Algebraic Curves : Solutions sheet 1

February 26, 2025

Exercise 1. Let R be a ring and $I \subsetneq R$ a proper ideal of R. A ring is called *reduced* if it does not contain any (non-zero) nilpotent element.

1. Show there is a bijection between the ideals of R/I and the ideals of R containing I.
2. Show that I is maximal if, and only if, R/I is a field.
3. Show that I is prime if, and only if, R/I is a domain.
4. Show that I is radical if, and only if, R/I is reduced.

Main idea.

1. Recall a similar statement for groups and the way to prove it.
2. If $\mathfrak{m}$ is a maximal ideal, then if $\mathfrak{m} \subsetneq J$ with J a bigger ideal, then $J = R$ and in particular $1 \in J$.
3. See the parallel in the definitions: in a prime ideal $\mathfrak{p}$, for all $a, b \in R$ such that $ab \in \mathfrak{p}$, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. In a domain, for all $a, b \in R$ such that $ab = 0$, $a = 0$ or $b = 0$.
4. Recall the definitions of radical ideals and reduced rings and try to parallel them.

Solution 1.
In general for this exercise, you can use the quotient map

$$\pi : R \longrightarrow R/I$$

which is a surjective ring morphism. It is helpful to transfer from one context to another.

1. The method consists of defining two maps of sets which are inverse to each other. The maps are given by the following:

$$\{I \subseteq I' \subseteq R \text{ ideal }\} \longleftrightarrow \{J \subseteq R/I \text{ ideal }\}$$
$$I' \longmapsto \pi(I')$$
$$\pi^{-1}(J) \longleftarrow J$$

   We need to check:

   - Well-defined:

  - if $I' \subseteq R$ is an ideal containing I, then $\pi(I')$ is an ideal in R/I.
  - if J is an ideal in R/I, then $\pi^{-1}(J)$ is an ideal of R containing I.
- Inverse: check that for $I \subseteq I' \subseteq R$, $\pi^{-1}(\pi(I')) = I'$. The inclusion $\pi^{-1}(\pi(I')) \subseteq I'$ requires crucially the hypothesis that $I \subset I'$.

2. Consider $x + \mathfrak{m} \in (R/\mathfrak{m}) \setminus \{0\}$. Then $x \notin \mathfrak{m}$, so that $\mathfrak{m} + (x) = R$, so there exists $a \in R, m \in \mathfrak{m}$ such that $1 = m + ax$. The multiplicative inverse of $x + \mathfrak{m}$ is then given by $a + \mathfrak{m}$. This way, we obtain an inverse for each non-zero element of $R/\mathfrak{m}$, which makes it a field. The proof of the converse is similar. We can also use the previous statement, then it is very direct but less intuitive.

3. If I is prime, let $a + I, b + I \in R/I$ be such that $(a + I)(b + I) = 0$. This implies that $ab \in I$. As I is prime, either a or b is in I, and so either $a + I$ or $b + I$ is zero in R/I. The proof of the converse is similar.

4. A similar reasoning works.

Exercise 2. Let R be a ring, S a multiplicative subset of R and M an R-module. Define the localization of M as the set $S^{-1}M = \{\frac{m}{s},\ m \in M,\ s \in S\}/\sim$, where: $\frac{m}{s} \sim \frac{m'}{s'} \Leftrightarrow \exists t \in S,\ t \cdot (s' \cdot m - s \cdot m') = 0$

1. Check that the relation $\sim$ defined above is indeed an equivalence relation and that $S^{-1}M$ is an $S^{-1}R$-module.

2. Show that localization preserves short exact sequences i.e. if

$$0 \to L \to M \to N \to 0$$

is an exact sequence of R-modules, then

$$0 \to S^{-1}L \to S^{-1}M \to S^{-1}N \to 0$$

is an exact sequence of $S^{-1}R$-modules.

3. Let $I \subset R$ be an ideal of R. Show that $S^{-1}I$ is an ideal of $S^{-1}R$ and that we have an isomorphism of rings

$$S^{-1}R/S^{-1}I \simeq (S/I)^{-1}(R/I),$$

where S/I denotes the image of S in R/I.

Solution 2.

1. - To check that this defines an equivalence relation, you need reflexivity, symmetry and transitivity. Reflexivity and symmetry are straightforward. Transitivity can be checked as follows: let $\frac{m_1}{s_1} \sim \frac{m_2}{s_2}$ and $\frac{m_2}{s_2} \sim \frac{m_3}{s_3}$. There are $t_1, t_2 \in R$ such that

$$t_1(s_2 m_1 - s_1 m_2) = 0$$
$$t_2(s_3 m_2 - s_2 m_3) = 0.$$

To cancel the m_2 we multiply the first equation by $t_2 s_3$ and the second by $t_1 s_1$ and add them together, giving

$$0 = t_1 t_2 s_3 (s_2 m_1 - s_1 m_2) + t_1 t_2 s_1 (s_3 m_2 - s_2 m_3) = t_1 t_2 s_2 s_3 m_1 - t_1 t_2 s_2 s_1 m_3 = t_1 t_2 s_2 (s_3 m_1 - s_1 m_3).$$

Hence we obtain $\frac{m_1}{s_1} \sim \frac{m_3}{s_3}$.

- **Direct approach:** $S^{-1}M$ is an $S^{-1}R$–module. We first have to endow $S^{-1}M$ with the structure of an abelian group: for $\frac{m_1}{s_1}, \frac{m_2}{s_2} \in S^{-1}M$ we define

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} := \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}.$$

First, we have to check that this doesn't depend on the choice of representative: assume $\frac{m_1}{s_1} \sim \frac{m_1'}{s_1'}$ and $\frac{m_2}{s_2} \sim \frac{m_2'}{s_2'}$, i.e. there exist $t_1, t_2 \in R$ such $t_1(s_1' m_1 - s_1 m_1') = 0$ and $t_2(s_2' m_2 - s_2 m_2') = 0$. We have to check that $\frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \sim \frac{s_2' m_1' + s_1' m_2'}{s_1' s_2'}$. To this end, notice that

$$t_1 t_2 (s_1' s_2')(s_2 m_1 + s_1 m_2) = t_2 s_2' s_2 \underbrace{(t_1 s_1' m_1)}_{= t_1 s_1 m_1'} + t_1 s_1' s_1 \underbrace{(t_2 s_2' m_2)}_{= t_2 s_2 m_2'} = t_1 t_2 (s_1 s_2)(s_2' m_1' + s_1' m_2').$$

Hence we conclude $\frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \sim \frac{s_2' m_1' + s_1' m_2'}{s_1' s_2'}$, so $+$ is well-defined on $S^{-1}M$. Using that M is an abelian group, it is then straightforward to check that $(S^{-1}M, +)$ is an abelian group with neutral element $\frac{0}{1}$ (and the additive inverse of $\frac{m}{s} \in S^{-1}M$ is $\frac{-m}{s}$).
In the next step, we endow $S^{-1}M$ with the structure of an $S^{-1}R$–module. For $\frac{r}{\sigma} \in S^{-1}R$ and $\frac{m}{s} \in S^{-1}M$ we define

$$\frac{r}{\sigma} \cdot \frac{m}{s} := \frac{rm}{\sigma s}.$$

Again we need to check that this is well-defined; to do so, take $\frac{r}{\sigma} \sim \frac{r'}{\sigma'}$ and $\frac{m}{s} \sim \frac{m'}{s'}$, i.e. there exist $\tau, t \in S$ such that $\tau(\sigma' r - \sigma r') = 0$ and $t(s' m - s m') = 0$. Therefore, we obtain

$$\tau t (\sigma' s' r m) = (\tau \sigma' r)(t s' m) = (\tau \sigma r')(t s m') = \tau t (\sigma s r' m'),$$

and thus $\frac{rm}{\sigma s} \sim \frac{r' m'}{\sigma' s'}$. Hence, scalar multiplication on $S^{-1}M$ is well-defined. Using that M is an R–module, it is then straightforward to check that $S^{-1}M$ is an $S^{-1}R$–module with this scalar multiplication, i.e. distributivity, associativity and multiplication by 1 is the identity.
More conceptual approach: While the above proof is more or less straightforward, it is a bit tedious, as we even have to check that $S^{-1}M$ is an abelian group. Here is a construction which is a bit more complicated, but where a lot of these things come for free: consider the R–module $M^{\oplus S}$, i.e. the direct sum of M with itself for every element of S. For $s \in S$ and $m \in M$, denote by $\iota_s(m) \in M^{\oplus S}$ the element which is m in the component corresponding to s and 0 otherwise. Now consider the R–submodule K of

$M^{\oplus S}$ defined by

$$K \coloneqq \langle \iota_s(m) - \iota_{s'}(m') \mid \exists t \in S\colon\ t(s'm - sm') = 0 \rangle.$$

Then in fact the R–module $M^{\oplus S}/K$ is isomorphic to $S^{-1}M$ constructed above, viewed as an R–module. Indeed, one can check that for every $s \in S$, the map $M \to S^{-1}M$ sending m to $\frac{m}{s}$ is a map of R–modules. By the universal property of the direct sum, we obtain a map $M^{\oplus S} \to S^{-1}M$ sending $\iota_s(m)$ to $\frac{m}{s}$, and by definition of $S^{-1}M$ we have that K is in the kernel. Hence we obtain an induced map $\varphi\colon M^{\oplus S}/K \to S^{-1}M$ sending $\iota_s(m) + K$ to $\frac{m}{s}$. This is a surjective morphism of R–modules, so to conclude it remains to show injectivity. This is the only tricky part. In fact, notice that every element $\sum_{s\in S} \iota_s(m_s) + K$ of $M^{\oplus S}/K$ can be written as $\iota_{s_0}(m_0) + K$ for some $s_0 \in S$ and $m_0 \in M$. Indeed, notice that we have

$$\iota_s(m) + \iota_{s'}(m') - \iota_{ss'}(s'm + sm') = \underbrace{\iota_s(m) - \iota_{ss'}(s'm)}_{\in K} + \underbrace{\iota_{s'}(m') - \iota_{ss'}(sm')}_{\in K} \in K.$$

Hence we have $\iota_s(m) + \iota_{s'}(m') + K = \iota_{ss'}(s'm + sm') + K$, so we can inductively reduce the number of summands required. So suppose we have $\varphi(x) = 0$ for some $x \in M^{\oplus S}/K$, and by the above write $x = \iota_s(m) + K$ for some $m \in M$ and $s \in S$. Then $0 = \varphi(x) = \frac{m}{s}$, so there exists $t \in S$ with $tm = 0$. But then $\iota_s(m) = \iota_s(m) - \iota_1(0)$ is in K, so $x = 0$. Hence φ is an isomorphism.

Therefore, we could have also defined $S^{-1}M$ as $M^{\oplus S}/K$, and then we immediately obtain that it is an R–module. To obtain the $S^{-1}R$–module structure, you can then observe that the corresponding ring map $R \to \mathrm{End}_{\mathbf{Ab}}(S^{-1}M)$ sends elements of S to units, and thus induces a ring map $S^{-1}R \to \mathrm{End}_{\mathbf{Ab}}(S^{-1}M)$ by the universal property of localiztion.

Remark. As for the localization of a ring, the localization of a module has a universal property: denote by $i\colon M \to S^{-1}M$ the map $m \mapsto \frac{m}{1}$ (this is a morphism of R–modules). Then for every R–module N such that for all $s \in S$ the map $n \in N \mapsto sn \in N$ is an isomorphism and every morphism $f\colon M \to N$ of R–modules there exists a unique morphism $g\colon S^{-1}M \to N$ such that $f = g \circ i$. Furthermore, every such N naturally admits the structure of an $S^{-1}R$–module (if $\mu_s\colon N \to N$ denotes multiplication by s, we define $\frac{r}{s} \cdot n \coloneqq \mu_s^{-1}(rn)$) and g is a morphism of $S^{-1}R$–modules. This is what you should use to define a morphism out of $S^{-1}M$.

2. Denote $f\colon L \to M$ and $g\colon M \to N$. There is a preliminary step for this proof, which is to understand that localization is functorial, i.e. a morphism of $R-$modules $f : L \to M$ induces a morphism of $S^{-1}R$–modules $S^{-1}f : S^{-1}L \to S^{-1}M$, defined by

$$\frac{x}{s} \longmapsto \frac{f(x)}{s}$$

Check that it is well-defined. You should also check that for $f\colon L \to M$ and $g\colon M \to N$ we have $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$ and $S^{-1}\,\mathrm{id}_M = \mathrm{id}_{S^{-1}M}$ (this is also part of being functorial). Instead of constructing and checking this by hand, you can also invoke the universal property: the composition $L \to M \to S^{-1}M$ is a morphism of L to a module where multiplication by any element of S is an isomorphism, and thus it induces $S^{-1}L \to S^{-1}M$ a morphism of $S^{-1}R$–modules. The uniqueness in the universal property gives you the part about composition and identity.

Now we check the exactness:

- Note that any localization of the zero module is the zero module, and any localization of the zero morphism is the zero morphism. Hence applying S^{-1} to the sequence and using functoriality, we still obtain a sequence

$$0 \to S^{-1}L \to S^{-1}M \to S^{-1}N \to 0$$

(i.e. the composition of two consecutive arrows is 0).

- For exactness at $S^{-1}L$, suppose that $S^{-1}f\left(\frac{l}{s}\right) = 0$ for some $\frac{l}{s} \in S^{-1}L$. Then $\frac{f(l)}{s} = 0$ in $S^{-1}M$, so there exists $t \in S$ such that $tf(l) = 0$. By injectivity of f we obtain $tl = 0$, and thus $\frac{l}{s} = 0$. Hence $S^{-1}f$ is injective.
- For exactness at $S^{-1}M$, consider $\frac{m}{s} \in \ker S^{-1}g$. That is, there exists $t \in S$ such that $tg(m) = 0$. By exactness of the original sequence, there exists $l \in L$ such that $f(l) = tm$. One can then check that $S^{-1}f\left(\frac{l}{st}\right) = \frac{m}{s}$.
- For exactness at $S^{-1}N$, let $\frac{n}{s} \in S^{-1}N$ be arbitrary. Then there exists $m \in N$ such that $g(m) = n$, so $S^{-1}g\left(\frac{m}{s}\right) = \frac{n}{s}$.

3. **Direct approach:** By exactness, the injection $I \to R$ induces an injection $S^{-1}I \to S^{-1}R$ (sending $\frac{i}{s} \in S^{-1}I$ to $\frac{i}{s} \in S^{-1}R$), so it is indeed an ideal. We now directly construct the isomorphism: consider the composition $R \to R/I \to (S/I)^{-1}(R/I)$. An element $s \in S$ is mapped to $\frac{s+I}{1+I}$, which is a unit (with inverse $\frac{1+I}{s+I}$). By the universal property of localization, we obtain a morphism of rings $S^{-1}R \to (S/I)^{-1}(R/I)$, sending $\frac{r}{s}$ to $\frac{r+I}{s+I}$. An arbitrary element $\frac{i}{s} \in S^{-1}I$ is mapped to $\frac{i+I}{s+I} = 0$, so we obtain an induced morphism of rings $\varphi\colon S^{-1}R/S^{-1}I \to (S/I)^{-1}(R/I)$, sending $\frac{r}{s} + S^{-1}I$ to $\frac{r+I}{s+I}$.

   On the other hand consider the composition $R \to S^{-1}R \to S^{-1}R/S^{-1}I$. An arbitrary element $i \in I$ is mapped to $\frac{i}{1} + S^{-1}I = 0$, so we obtain an induced map $R/I \to S^{-1}R/S^{-1}I$ sending $r + I$ to $\frac{r}{1} + S^{-1}I$. Then, an arbitrary element $s + I$ of S/I is mapped to $\frac{s}{1} + S^{-1}I$, which is a unit (with inverse $\frac{1}{s} + S^{-1}I$). Hence by the universal property of localization, we obtain a morphism of rings $\psi\colon (S/I)^{-1}(R/I) \to S^{-1}R/S^{-1}I$ sending $\frac{r+I}{s+I}$ to $\frac{r}{s} + S^{-1}I$. Hence φ and ψ are mutually inverse ring morphisms.

   Conceptual approach: We can use the previous question with the short exact sequence

$$0 \to I \to R \to R/I \to 0.$$

   Hence,

$$0 \to S^{-1}I \to S^{-1}R \to S^{-1}(R/I) \to 0$$

   is an exact sequence of $S^{-1}R$–modules. We get directly that $S^{-1}I$ is a $S^{-1}R$–submodule of $S^{-1}R$, which is precisely the definition of an ideal. It also described our quotient as $S^{-1}(R/I)$, which a priori is only a module. So the last step is to understand what happens when localizing an R–algebra, i.e. a ring A with a ring map $\sigma\colon R \to A$, which we view as an R–module through $r \cdot a := \sigma(r)a$. One can check that the $S^{-1}R$–module $S^{-1}A$ carries a natural multiplication, defined by $\frac{a}{s} \cdot \frac{a'}{s'} := \frac{aa'}{ss'}$ (again, check that this is well-defined). Then, one checks that this makes $S^{-1}A$ into a ring.

   But there is also another way one can construct a ring out of S and A: the image $\sigma(S)$ of S in A is a multiplicative subset, and so we can form the localization $\sigma(S)^{-1}A$. It remains to check that this is isomorphic to the ring $S^{-1}A$ constructed above: one checks that the map $A \to S^{-1}A$ is a morphism of rings and sends an element $\sigma(s) \in \sigma(S)$ to $\frac{\sigma(s)}{1}$, which is a unit with inverse $\frac{1}{s}$. Hence we obtain an induced ring morphism $\sigma(S)^{-1}A \to S^{-1}A$ sending $\frac{a}{\sigma(s)}$ to $\frac{a}{s}$. It is clearly surjective, and from the definition of the equivalence relation one can check that it is also injective.

Applying the above to $A = R/I$ and the quotient map $\sigma\colon R \to R/I$, we obtain that $S^{-1}(R/I)$ has a natural ring structure and is isomorphic as a ring to $\sigma(S)^{-1}(R/I) = (S/I)^{-1}(R/I)$.

Exercise 3. Show that, for any exact sequence of finite-dimensional vector spaces:

$$0 \to V_1 \to V_2 \to \ldots \to V_n \to 0$$

the following relation holds:

$$\sum_{i=1}^{n} (-1)^i \cdot \dim(V_i) = 0$$

Solution 3. We give a names to the maps in the sequence as follows

$$0 \to V_1 \xrightarrow{d_1} V_2 \xrightarrow{d_2} \ldots \xrightarrow{d_{n-1}} V_n \xrightarrow{d_n} 0 \xrightarrow{d_{n+1}} 0.$$

By the rank theorem and definition of exact sequences, we obtain

$$\dim V_i = \dim\ker d_i + \dim \underbrace{\operatorname{im} d_i}_{=\ker d_{i+1}} = \dim\ker d_i + \dim\ker d_{i+1}$$

for all i. Therefore, it follows that

$$\begin{aligned}
\sum_{i=1}^{n} (-1)^i \cdot \dim(V_i) &= \sum_{i=1}^{n} (-1)^i (\dim\ker d_i + \dim\ker d_{i+1}) \\
&= \sum_{i=1}^{n} (-1)^i \dim\ker d_i - \sum_{i=2}^{n+1} (-1)^i \dim\ker d_i \\
&= -\dim\ker d_1 - (-1)^{n+1} \dim\ker d_{n+1} \\
&= 0.
\end{aligned}$$

Exercise 4.

1. Let k be an infinite field, $F \in k[X_1, ..., X_n]$. Suppose $F(a_1, ..., a_n) = 0$ for all $a_1, ..., a_n \in k$. Show that $F = 0$.
2. Give an example showing that a similar result doesn't hold for a finite field.

Main idea.

1. Use induction.
2. Use Fermat's little theorem.

Solution 4.

1. - Base case : if $F \in k[X]$ is of degree $n \geq 1$, it has at most n roots so if k is infinite, there are $a \in k$, $f(a) \neq 0$. If f is constant, it is clear that the hypothesis implies $f = 0$.
   - Induction step : assume the statement holds for $k[X_1, \ldots, X_n]$. Let $F \in k[X_1, \ldots, X_n, X_{n+1}] \simeq k[X_1, \ldots, X_n][X_{n+1}]$ satisfying $F(a_1, ..., a_{n+1}) = 0$ for all $a_1, ..., a_{n+1} \in k$. We call $f_i \in k[X_1, \ldots, X_n]$ the coefficient of X_{n+1}^i in F, for $0 \leq i \leq \deg_{X_{n+1}} F$. For all $(a_1, \ldots, a_n) \in k^n$, $F(a_1, \ldots, a_n, X_{n+1})$, is a polynomial in one variable which vanishes at all $a_{n+1} \in k$, so it is 0. Thus for all $(a_1, \ldots, a_n) \in k^n$, $f_i(a_1, \ldots, a_n) = 0$. By induction hypothesis, $f_i = 0$ so $F = 0$.

2. $X^p - X$ in $\mathbb{F}_p[X]$ is zero at all elements of $\mathbb{F}_p$. But it is not zero in the polynomial ring.

Exercise 5. Let $F \in k[X_1, \ldots, X_n]$ be homogeneous of degree d. Show that:

$$\sum_{i=1}^{n} X_i \cdot \frac{\partial F}{\partial X_i} = d \cdot F$$

Solution 5.
By linearity, it suffices to prove it for monomials $F = X_1^{i_1} \cdots X_n^{i_n}$. Then, given $j \in \{1, \ldots, n\}$, we see

$$\frac{\partial F}{\partial X_j} = i_j X_1^{i_1} \cdots X_j^{i_j - 1} \cdots X_n^{i_n}$$

and thus

$$X_j \cdot \frac{\partial F}{\partial X_j} = i_j F.$$

Hence we have

$$\sum_{j=1}^{n} X_i \cdot \frac{\partial F}{\partial X_j} = \left(\sum_{i=1}^{n} i_j \right) \cdot F$$

If F has degree d then $\sum_{j=1}^{n} i_j = d$ and we are done.