction. Thus $\frac{m}{1} \neq 0 \in M_\mathfrak{p}$. In particular $M_\mathfrak{p} \neq 0$ i.e. $\mathfrak{p} \in \mathrm{Supp}(M)$.

3. Let us denote $\varphi : M \to \prod_{\mathfrak{p}\in\mathrm{Ass}(M)} M_\mathfrak{p}$.
   Let first prove that $\mathrm{Ass}(M) \neq \emptyset$ as soon as $M \neq 0$ (using Noetherianess of A): take $0 \neq m \in M$, then $0 \in \mathrm{Ann}(m) \neq A$. If $\mathrm{Ann}(m)$ is prime, we can find $a, b \in A\backslash\mathrm{Ann}(m)$ such that $ab \in \mathrm{Ann}(m)$ i.e. $am \neq 0$ and $bm \neq 0$ but $abm = 0$. Then $b \in \mathrm{Ann}(am)$ and for any $c \in \mathrm{Ann}(am)$, $cam = acm = a \cdot 0 = 0$ i.e. $\mathrm{Ann}(m) \subset \mathrm{Ann}(am)$; thus $\mathrm{Ann}(m) \subsetneq \mathrm{Ann}(m) + (b) \subset \mathrm{Ann}(am)$. Next, if $\mathrm{Ann}(am) \neq A$ is not prime, we can repeat the process and find a $c \in A$ such that $\mathrm{Ann}(m) \subsetneq \mathrm{Ann}(am) \subsetneq \mathrm{Ann}(acm) \neq A$. So we can construct inductively, an ascending chain of proper ideals. As S is Noetherian, the chain has to stop so we reach a $0 \neq m' \in \langle m\rangle$ (the cyclic submodule generated by m) for which $\mathrm{Ann}(m')$ is a prime ideal i.e. such that $\mathrm{Ann}(m') \in \mathrm{Ass}(M)$.
   Now, if $\ker(\varphi) \neq 0$, take $0 \neq m \in \ker(\varphi)$; then since $m \neq 0$, $\mathrm{Ann}(m) \neq A$ and if $\mathrm{Ann}(m)$ is not a prime ideal, we can proceed as above to find a $m' \in \langle m\rangle$ such that $\mathrm{Ann}(m')$ is a prime ideal i.e. $\mathrm{Ann}(m') \in \mathrm{Ass}(M)$. But since $m' \in \langle m\rangle$ we can write $m' = am$; thus $\varphi(m') = a\varphi(m) = 0$ i.e. $m' \in \ker(\varphi)$. But looking at the component corresponding to $\mathrm{Ann}(m')$, we get a contradiction by the previous question. So $\ker(\varphi) = 0$.

Exercise 50. (Discrete valuation rings (or not), 6 points)

1. $\mathbb{Z}$ is not local (for any prime number $p > 0$, (p) is maximal) thus not a discrete valuation ring.

2. We have seen (solution for exercise 8) the non-zero ideals of $k[[x]]$ are of the form (x^d) for some $d \geq 0$. So $k[[x]]$ is a principal ideal domain, in particular any ideal in $k[[x]]$ is finitely generated (by one element) thus $k[[x]]$ is Noetherian. Among the ideals (x^d) of $k[[x]]$, only (x) is prime; thus $\mathrm{Spec}(k[[x]]) = \{(0), (x)\}$. So $\mathrm{MaxSpec}(k[[x]]) = \{(x)\}$ i.e. $k[[x]]$ is local. Observe that $(x)/(x)^2 = (x)/(x^2) \simeq k \cdot \overline{x}$. So according to Corollary 11.16 $k[[x]]$ is a discrete valuation ring.

Solutions to be handed in before Tuesday June 22, 4pm.

3. We have $\mathrm{Spec}(k[x]_x) \simeq D(x)$; since $k[x]$ has infinitely many maximal ideals (irreducible elements) and $D(x)$ consists of all maximal ideals of $k[x]$ but (x), $k[x]_x$ is not local hence not a discrete valuation ring.

4. the ring $k[x^2, x^3]$ is an integral domain as subring of an integral domain. We have $x = \frac{x^3}{x^2} \in Q(k[x^2, x^3])$ and x is annhilated by $Y^2 - x^2 \in k[x^2, x^3][Y]$ so it is integral over $k[x^2, x^3]$ but $x \notin k[x^2, x^3]$ (looking at the expansions in $k[x]$). So $k[x^2, x^3]$ is not normal. In particular it cannot be a discrete valuation ring.

5. We have $\mathrm{Spec}(\mathbb{F}_3[x, y]/(x^2 - y)) \simeq V((x^2 - y)) \subset \mathrm{Spec}(\mathbb{F}_3[x, y])$. The ideal $(x^2 - y) \subset (x^2 - y, x) = (y, x)$ satisfies $\mathbb{F}_3[x, y]/(x^2 - y, x) \simeq \mathbb{F}_3$ so it is a maximal ideal of $\mathbb{F}_3[x, y]$ i.e. $(\overline{x}) \in \mathrm{MaxSpec}(\mathbb{F}_3[x, y]/(x^2 - y))$ is maximal.
   Likewise the ideal $(x^2-y) \subset (x^2-y, x-1) = (1-y, x-1)$ satisfies $\mathbb{F}_3[x, y]/(x^2-y, x-1) \simeq \mathbb{F}_3$ i.e. is maximal; thus $(\overline{x} - 1) \in \mathrm{MaxSpec}(\mathbb{F}_3[x, y]/(x^2 - y))$. But $(\overline{x} - 1) \neq (\overline{x})$. Otherwise $x - 1 \in (x^2 - y, x) = (y, x)$ but evaluating the polynomials at $(0, 0)$, we get a contradiction.
   So $\mathbb{F}_3[x, y]/(x^2 - y)$ is not local, in particular not a discrete valuation ring.

For any field, the constant map $\nu : K^* \to \mathbb{Z}$, $a \mapsto 0$ satisfies Lemma 13.4 (i) and (ii); but $\{\nu(\cdot) \geq 0\} \cup \{0\} = K$ is not a discrete valuation ring.
As soon as the valuation $\nu : K^* \to \mathbb{Z}$ is not constant, by the property (ii) of Lemma 13.4 (and $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$ so $\nu(1) = 0$) $\nu(K^*) \subset \mathbb{Z}$ is a non-zero subgroup of $\mathbb{Z}$ i.e. of the form (d) for some $d > 0$. Then looking at $\widetilde{\nu} : K^* \to \mathbb{Z}$, $a \mapsto \frac{\nu(a)}{d}$ we get a surjective group homomorphism and $\{a \in K^*,\ \widetilde{\nu}(a) \geq 0\} = \{a \in K^*,\ \nu(a) \geq 0\}$ so $\{0\} \cup \{a \in K^*,\ \nu(a) \geq 0\}$ is a discrete valuation ring.

Exercise 51. (Rings that are not Dedekind rings, 5 points)

1. Let us consider the ideal $(x_1, x_2) \subset A$. It is fractional as an ideal of A. If it is invertible, consider $M \subset k(x_1, x_2)$ its inverse. It is finitely generated by Remark 14.12 (ii) and (iii). Let us denote $f_1, \ldots, f_k \in k(x_1, x_2)$ a set of generators of M as A-module. Then for any i, $f_i x_1 \in A$ thus the only denominator that can appear in the f_i's is x_1. But we also have $f_i x_2 \in A$ so actually $f_i \in A$ for any i i.e. $M \subset A$ is an ideal. Then $M \cdot (x_1, x_2) = ((x_1 f_i, x_2 f_i)_{i=1,\ldots,k})$; thus evaluating at $(0, 0)$ we see that $1 \notin M \cdot (x_1, x_2)$. Contradiction. So (x_1, x_2) is not invertible.

2. We compute $(\overline{x_1}, \overline{x_2})^2 = (\overline{x_1}^2, \overline{x_2}^2, \overline{x_1 x_2}) = (\overline{x_1}^3, \overline{x_1}^2, \overline{x_1 x_2}) = (\overline{x_1}^2, \overline{x_1 x_2}) = (\overline{x_1}) \cdot (\overline{x_1}, \overline{x_2})$. Thus if $(\overline{x_1}, \overline{x_2})$ is invertible, we get $(\overline{x_1}, \overline{x_2}) = (\overline{x_1})$.
   This is impossible as $\overline{x_2} \notin (\overline{x_1})$; otherwise $x_2 = x_1 f + (x_2^2 - x_1^3) g$ in $k[x_1, x_2]$ for some $f, g \in k[x_1, x_2]$; then evaluating at $x_1 = 0$ we get $x_2 = x_2^2 g(0, x_2) \in k[x_2]$ which is impossible for degree reason. So $(\overline{x_1}, \overline{x_2})$ is not invertible.

Exercise 52. (Absolute values, 4 points)

1. Define $|\cdot| : Q(A) \to \mathbb{R}$ by $|\frac{a}{b}| = \frac{|a|}{|b|}$. It is well-defined as, if $\frac{a}{b} = \frac{c}{d} \in Q(A)$, we have ($A$ integral domain) $ad = bc$ in A. Thus $|a||d| = |ad| = |bc| = |b||c|$ in $\mathbb{R}$ so $|\frac{a}{b}| = |\frac{c}{d}|$; proving well-definedss. By axiom 3, $|1| = |1 \cdot 1| = |1| \cdot |1|$ i.e. $|1| \in \mathbb{R}$ is idempotent so it is either 0 or 1. But because of axiom 2 ($1 \neq 0$), we have $|1| = 1$.
   So $|\cdot|$ on $Q(A)$ extends the absolute value on A: $|\frac{a}{1}| = \frac{|a|}{|1|} = |a|$.
   We have $|\frac{a}{b}| = \frac{|a|}{|b|} \geq 0$.
   If $|\frac{a}{b}| = \frac{|a|}{|b|} = 0 \in \mathbb{R}$ then $|a| = 0$ i.e. (axiom 2) $a = 0$. But then $\frac{a}{b} = \frac{0}{b} = 0 \in Q(A)$.
   A direct caluclation shows multiplicativity: $|\frac{a}{b} \cdot \frac{c}{d}| = |\frac{ac}{bd}| = \frac{|a||c|}{|b||d|} = |\frac{a}{b}||\frac{c}{d}|$.
   Finally
   $$|\frac{a}{b} + \frac{c}{d}| = |\frac{ad + bc}{bd}| = \frac{|ad + bc|}{|bd|} \leq \frac{|ad| + |bc|}{|bd|} = \frac{|a||d|}{|b||d|} + \frac{|b||c|}{|b||d|} = |\frac{a}{b}| + |\frac{c}{d}|$$

2. We have $\nu(\frac{a}{b}\cdot\frac{c}{d}) = -\log_\alpha(|\frac{a}{b}\cdot\frac{c}{d}|) = -\log_\alpha(\frac{|a||c|}{|b||d|}) = -\log_\alpha(|\frac{a}{b}|) - \log_\alpha(|\frac{c}{d}|) = \nu(\frac{a}{b}) + \nu(\frac{c}{d})$.

   We have

$$
\begin{aligned}
\nu(\frac{a}{b}+\frac{c}{d}) = \nu(\frac{ad+bc}{bd}) = -\log_\alpha(|ad+bc|) + \log_\alpha(|bd|) &\geq -\log_\alpha(\max(|ad|,|bc|)) + \log_\alpha(|bd|)\\
&= \min(-\log_\alpha(|ad|), -\log_\alpha(|bc|)) + \log_\alpha(|bd|)\\
&= \min(-\log_\alpha(\frac{|ad|}{|bd|}), -\log_\alpha(\frac{|bc|}{|bd|}))\\
&= \min(\nu(\frac{a}{b}), \nu(\frac{c}{d})).
\end{aligned}
$$

3. The inequality $|a+b| \leq \max(|a|,|b|)$ does not hold for $\mathbb{C}, |\cdot|$; indeed, $|1+i| = \sqrt{2} > 1 = |1|,\ 1 = |i|$. So $-\log_\alpha(|1+i|) = -\log_\alpha(\sqrt{2}) < -\log_\alpha(1)$ i.e. $-\log_\alpha(|\cdot|)$ does not satisfy Lemma 13.4 (i).

4. As in example 13.3 (iii), $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ admits the following description $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q},\ p \nmid b \text{ and } (a,b) = 1\}$. So set $|\cdot| : \mathbb{Z}_{(p)}\backslash\{0\} \to \mathbb{N}$, by $\frac{a}{b} \mapsto p^{-\nu(a)}$ where $(a,b)=1$, $a \neq 0$ and $\nu(a) = \max\{\ell \in \mathbb{N},\ p^\ell|a\}$ and extend by 0 at $0 \in \mathbb{Z}_{(p)}$. If $\frac{a}{b} \in \mathbb{Z}_{(p)}\backslash\{0\}$, we have $|\frac{a}{b}| = p^{-\nu(a)} > 0$ and $|0| = 0 \geq 0$. So $|\cdot|$ satisfies axioms 1 and 2.
   Moreover, $|\frac{a}{b}\cdot\frac{c}{d}| = |\frac{ac}{bd}|$, then $p \nmid bd$, so taking out common primes in the numerator and the denominator does not affect $\nu(ac)$, which is equal $\nu(a)\nu(c)$ as readily seen from the decomposition in primes. So $|\frac{a}{b}\cdot\frac{c}{d}| = p^{-\nu(a)\nu(c)} = p^{-\nu(a)}p^{-\nu(c)} = |\frac{a}{b}||\frac{c}{d}|$.
   Finally, $|\frac{a}{b}+\frac{c}{d}| = |\frac{ad+bc}{bd}|$ and again $p \nmid bd$; since $p \nmid d$, we have $\nu(ad) = \nu(a)$ and likewise $\nu(bc) = \nu(c)$. If $\nu(a) \leq \nu(c)$ (i.e. $|\frac{a}{b}| = p^{-\nu(a)} \geq p^{-\nu(c)} = |\frac{c}{d}$ in other words $|\frac{a}{b}| = \max(|\frac{a}{b}|,|\frac{c}{d}|)$), then $p^{\nu(a)}|ad+bc$ so $\nu(ad+bc) \geq \nu(a)$ i.e. $|\frac{ad+bc}{bc}| = p^{-\nu(ad+bc)} \leq p^{-\nu(a)} = |\frac{a}{b}| = \max(|\frac{a}{b}|,|\frac{c}{d}|)$. Likewise, one shows that when $\nu(a) > \nu(c)$, $\max(|\frac{a}{b}|,|\frac{c}{d}|) = |\frac{c}{d}|$ and $\nu(ad+bc) \geq \nu(c)$ i.e. $|\frac{ad+bc}{bd}| = p^{-\nu(ad+bc)} \leq p^{-\nu(c)} = \max(|\frac{a}{b}|,|\frac{c}{d}|)$. As a conclusion $|\cdot|$ satisfies the axioms for an absolute value with the strengthened axiom 4 of question (ii). In particular $-\log_p(|\cdot|)$ is a valuation on $\widetilde{\nu} := \mathbb{Q}^* = Q(\mathbb{Z}_{(p)})$, which is equal to ν on $\mathbb{Z}_{(p)}$ (direct calculation).

   Let us describe its valuation ring $\{\nu(\cdot) \geq 0\} \cup \{0\}$. Looking at the natural extension (question (i)) of $|\cdot|$ to $\mathbb{Q}$, we see that $\widetilde{\nu}(\frac{a}{b}) = \nu(a) - \nu(b)$. But can always take a representative for which $(a,b) = 1$, then p does not divide a and b i.e. $\nu(a)\nu(b) = 0$. Then from the formula, we see that $\widetilde{\nu}(\frac{a}{b}) \geq 0$ if and only if $\nu(b) = 0$ i.e. $p \nmid b$ i.e. $\frac{a}{b} \in \mathbb{Z}_{(p)}$.

Exercise 53. (Picard group, 6 points)

1. For $M, N \in \mathrm{Pic}(A)$, let us show that $M \otimes N \in \mathrm{Pic}(A)$: as M, N are finitely generated there are surjective homomorphism of A-modules $A^{\oplus m} \twoheadrightarrow M$ and $A^{\oplus n} \twoheadrightarrow N$ and since M, N are projective those homomorphisms admit a section (a homomorphism lifting the identity) i.e. M, N are direct summands of finite free A-modules $A^{\oplus m} = M \oplus P$, $A^{\oplus n} = N \oplus Q$. Then $A^{\oplus mn} = A^{\oplus m} \otimes A^{\oplus n} = M \otimes N \oplus (M \otimes Q \oplus P \otimes N \oplus P \otimes Q)$ i.e. $M \otimes N$ is a direct summand of a finite free A-module; thus $M \otimes N$ is a finite (look at the projection $A^{\oplus mn} \twoheadrightarrow M \otimes N$) projective module. Moreover for any $\mathfrak{p} \in \mathrm{Spec}(A)$, we have (see tensor identity (3) on exercise sheet 6 and solution to exercise 15)

$$(M \otimes_A N)_\mathfrak{p} \simeq M \otimes_A N \otimes_A A_\mathfrak{p} \simeq (M \otimes_A A_\mathfrak{p}) \otimes_{A_\mathfrak{p}} (N \otimes_A A_\mathfrak{p}) \simeq A_\mathfrak{p} \otimes_{A_\mathfrak{p}} A_\mathfrak{p} \simeq A_\mathfrak{p}.$$

   Associativity follows from associativity of tensor product.
   As a A-module A is obviously finite and free (hence projective) and $A_\mathfrak{p} \simeq A \otimes_A A_p p$; thus $A \in \mathrm{Pic}(A)$.
   Moreover for any $M \in \mathrm{Pic}(A)$, we have natural isomorphisms $M \otimes_A A \simeq M$ and

$A \otimes_A M \simeq M$.
For any $M \in \mathrm{Pic}(A)$, let us denote $M^{-1} := \mathrm{Hom}_A(M, A)$. As we have seen M is a direct summand of a finite free module: $A^{\oplus m} \simeq M \oplus P$; applying the functor $\mathrm{Hom}_A(\cdot, A)$ yields $A^{\oplus m} \simeq \mathrm{Hom}_A(A^{\oplus m}, A) \simeq \mathrm{Hom}_A(M, A) \oplus \mathrm{Hom}_A(P, A)$. So M^{-1} is a direct summand of a finite free module so it is finite and projective. Now, since for any finite free module, there is a natural isomorphism $\mathrm{Hom}(A^{\oplus k}, A) \simeq \prod_{i=1}^k \mathrm{Hom}(A, A) \simeq A^{\oplus k}$ for any $\mathfrak{p} \in \mathrm{Spec}(A)$, we get $\mathrm{Hom}(A^{\oplus k}, A)_\mathfrak{p} \simeq A^{\oplus k} \simeq A_\mathfrak{p} \simeq A_\mathfrak{p}^{\oplus k}$. The decomposition $A^{\oplus m} \simeq M \oplus P$ gives the exact sequence $0 \to P \to A^{\oplus m} \to M \to 0$. Composition the first homomorphism with the surjective homomorphism $A^{\oplus m} \twoheadrightarrow P$ given by the second projection, gives an exact sequence

$$A^{\oplus m} \xrightarrow{f} A^{\oplus m} \xrightarrow{g} M \to 0. \qquad (*)$$

Applying the functor $\mathrm{Hom}(\cdot, A)$ yields $0 \to \mathrm{Hom}_A(M, A) \xrightarrow{-\circ g} \mathrm{Hom}(A^{\oplus m}, A) \xrightarrow{-\circ f} \mathrm{Hom}(A^{\oplus m}, A)$ i.e. $\mathrm{Hom}(M, A)$ is the kernel of $- \circ f$. Since localization is an exact functor, for any $\mathfrak{p} \in \mathrm{Spec}(A)$, we get the exact sequence

$$0 \to \mathrm{Hom}_A(M, A)_\mathfrak{p} \xrightarrow{-\circ g_\mathfrak{p}} \underbrace{\mathrm{Hom}(A^{\oplus m}, A)_\mathfrak{p}}_{\simeq A_\mathfrak{p}^{\oplus m} \simeq \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}^{\oplus m}, A_\mathfrak{p})} \xrightarrow{-\circ f_\mathfrak{p}} \underbrace{\mathrm{Hom}(A^{\oplus m}, A)_\mathfrak{p}}_{\simeq A_\mathfrak{p}^{\oplus m} \simeq \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}^{\oplus m}, A_\mathfrak{p})}$$

i.e. $\mathrm{Hom}_A(M, A)_\mathfrak{p} \simeq \ker(- \circ f_\mathfrak{p})$. But tensoring (*) with $A_\mathfrak{p}$ yields the exact sequence: $A_\mathfrak{p}^{\oplus m} \xrightarrow{f_\mathfrak{p}} A_\mathfrak{p}^{\oplus m} \xrightarrow{g_\mathfrak{p}} M_\mathfrak{p} \to 0$; then applying $\mathrm{Hom}_{A_\mathfrak{p}}(\cdot, A_\mathfrak{p})$ gives the exact sequence $0 \to \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p}) \xrightarrow{-\circ g_\mathfrak{p}} \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}^{\oplus m}, A_\mathfrak{p}) \xrightarrow{-\circ f_\mathfrak{p}} \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}^{\oplus m}, A_\mathfrak{p})$ i.e. $\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p}) \simeq \ker(- \circ f_\mathfrak{p})$. As a conclusion, $\mathrm{Hom}_A(M, A)_\mathfrak{p} \simeq \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p})$. but by assumption $M_\mathfrak{p} \simeq A_\mathfrak{p}$; thus $\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p}) \simeq \mathrm{Hom}_{A_\mathfrak{p}}(A_\mathfrak{p}, A_\mathfrak{p}) \simeq A_\mathfrak{p}$. So $M^{-1} \in \mathrm{Pic}(A)$.

Moreover the natural homomorphism $c : \mathrm{Hom}_A(M, A) \otimes M \to A$, $\lambda \otimes m \mapsto \lambda(m)$ is an isomorphism: indeed we have an exact sequence $0 \to \ker(c) \to \mathrm{Hom}_A(M, A) \otimes M \xrightarrow{c} A \to \mathrm{coker}(c) \to 0$ so that tensoring with the flat A-algebra $A_\mathfrak{p}$, we get the exact sequence $0 \to \ker(c)_\mathfrak{p} \to \mathrm{Hom}_A(M, A)_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p} \xrightarrow{c_\mathfrak{p}} A_\mathfrak{p} \to \mathrm{coker}(c)_\mathfrak{p} \to 0$. But $c_\mathfrak{p} : \underbrace{\mathrm{Hom}_A(M, A)_\mathfrak{p} \otimes_{A_\mathfrak{p}} M_\mathfrak{p}}_{\simeq \mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p}) \otimes_{A_\mathfrak{p}} A_\mathfrak{p} \simeq A_\mathfrak{p}} \to A_\mathfrak{p}$ is an isomorphism (check it, the isomorphism $M_\mathfrak{p} \simeq A_\mathfrak{p}$ tells that there is a $m \in M_\mathfrak{p}$ such that $A_\mathfrak{p} \to M_\mathfrak{p}$, $a \mapsto am$ is an isomorphism). Thus for any $\mathfrak{p} \in \mathrm{Spec}(A)$, $\ker(c)_\mathfrak{p} = 0 = \mathrm{coker}(c)_\mathfrak{p}$ i.e. (Proposition 8.24) $\ker(c) = 0 = \mathrm{coker}(c)$.

2. Let $M \subset K$ be an invertible A-submodule and $N \subset K$ its inverse i.e. $M \cdot N = A$. In particular $1 \in A$ can be written

$$1 = \sum_{i=1}^k m_i n_i \qquad (**)$$

for some $m_i \in M$ and $n_i \in N$. Then for any $m \in M$, $m = \sum_{i=1}^k (\underbrace{mn_i}_{\in M \cdot N = A}) m_i$ in K i.e. $m_1, \ldots, m_k$ generate M as a A-module. So we have a surjective homomorphism of A-modules $f : A^k \twoheadrightarrow M$, $(a_1, \ldots, a_k) \mapsto \sum_i a_i m_i$. But using (**), we can also define a homomorphism of A-modules $g : M \to A^k$, $m \mapsto (mn_1, \ldots, mn_k)$ (straightforward to see that it is a homomorphism). Observe that for $m \in M$, $f(g(m)) = f((mn_1, \ldots, mn_k)) = \sum_{i=1}^k (mn_i) m_i$ which, as seen above, is equal to m. So $f \circ g = \mathrm{id}_M$ i.e. M is a direct summand of A^k; so M is a finite projective A-module.
Moreover, for any $\mathfrak{p} \in \mathrm{Spec}(A) \backslash \{(0)\}$, $A_\mathfrak{p}$ is a discrete valuation ring and $M_\mathfrak{p}$ an invertible $A_\mathfrak{p}$ submodule (by Lemma 14.15) of K; in particular it is fractional so there is a $a \in K$ such that $aM_\mathfrak{p} \subset A_\mathfrak{p}$ is an ideal. But as $A_\mathfrak{p}$ is a discrete valuation ring, according to Proposition 13.14, $aM_\mathfrak{p}$ is principal, of the form (t^ℓ), for $\ell \geq 0$ and $t \in \mathfrak{p}A_\mathfrak{p}$ a uniformizing parameter. So in K, we have $M_\mathfrak{p} \simeq (\frac{t^\ell}{a})$ as $A_\mathfrak{p}$-modules and the cyclic

$A_{\mathfrak{p}}$-module $\frac{t^\ell}{a} \cdot A_{\mathfrak{p}} \subset K$ is isomorphic to $A_{\mathfrak{p}}$ (look at $A_{\mathfrak{p}} \to \frac{t^\ell}{a} \cdot A_{\mathfrak{p}}$, $x \mapsto x\frac{t^\ell}{a}$) since it has no torsion (as submodule of a field). So $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}}$.
For $\mathfrak{p} = (0)$, by Lemma 14.15, $M_{(0)}$ is an invertible $A_{(0)} \simeq K$-submodule of K so $K \supset M_{(0)} \neq 0$ thus $M_{(0)} \simeq K = A_{(0)}$. As a conclusion $M \in \mathrm{Pic}(A)$.

Let us prove that this forgetful map respects the composition laws: let $M, N \subset K$ be invertible A-submodules. We can look at the homomorphism of A-modules $f : M \otimes_A N \to M \cdot N$, $m \otimes n \mapsto mn$. It is readily seen to be surjective. Now, for a $\mathfrak{p} \in \mathrm{Spec}(A)$, we have the localization $f_{\mathfrak{p}} : M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \to (M \cdot N)_{\mathfrak{p}}$; but $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \simeq (m \cdot A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} (n \cdot A_{\mathfrak{p}})$ where $m \in M_{\mathfrak{p}}$ (resp. $n \in N_{\mathfrak{p}}$) gives the isomorphism $A_{\mathfrak{p}} \simeq M_{\mathfrak{p}}$ (resp. $A_{\mathfrak{p}} \simeq N_{\mathfrak{p}}$). Since $M \cdot N$ is invertible, $(M \cdot N)_{\mathfrak{p}} \simeq A_{\mathfrak{p}}$ is a cyclic $A_{\mathfrak{p}}$-module and $(M \cdot N)_{\mathfrak{p}} \simeq M_{\mathfrak{p}} \cdot N_{\mathfrak{p}}$, it is generated by mn. So $f_{\mathfrak{p}}$ is an isomorphism; in particular $\ker(f_{\mathfrak{p}}) = 0$.
So $\ker(f)_{\mathfrak{p}} = 0$ for any $\mathfrak{p} \in \mathrm{Spec}(A)$ i.e. $\ker(f) = 0$; thus $M \otimes_A N \simeq M \cdot N$ as A-module.

If an invertible A-submodule $M \subset K$ is principal i.e. $M = \alpha \cdot A$ for some $\alpha \in K^*$, since the cyclic A-module $(\alpha) \subset K$ has no torsion (as a submodule of the field K), we have $A \simeq \alpha \cdot A$ as A-modules, so $M \simeq A$ as A-modules. But A is the neutral element of the group $\mathrm{Pic}(A)$. So the forgetful map $\mathrm{Cl}(A) \to \mathrm{Pic}(A)$ is a group homomorphism.

Surjectivity: if $M \in \mathrm{Pic}(A)$, then for any $a \in A \backslash \{0\}$, let us prove that $t_a : M \to M$, $m \mapsto am$ is injective: for any $\mathfrak{p} \in \mathrm{Spec}(A) \backslash \{(0)\}$, $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}} \cdot m_{\mathfrak{p}} \simeq A_{\mathfrak{p}}$ and since $A_{\mathfrak{p}}$ is an integral domain (and $A \hookrightarrow A_{\mathfrak{p}}$, all because A is an integral domain see for example Exercise 24(i)), $t_{a,\mathfrak{p}} : M_{\mathfrak{p}} \simeq A_{\mathfrak{p}} \to M_{\mathfrak{p}} \simeq A_{\mathfrak{p}}$ is injective; thus $\ker(t_a)_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m} \in \mathrm{Spec}(A)$ i.e. $\ker(t_a) = 0$.
As a consequence, the natural homomorphism $M \to M_{(0)}$ is injective: if $\frac{m}{1} \in M_{(0)}$ then there is a $a \in A \backslash \{0\}$ such that $am = 0$ in M. But we have seen that this implies that $m = 0$.

Moreover $M_{(0)} \simeq A_{(0)} \simeq K$, so M is isomorphic to a A-submodule of K. The isomorphism $M_{(0)} \simeq K$ is given by the datum of some $0 \neq \frac{m}{a} \in M_{(0)}$ (the preimage of 1) i.e. $K \simeq K \cdot \frac{m}{a} \simeq M_{(0)}$. Let $m_1, \ldots, m_k \in M$ be a set of generators of M as a A-module; since $M_{(0)}$ is cyclic, we have $\frac{m_i}{1} = \frac{b_i}{a_i}\frac{m}{a} \in M_{(0)}$ for some $b_i, a_i \in A$ ($a_i \neq 0$). Consider $\alpha = \Pi_{i=1}^k a_i \in A$; for any i, we have $\alpha \frac{m_i}{1} = b_i \Pi_{j \neq i} a_j \cdot \frac{m}{a}$, i.e. under the inclusion $M \hookrightarrow K = M_{(0)}$, $\alpha m_i \in A$ so M is isomorphic to a fractional ideal. Now since for any $\mathfrak{p} \in \mathrm{Spec}(A)$, $M_{\mathfrak{p}} \simeq A_{\mathfrak{p}}$ (so $M_{\mathfrak{p}}$ is in particular cyclic) and the localization is compatible with the inclusion $M \hookrightarrow K \simeq M_{(0)}$ i.e. $M \hookrightarrow M_{\mathfrak{p}} \hookrightarrow M_{(0)}$ (successive localizations with respect to $(0) \subset \mathfrak{p}$, see Exercise 28), $M_{\mathfrak{p}}$ is invertible. So according to Lemma 14.15, M is isomorphic to an invertible A-submodule of K; proving surjectivity.

Injectivity: Assume $M \in J(A)$ is sent to A by the forgetful map i.e. $M \simeq A$ as A-module, then M is cyclic (take the preimage of $1 \in A$), generated by some $m \in M \subset K$ i.e. $M \simeq m \cdot A \simeq A$. So $M \in P(A)$; proving injectivity.

Exercise 54. (Class number, 5 points)

1. For $\mathbb{Q}(i)$, $\mathcal{O}_K \simeq \mathbb{Z}[i]$. It is sufficient to prove that $\mathcal{O}_K$ is a principal ideal domain. Let us define $N : \mathbb{Q}[i] \to \mathbb{R}_{\geq 0}$, by the usual euclidean norm of $\mathbb{C}$ i.e. $a+ib \mapsto |a+ib|^2 = a^2+b^2$. Then it is an absolute value in the sense of Exercise 52. Let us prove that there is a Euclidean division in $\mathbb{Q}(i)$ i.e. given $z, z' \in \mathbb{Z}(i)$ with $z' \neq 0$, there are $q \in \mathbb{Z}(i)$ and $r \in \mathbb{Z}(i) \cap \{N(\cdot) < N(z')\}$ such that $z = qz' + r$: if $N(z) < N(z')$ take $q = 0$ and $r = z$. Otherwise, consider $\frac{z}{z'} = a + ib \in \mathbb{C}$ which by direct calculation sits in $\mathbb{Q}(i)$. Let us consider the closest integers $k, \ell \in \mathbb{Z}$ to respectively a and b i.e. $|k - a| \leq \frac{1}{2}$ and

$|\ell - b| \leq \frac{1}{2}$. Then

$$\begin{aligned}\frac{z}{z'} &= a + ib \\ &= (a-k) + i(b-\ell) + (k + i\ell)\end{aligned}$$

so that $z = (k+i\ell)z' + [(a-k)+i(b-\ell)]z'$. Since $z,\ k+i\ell,\ z' \in \mathbb{Z}[i]$, we get that $[(a-k)+i(b-\ell)]z' = z - (k+i\ell)z' \in \mathbb{Z}[i]$; moreover

$$\begin{aligned}N([(a-k)+i(b-\ell)]z') = N(z')N((a-k)+i(b-\ell)) &= N(z')[(a-k)^2+(b-\ell)^2] \\ &\leq N(z')\frac{1}{2} \\ &< N(z')\end{aligned}$$

proving the statement.
Let $M \subset \mathbb{Q}(i)$ be an invertible $\mathbb{Z}[i]$-submodule. Let $0 \neq a \in \mathbb{Q}(i)$ such that $aM \subset \mathbb{Z}[i]$, the non-empty set $\{N(x+iy) = x^2+y^2,\ 0 \neq x+iy \in aM\} \subset \mathbb{N}$ has a minimal element $d > 0$; let $x_0 + iy_0 \in aM$ such that $N(x_0+iy_0) = d$. For any $z \in aM \subset \mathbb{Z}[i]$, there are $q, r \in \mathbb{Z}[i]$ such that $z = q(x_0+iy_0) + r$ with $N(r) < N(x_0+iy_0) = d$. But since aM is an ideal $q(x_0+iy_0) \in aM$ and thus $r = z - q(x_0+iy_0) \in aM$; but definition of d, we must have $r = 0$ i.e. $z \in (x_0+iy_0)$; as a conclusion $aM = (x_0+iy_0)$. So $M = (\frac{x_0+iy_0}{a}) \subset \mathbb{Q}(i)$ is principal. So $h_{\mathbb{Q}(i)} = 1$.

2. For $\mathbb{Q}(\sqrt{-2})$, $\mathcal{O}_K \simeq \mathbb{Z}[\sqrt{-2}]$. Let us define $N : \mathbb{Q}[\sqrt{-2}] \to \mathbb{R}_{\geq 0}$ by $a+\sqrt{-2}b \mapsto a^2+2b^2$. If $N(a+\sqrt{-2}b) = 0$ then since $a^2 \geq 0$ and $b^2 \geq 0$, we have $a = 0 = b$.
A direct calculation shows that N is mutlplicative i.e.

$$\begin{aligned}N((a+\sqrt{-2}b)(c+\sqrt{-2}d)) &= N(ac-2bd+\sqrt{-2}(ad+bc)) \\ &= (ac-2bd)^2 + 2(ad+bc)^2 \\ &= (ac)^2 - 4abcd + 4(bd)^2 + 2(ad)^2 + 4abcd + 2(bc)^2 \\ &= (a^2+2b^2)(c^2+2d^2) \\ &= N(a+\sqrt{-2}b)N(c+\sqrt{-2}d)\end{aligned}$$

for any pair $a+\sqrt{-2}b,\ c+\sqrt{-2}d \in \mathbb{Z}[\sqrt{-2}]$ and it is not difficult to check the other property to show that N is an absolute value in the sense of Exercise 52.

Let us show that there is an Euclidean division in $\mathbb{Z}[\sqrt{-2}]$, the proof is the same as above: for any $z, z' \in \mathbb{Z}[\sqrt{-2}]$ with $z' \neq 0$, there is a pair $(q, r) \in \mathbb{Z}[\sqrt{-2}]$, such that $z = qz' + r$ and $N(r) < N(z')$.
If $N(z) < N(z')$ we are done ($q = 0$, $r = z$). Otherwise look at $\frac{z}{z'}$ which is in $QQ(\sqrt{-2})$ i.e. can be written $a + \sqrt{-2}b$, with $a, b \in \mathbb{Q}$. Let $k, \ell \in \mathbb{Z}$ the closest integers to resp. a and b i.e. $|a-k| \leq \frac{1}{2}$ and $|b-\ell| \leq \frac{1}{2}$. Then $z = (k+\sqrt{-2}\ell)z' + [(a-k)+\sqrt{-2}(b-\ell)]z'$; $z \in \mathbb{Z}[\sqrt{-2}]$, $z' \in \mathbb{Z}[\sqrt{-2}]$, $k+\sqrt{-2}\ell \in \mathbb{Z}[\sqrt{-2}]$, so that $[(a-k)+\sqrt{-2}(b-\ell)]z' \in \mathbb{Z}[\sqrt{-2}]$ and

$$\begin{aligned}N([(a-k)+\sqrt{-2}(b-\ell)]z') = N(z')N((a-k)+\sqrt{-2}(b-\ell)) &= N(z')[(a-k)^2+2(b-\ell)^2] \\ &\leq N(z')(\frac{1}{4}+\frac{1}{2}) \\ &= N(z')(\frac{3}{4}) \\ &< N(z')\end{aligned}$$

proving Euclidean division.
Conclude as done in the previous question.