Commutative Algebra - Assignment 1

Matteo Durante, 2303760, Leiden University
Waifod@protonmail.com

14th October 2018

Exercise 1

In this proof we will prove that the hypothesis of [1, cor. 3.2] are satisfied for the natural ring homomorphism $A \xrightarrow{g} A[x]/(xf-1)$ s.t. $a \mapsto a$ and thus find the desired A-algebra isomorphism $A_f \xrightarrow{h} A[x]/(xf-1)$.

First, observe that $g(f^n) = (g(f))^n$ has inverse x^n in $A[x]/(xf-1)$, for $xf = 1$.

Furthermore, the elements of $A[x]/(xf-1)$ have a representative of the form $b = \sum_{i=0}^n a_i x^i$, $a_i \in A$, hence, rewriting the representative as $b = \sum_{i=0}^n a_i f^{n-i} x^n = (\sum_{i=0}^n a_i f^{n-i}) x^n$, we get that $b = g(\sum_{i=0}^n a_i f^{n-i})(g(f^n))^{-1}$.

Suppose that $g(a) = 0$. This means that, for some $p = \sum_{i=0}^n a_i x^i$, $a = p(xf-1)$ in $A[x]$, i.e. $a = -a_0$, $\forall i < n$ we have that $a_{i+1} = a_i f$ and finally $a_n f = 0$. Inductively, we get that $a_n = a_0 f^n = -af^n$, and in particular $0 = -a_n f = af^{n+1}$, which concludes the proof.

Now, we have shown that there is a canonical A-algebra isomorphism (indeed, by the same proposition, $hi = g$, where $i : A \to A_f$ is the natural arrow) $A_f \xrightarrow{h} A[x]/(xf-1)$, which is defined as $h(a/f^n) = g(a)g(f^n)^{-1}$.

Exercise 2

(a) We know that A/aA is an A-module, hence we will prove that $A/aA \otimes_A M \cong M/aM$ and later use this result.

Consider a flat A-module M. Then, applying the exact functor $-\otimes_A M$, we get the following exact sequence:

$$0 \to aA \otimes_A M \xrightarrow{i} A \otimes_A M \to A/aA \otimes_A M \to 0$$

Being the sequence exact, $A/aA \otimes_A M \cong (A \otimes_A M)/\operatorname{Im}(i)$. Knowing that $A \otimes_A M \cong M$ and the canonical isomorphism sends $b \otimes_A m$ to bm, we have that $\operatorname{Im}(i)$ is sent to aM, hence $A/aA \otimes_A M \cong M/aM$.

Applying this to the case $M = A/aA$, we see that $A/aA \otimes_A A/aA \cong (A/aA)/(aA/aA) \cong A/aA$.

Applying the exact functor $-\otimes_A A/aA$ to the original exact sequence, we get the following one:

$$0 \to aA \otimes_A A/aA \to A \otimes_A A/aA \to A/aA \otimes_A A/aA \to 0$$

This, thanks to the isomorphisms previously remarked, becomes:

$$0 \to aA \otimes_A A/aA \to A/aA \xrightarrow{Id_{A/aA}} A/aA \to 0$$

Indeed, $b \in A/aA$ in is sent through $1 \otimes_A b \in A \otimes_A A/aA$ to $1 \otimes_A b \in A/aA \otimes_A A/aA$ and finally in $b \in A/aA$.

By exactness, $aA \otimes_A A/aA \cong 0$.

(b) Consider the following exact sequence:

$$0 \to aA \to A \to A/aA \to 0$$

Apply the right-exact functor $- \otimes_A aA$:

$$aA \otimes_A aA \to A \otimes_A aA \to A/aA \otimes_A aA \to 0$$

Remembering the previously shown isomorphisms, this becomes:

$$aA \otimes_A aA \to aA \to 0 \to 0$$

Now, notice that the induced epimorphism $aA \otimes_A aA \to A \otimes_A aA \xrightarrow{\sim} aA$ is such that $ab \otimes_A ab'$ is sent to $ab \otimes_A ab'$ and finally to a^2bb', hence its image is precisely a^2A (we may pick $b' = 1$) and it is equal, by exactness, to aA. It follows that the inclusion $a^2A \to aA$ is an epimorphism making the desired sequence exact.

(c) Being the last sequence exact, since all of aA is mapped to 0, there must be an element $a^2b \in a^2A$ s.t. $a = a^2b$.

Exercise 3

(a) Let $f \in \mathbb{Q}[x]$. Fixate a representation where each numerator is coprime to its denominator, which we require to be positive. Then, there exist some $N \in \mathbb{Z}_{>0}$ s.t. $Nf \in \mathbb{Z}[x]$. Let N be the minimum among them, M another one. Then, to be the minimum, N will be the lcm among all the denominators, while M will have to be divisible by N.

$$\begin{aligned}
\frac{1}{M}\operatorname{cont}(Mf) &= \frac{1}{M}\gcd(Mq_0, \ldots, Mq_n) \\
&= \frac{N}{M}\frac{1}{N}\gcd(\frac{M}{N}Nq_0, \ldots, \frac{M}{N}Nq_n) \\
&= \frac{N}{M}\frac{1}{N}\frac{M}{N}\operatorname{cont}(Nq_0, \ldots, Nq_n) \\
&= \frac{1}{N}\gcd(Nq_0, \ldots, Nq_n) \\
&= \frac{1}{N}\operatorname{cont}(Nf)
\end{aligned}$$

This proves that our function does not depend on the choice of M for each $f \in \mathbb{Q}[x]$.

Now notice that, $\forall n \in \mathbb{Z} \setminus \{0\}$, chosen an N big enough, s.t. $Nf \in \mathbb{Z}[x]$, we get that:

$$\operatorname{cont}(nf) = \frac{1}{N}\gcd(Nnq_0, \ldots, Nnq_n) = n\frac{1}{N}\gcd(Nq_0, \ldots, Nq_n) = n\operatorname{cont}(f)$$

Thanks to this, we may assume that f is a polynomial in $\mathbb{Z}[x]$ while computing.

Since $f \in \mathbb{Z}[x]$, we have that $f = \operatorname{cont}(f)f'$, $f' \in \mathbb{Z}[x]$ (we are taking $f' = f/\operatorname{cont}(f)$, i.e. dividing the coefficients by their gcd, s.t. f' is a primitive polynomial). Doing the same for g, we have $fg = \operatorname{cont}(f)\operatorname{cont}(g)f'g'$. Since the product of two primitive polynomials is primitive, we get that $\operatorname{cont}(fg) = \operatorname{cont}(\operatorname{cont}(f)\operatorname{cont}(g)f'g') = \operatorname{cont}(f)\operatorname{cont}(g)\operatorname{cont}(f'g') = \operatorname{cont}(f)\operatorname{cont}(g)$.

(b) Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{Z}[x]$ and suppose $\mathfrak{m}\cap\mathbb{Z} = (0)$. Let $\mathfrak{m}'$ be a maximal ideal of $\mathbb{Q}[x]$ containing $\mathfrak{m}$. It is a proper ideal of $\mathbb{Q}[x]$ because it doesn't contain any units, hence $\mathfrak{m}'\cap\mathbb{Z}[x] = \mathfrak{m}$ (for otherwise it would be a proper ideal of $\mathbb{Z}[x]$ containing $\mathfrak{m}$) with $\mathfrak{m}' = (f(x))$, $\deg(f) > 0$, where f is irreducible in $\mathbb{Q}[x]$ and hence in $\mathbb{Z}[x]$. Without loss of generality, let $f \in \mathbb{Z}[x]$, $\operatorname{cont}(f) = 1$ (we can do this by looking at the arguments given earlier in point (a); furthermore, by an argument I am about to give, $\operatorname{cont}(f) = 1$ is a necessary requirement to be irreducible in $\mathbb{Z}[x]$).

We will show that $\mathfrak{m} = (f(x))$.

Let $h \in \mathfrak{m}$ be an irreducible polynomial $\mathbb{Z}[x]$. It has to have content 1, for otherwise it would be divisible by a non-invertible element of $\mathbb{Z}$ and a polynomial of degree greater than 0, which are both non-invertible elements of $\mathbb{Z}[x]$. It is a multiple of f by an element of $\mathbb{Q}[x]$, $h = fg$. This element, since $\operatorname{cont}(h) = \operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$, has to have $\operatorname{cont}(g) = 1$.

If $g \in \mathbb{Z}[x]$, then we are done. Suppose $g \notin \mathbb{Z}[x]$. Then, there would be an $n \in \mathbb{Z}_{>0}$ s.t. $ng \in \mathbb{Z}[x]$, thus $nh = nfg$. Being $\mathbb{Z}[x]$ a UFD, since f is irreducible and hence prime, $nh \in (f)$ implies that $h \in (f)$, for otherwise $n \in (f) \subset \mathfrak{m}$, against the assumption. It follows that $(f) = \mathfrak{m}$ because, given any element of $\mathfrak{m}$, there is an irreducible factor in $\mathfrak{m}$.

Now, we prove that $\mathbb{Z}[x]/(f(x))$ is not a field. Let $a \in \mathbb{Z}$ be s.t. $f(a) \notin \mathbb{Z} \setminus \{0, \pm 1\}$, while p is prime dividing $f(a)$. Consider $\phi : \mathbb{Z}[x] \to \mathbb{F}_p$, the unique homomorphism with $\phi(x) = [a]$.

ϕ factors through $\mathbb{Z}[x]/(f(x))$ because $\phi(f(a)) = [f(a)] = [0]$. Since $\mathbb{Z}[x]/(f(x))$ is infinite, the induced map $\tilde{\phi} : \mathbb{Z}[x]/(f(x)) \to \mathbb{F}_p$ is not bijective.

Now, we want to show that $\tilde{\phi}$ is not the zero-map, such that $\ker(\tilde{\phi})$ will be a non-trivial ideal of $\mathbb{Z}[x]/(f(x))$, which therefore will not be a field.

If it was the zero-map, then $\tilde{\phi}(1) = 0$, i.e. there would be $u, v \in \mathbb{Z}[x]$ s.t. $1 = u(x)f(x) + pv(x)$. Choosing $x = a$, we get $1 = u(a)f(a) + pv(a)$, which is divisible by p and at the same time equal to 1, hence the map can't be trivial.

(c) Now, assume that $\mathfrak{m}\cap\mathbb{Z} \neq (0)$. Since $\mathbb{Z}/(\mathfrak{m}\cap\mathbb{Z})$ injects into $\mathbb{Z}[x]/\mathfrak{m}$, it is a domain, hence $\mathfrak{m}\cap\mathbb{Z}$ is prime in $\mathbb{Z}$ and $\mathfrak{m}\cap\mathbb{Z} = (p)$, where p is prime.

Let $\mathfrak{m}'$ be the image of $\mathfrak{m}$ in $\mathbb{F}_p[x]$ (under the epimorphism). By the 1:1 correspondence between the ideals containing the kernel and the ones in the codomain, composing the projections, we get the isomorphism $\mathbb{Z}[x]/\mathfrak{m} \cong \mathbb{F}_p[x]/\mathfrak{m}'$. It follows that, since $\mathbb{F}_p[x]$ is a PID, $\mathfrak{m}' = (f(x))$, where $f(x) \in \mathbb{F}_p[x]$ is irreducible.

Now, let $g(x) \in \mathbb{Z}[x]$ be s.t. $g(x) = f(x) \mod p$. Clearly, $\mathfrak{m} = (p, g(x))$, and the proof is finished.

References

[1] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, CRC Press, 1994.