Algebraic Geometry Assignment 1

Liam Carroll - 830916

Due Date: 20th August 2020

1 Sets

Q4. Relative Diagonal

For maps $p : X \to Z$ and $q : Y \to Z$ define the fiber product of p and q as

$$X \times_{p,Z,q} Y = \{(x, y) \in X \times Y : p(x) = q(y)\} . \tag{1.4.1}$$

Let $f : X \to Y$ be a map of sets. Let

$$\Delta_f : X \to X \times_{f,Y,f} X : x \mapsto (x, x) \tag{1.4.2}$$

be the induced relative diagonal map.

Part a)

Suppose for $x, x' \in X$ we have $\Delta_f(x) = \Delta_f(x')$, then $(x, x) = (x', x')$ as elements of $X \times X$, thus we necessarily have $x = x'$ and so Δ_f is always injective.

Part b)

Suppose Δ_f is surjective. Then for all $(x, x') \in X \times_{f,Y,f} X$, there is some $z \in X$ such that $\Delta_f(z) = (x, x')$, where we necessarily have $f(x) = f(x')$ by definition of of the fiber product. But then

$$\Delta_f(z) = (z, z) = (x, x') , \tag{1.4.3}$$

so by the transitivity of equality we must have $x = x'$ and so f itself is injective.

Suppose f is injective, then every element of $X \times_{f,Y,f} X$ must be of the form (x, x) for some $x \in X$, hence we have $\Delta_f(x) = (x, x)$ for any $(x, x) \in X \times_{f,Y,f} X$ and so Δ_f is surjective. Thus Δ_f is bijective if and only if f is injective.

Part c)

From part a) we know that Δ_f is always injective, hence we can apply part b) to deduce that we must have Δ_{Δ_f} is always bijective. □

Q7. Coequiliser

Let $f, g : X \to Y$ be maps of sets. Define $\mathrm{coeq}(f,g) = Y/R$ the coequiliser, where R is the smallest equivalence relation containing the subset

$$\{(f(x), g(x)) \subseteq Y \times Y : x \in X\}\,. \tag{1.7.1}$$

We want to show that the induced map $\pi : Y \to \mathrm{coeq}(f,g)$ has the following universal property: if $s : Y \to S$ is a map such that $s \circ f = s \circ g$, then the following diagram commutes:

$$X \underset{g}{\overset{f}{\rightrightarrows}} Y \xrightarrow[\pi]{} \mathrm{coeq}(f,g) \underset{\exists! w}{\dashrightarrow} S \,, \quad s : Y \to S \tag{1.7.2}$$

Let $b \in Y$ and $\pi(b) \in \mathrm{coeq}(f,g)$ (where we note that we can indeed write every element of $\mathrm{coeq}(f,g)$ as $\pi(b)$ since π is naturally surjective). Define the map w as

$$\begin{aligned} w : \mathrm{coeq}(f,g) &\to S \\ \pi(b) &\mapsto s(b)\,. \end{aligned} \tag{1.7.3}$$

We know that $w(\pi(b)) = s(b) \in S$ by definition of s. Further, suppose $\pi(b) = \pi(b')$ for $b, b' \in Y$, then we have three possibilities due to the definition of quotienting by the smallest equivalence relation containing (1.7.1). We either have $b = b'$ or; for some $x \in X$, $f(x) = b$ and $g(x) = b'$ or; $f(x) = b'$ and $g(x) = b$. In the first case:

$$w(\pi(b)) = s(b) = s(b') = w(\pi(b'))\,; \tag{1.7.4}$$

in the second case,

$$w(\pi(b)) = s(b) = s(f(x)) = s(g(x)) = s(b') = w(\pi(b'))\,; \tag{1.7.5}$$

and the third case is clearly identical by symmetry. Therefore w is well defined. Uniqueness follows from the fact that if w' also satisfied all of these same properties then it would have to satisfy $w'(\pi(b)) = s(b) = w(\pi(b))$ and so the universal property holds true. □

2 Monoids

Q6. Classification of submonoids

We will treat this as an exploratory question. We first note that the canonical submonoids of $(\mathbb{N}, +)$ are $a\mathbb{N}$ for some $a \in \mathbb{N}$. However, the complement $\mathbb{N}\backslash a\mathbb{N}$ is clearly not finite, for example $\mathbb{N}\backslash 3\mathbb{N} = \{1, 2, 4, 5, 7, 8, \dots\}$ is not finite.

We can then investigate submonoids S in which a finite subset $S' \subset \mathbb{N}$ is "deleted", i.e. $S = \mathbb{N}\backslash S'$, which gives us the desired finiteness of $\mathbb{N}\backslash S = \mathbb{N}\backslash(\mathbb{N}\backslash S') = S'$. In order to maintain submonoid structure, we always need $0 \in S$, so 0 will never be in S', but the trickier condition to uphold is maintaining closure under addition. We then see that the simplest example one could write down would be $S' = \{1\}$ and indeed $S = \mathbb{N}\backslash\{1\}$ is a submonoid.

We can generalise this and come up with our first form of submonoid: let $n \in \mathbb{N}$, then

$$S_n = \mathbb{N}\backslash\{1, \dots, n\} = \{0, n+1, n+2, \dots\} \quad \text{is a submonoid,} \tag{2.6.1}$$

since it clearly contains the identity and it is closed under addition.

Interestingly though, we can go further than this. If we want to add elements back into S_n by deleting elements from S'_n, this will sometimes work - for example $\mathbb{N}\backslash\{1, 3\}$ is also a submonoid, but $\mathbb{N}\backslash\{1, 3, 4\}$ is not since $2 \in \mathbb{N}\backslash\{1, 3, 4\}$ but $2 + 2 = 4 \notin \mathbb{N}\backslash\{1, 3, 4\}$ so it isn't closed under addition. This gives us a clue: if we choose to delete an element from S'_n, then we also need to delete all of its linear combinations with other deleted elements.

Generalising this last paragraph we can finally classify all submonoids of $(\mathbb{N}, +)$. For any given $n \in \mathbb{N}$, let $S'_n = \{1, \dots, n\}$. For any subset $A'_n \subset S'_n\backslash\{1\}$, let $\text{span}(A'_n)$ be the set of all linear combinations of elements in A'_n. Then the set of all submonoids of $\mathbb{N}$ with finite complement is

$$\left\{ \mathbb{N}\backslash\big(S'_n\backslash\text{span}(A'_n)\big) \;\middle|\; S'_n = \{1, \dots, n\} \text{ for some } n \in \mathbb{N} \text{ and } A'_n \subset S'_n\backslash\{1\} \right\}. \tag{2.6.2}$$

3 Groups

Q7. Kernels and cokernels

Let $f : G \to H$ be a group homomorphism. Define

$$\text{ker}f = \text{eq}(f, 1) \quad \text{and} \quad \text{coker}f = \text{coeq}(f, 1), \tag{3.7.1}$$

where $1 : G \to H$ is the constant group homomorphism, i.e. for every $g \in G$ we have $1(g) = 1_H \in H$.

Part a)

We want to prove that the following are equivalent:

(a) f is injective as a map of sets;

(b) $\text{ker}f = \{1\}$;

(c) if $q_1, q_2 : Q \to G$ is a group homomorphism, then $q_1 = q_2$ if and only if $fq_1 = fq_2$, i.e. f is an epimorphism.

First suppose (a) is true, so for $x_1, x_2 \in G$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. Since f is a group homomorphism this can be re-expressed as $f(x_1 x_2^{-1}) = 1_H$ implies $x_1 x_2^{-1} = 1_G$, which is precisely the statement that $\text{eq}(f, 1) = \text{ker}f = 1_G$, so (a) implies (b).

Now suppose $\ker f = \{1\}$. The first direction of (c) is clearly trivial since f is a well defined function, so suppose $fq_1 = fq_2$. Since f is a homomorphism, this is equivalent to $f(q_1(x)q_2(x)^{-1}) = 1_H$ for some $x \in Q$, but since $\ker f = \{1\}$, we clearly have that $q_1(x)q_2(x)^{-1} = 1_G$, so $q_1 = q_2$ and so (b) implies (c).

Finally, suppose (c) holds - note that this statement is really saying that for any arbitrary Q this if and only if statement holds. So, we can set $Q = \mathbb{Z}$ (where id $= 0$, not 1) and define $q_1(1) = x_1 \in G$ and $q_2(1) = x_2 \in G$. Suppose $x_1, x_2 \in G$ is such that $f(x_1) = f(x_2)$, so $f(q_1(1)) = f(q_2(1))$ and by the assumption this yields $q_1(1) = q_2(1)$ and so $x_1 = x_2$, hence f is injective. □

Part b)

To prove the "dual" version of this statement, we work with the cokernel instead of the kernel and replace injectivity with surjectivity. We also now suppose that H is Abelian (and non-trivial). Also, since we are now working with Abelian groups, it is more convenient to let the identity element be 0. Further, condition (c) becomes: if $q_1, q_2 : H \to Q$ are group homomorphisms, then $q_1 = q_2$ if and only if $q_1 f = q_2 f$. Note that using Sets Q7 and also a definition from lectures, we can write (where the Abelian nature of H allows us to take a quotient in good faith)

$$\text{coker}(f) = \text{coeq}(f, 0) = H/\text{im} f\,. \tag{3.7.2}$$

Suppose f is surjective, so $\text{im} f = H$ and so $H/\text{im} f = \{0\}$, so (a) implies (b). The opposite direction is an identical argument.

To show (a) implies (c), suppose f is surjective again and suppose we have $q_1(f(g)) = q_2(f(g))$ for some $g \in G$, then since f is surjective we are guaranteed to have a $b \in H$ such that $f(g) = b$, so $q_1(b) = q_2(b)$ so $q_1 = q_2$.

Now suppose (c) is true and let $Q = H/\text{im}\, f$. By being clever, we can define $q_1 : H \to H/\text{im}\, f$ as $q_1(h) = 0$ for all $h \in H$ but more importantly, we can define $q_2 : H \to H/\text{im}\, f$ as, being a simplified version of the canonical quotient map where $0 \neq a \in H/\text{im}\, f$,

$$q_2(h) = \begin{cases} 0 & \text{if } h \in \text{im}\, f \\ a & \text{otherwise} \end{cases}\,. \tag{3.7.3}$$

Then using this construction, we see that for any $g \in G$ we have $(q_1 \circ f)(g) = 0$ and $(q_2 \circ f)(g) = 0$ by the above construction. Therefore we must have $q_1 = q_2$ by assumption, which necessarily says that $\text{im}\, f = H$ by (3.7.3), hence showing that f is surjective so (c) implies (a) and we are done. □

With reference to [5].

4 Abelian Groups

Q2. Splitting lemma

Consider a short exact sequence of Abelian groups

$$0 \longrightarrow N_1 \xrightarrow{i} N_2 \xrightarrow{p} N_3 \longrightarrow 0 \,. \tag{4.2.1}$$

We will prove that the following conditions are equivalent:

(a) there exists a homomorphism $r : N_2 \to N_1$ such that $r \circ i = \mathrm{id}$;

(b) there exists a homomorphism $s : N_3 \to N_2$ such that $p \circ s = \mathrm{id}$;

(c) there is an isomorphism $N_1 \oplus N_3 \to N_2$, where the composition $N_1 \to N_1 \oplus N_3 \to N_2$ coincides with i and the composition $N_2 \to N_1 \oplus N_3 \to N_3$ coincides with p.

We first show that (a) implies (c), so assume that (a) is true. Let $b \in N_2$, then in writing

$$b = (b - (i \circ r)(b)) + (i \circ r)(b) \,, \tag{4.2.2}$$

we can show that $b \in \ker(r) + \mathrm{im}(i)$. Clearly $i(r(b)) \in \mathrm{im}(i)$, but further we have (noting that r is a homomorphism)

$$r(b - (i \circ r)(b)) = r(b) - (r \circ i \circ r)(b) = r(b) - (\mathrm{id} \circ r)(b) = 0 \,, \tag{4.2.3}$$

and so $b - i(r(b)) \in \ker(r)$.

We next show that $\ker(r) \cap \mathrm{im}(i) = \{0\}$. Let $b \in \mathrm{im}(i)$, so for some $a \in N_1$ we have $i(a) = b$, and suppose that $b \in \ker(r)$ so $r(b) = 0$. But then $0 = r(b) = (r \circ i)(a) = a$, so $a = 0$ and so $0 = i(0) = b$ since i is a homomorphism, thus proving the intersection is $\{0\}$. Hence, we see that

$$N_2 \cong \ker(r) \oplus \mathrm{im}(i) \tag{4.2.4}$$

and so for all $b \in N_2$ we can write $b = i(a) + k$ for some $a \in N_1$ and $k \in \ker(r)$. The next step is to show that $\mathrm{im}(i) \oplus \ker(r) \cong N_1 \oplus N_3$.

Since this is a short exact sequence, we know that i is injective and p is surjective, and also that $\mathrm{im}(i) = \ker(p)$. Hence, for any $c \in N_3$ we have some $b = i(a) + k$ such that

$$c = p(b) = p(i(a) + k) = p(i(a)) + p(k) = p(k) \,, \tag{4.2.5}$$

so for any $c \in N_3$ we can find a $k \in \ker(r)$ such that $c = p(k)$, so p is a surjection between $\ker(r)$ and N_3. For injectivity, suppose $p(k) = 0$ for $k \in \ker(r)$ (it is a group homomorphism after all), then by exactness we must have $k \in \mathrm{im}(i)$, but since the intersection of these sets is $\{0\}$ we see that $k = 0$ and so p must be injective. Hence $\ker(r) \cong N_3$.

Since i is injective by exactness, we only need to show that i is surjective as a map into N_2, but this is immediate from (4.2.4) and so i induces an isomorphism of $\mathrm{im}(i) \cong N_1$. Therefore, putting all of this together, we finally see that

$$N_2 \cong \mathrm{im}(i) \oplus \ker(r) \cong N_1 \oplus N_3 \,. \tag{4.2.6}$$

The proof of (b) implies (c) is remarkably similar. Performing identical calculations (a good exercise for the active reader), we can determine that $N_2 \cong \ker(p) + \mathrm{im}(s)$. Arguments of exactness then gives us that $N_1 \cong \ker(p)$ and $N_3 \cong \mathrm{im}(s)$, hence showing the desired property once again.

The good news is that we have done the hard yards now. To show that (c) implies (a), we define

$$\begin{aligned} r = \pi_1 : N_1 \oplus N_3 &\to N_1 & \qquad s = \iota : N_3 &\hookrightarrow N_1 \oplus N_3 \\ \pi_1(n_1 + n_3) &= n_1 & \iota(n_3) &= 0 + n_3 \,. \end{aligned} \tag{4.2.7}$$

Because of our isomorphism $N_2 \cong N_1 \oplus N_3$ we have our necessary homomorphisms: let $a \in N_1$ and $c \in N_3$, then

$$\pi_1(i(a)) = a \,, \quad \text{and} \quad p(\iota(c)) = c \,, \tag{4.2.8}$$

where the former is due to injection of i and the latter is due to the surjection of p and so we are done! $\square$

With reference to [7] and [8].

5 Rings

Q12. Nilradical

Let A be a commutative ring and $I \subseteq A$ an ideal. Define the nilradical of I as

$$\mathcal{N}(I) = \sqrt{I} = \{a \in A : a^n \in I \text{ for some } n > 0\} . \tag{5.12.1}$$

To show the nilradical is an ideal, first suppose $x \in \sqrt{I}$ and $r \in A$. Then we have $(rx)^n = r^n x^n$ since A is commutative, and since $x^n \in I$ and $r^n \in A$ we must have $r^n x^n \in I$ by the definition of an ideal, hence $rx \in \sqrt{I}$.

To show that $\sqrt{I}$ is a subgroup, we first note that $0 \in \sqrt{I}$ since $0 \in I$ for any ideal I, and if $x \in \sqrt{I}$ with $x^n \in I$ then we clearly have $-x \in I$ since $(-x)^n = (-1)^n x^n \in I$ since I is itself an ideal. The trickier point is closure: suppose that $x, y \in \sqrt{I}$ such that $x^n \in I$ and $y^m \in I$, we want to show that $x + y \in \sqrt{I}$, i.e. there is some $p \in \mathbb{N}$ such that $(x+y)^p \in \sqrt{I}$. Since we already have n and m given to us, we can exploit this and calculate:

$$\begin{aligned}(x+y)^{n+m} = \sum_{k=0}^{n+m} x^k y^{n+m-k} &= \sum_{k=0}^{n} x^k y^{n+m-k} + \sum_{k=n+1}^{n+m} x^k y^{n+m-k} \\ &= y^m \sum_{k=0}^{n} x^k y^{n-k} + x^n \sum_{k=1}^{m} x^k y^{m-k} .\end{aligned} \tag{5.12.2}$$

We then see that both summation terms after factorisation are in A, whereas $x^n, y^m \in I$, hence both terms in (5.12.2) are themselves in I which is closed, hence $(x+y)^{n+m} \in I$, and so $x + y \in \sqrt{I}$. Therefore we conclude that the nilradical of I is itself an ideal. □

With reference to [10].

Q13. Height of a prime ideal

Let A be a ring. We define the *height* of a prime ideal $\mathfrak{p} \subseteq A$ as the largest number h such that there is a chain of prime ideals that are strict subsets of $\mathfrak{p}$, that is,

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_h = \mathfrak{p} . \tag{5.13.1}$$

If we have an inclusion of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}$ where $\mathfrak{p}_0$ contains no other prime ideals besides itself, then $\mathfrak{p}$ has height 1.

Suppose A is a UFD and $\mathfrak{p}$ is a height 1 prime ideal, we will show that $\mathfrak{p}$ is principal. Since we must always have $(0) \subseteq \mathfrak{p}$ but $\mathfrak{p}$ has height 1, we see that $\mathfrak{p} \neq (0)$ so contains some nonzero element $x \in \mathfrak{p}$. Since A is a UFD, x must be the product of a unit $u \in A$ and nonzero prime elements $p_1, \ldots, p_n \in A$,

$$x = up_1 \ldots p_n . \tag{5.13.2}$$

But since $\mathfrak{p}$ is a prime ideal (so if $x = ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$), we know that we must have at least one p_i in $\mathfrak{p}$. We then see that (p_i) is also prime ideal in A, but by (5.13.2) it must be contained in $\mathfrak{p}$, so $(p_i) \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ has height 1, it is immediate that $(p_i) = \mathfrak{p}$, hence showing that $\mathfrak{p}$ must be principal. □

With reference to [2], [9] and [11].

Q14. Jacobson radical

Let A be a ring. Define the *Jacobson* radical as

$$\mathcal{R}(A) = \bigcup_{\mathfrak{m} \subseteq A\colon \mathfrak{m} \text{ is maximal}} \mathfrak{m} \subseteq A\,. \tag{5.14.1}$$

We will show that $a \in \mathcal{R}(A)$ if and only if $1 - ax \in A^\times$ (i.e. is a unit) for all $x \in A$.

Suppose $a \in \mathcal{R}(A)$. For a contradiction, assume there is some $x \in A$ such that $1 - ax$ is not a unit. Since $1 - ax$ is not a unit, there exists a maximal ideal $\mathfrak{m}$ that contains it (by a Zorn's lemma argument - see [1]), so $1 - ax \in \mathfrak{m}$. Since a is in $\mathcal{R}(A)$, the intersection of all maximal ideals, we know that $a \in \mathfrak{m}$, hence $ay \in \mathfrak{m}$. But since $\mathfrak{m}$ is a subring, hence closed under addition, we have that

$$(1 - ax) + ax = 1 \in \mathfrak{m}\,, \tag{5.14.2}$$

which is clearly a contradiction because then $\mathfrak{m}$ contains a unit, hence $\mathfrak{m} = A$ and so is not maximal. Thus if $a \in \mathcal{R}(A)$ then $1 - ax \in A^\times$ for all $x \in A$.

For the converse, suppose $1 - ax \in A^\times$ for all $x \in A$, but again for contradiction, suppose that $a \notin \mathcal{R}(A)$, then there exists some $\mathfrak{m}$ such that $a \notin \mathfrak{m}$, meaning we can construct $\mathfrak{m}_a = \mathfrak{m} \cup \{a\}$. But since $\mathfrak{m}$ is maximal, we must have

$$A = (\mathfrak{m}_a) = \{m + ay : m \in \mathfrak{m} \text{ and } y \in A\}\,. \tag{5.14.3}$$

This importantly means that $1 \in (\mathfrak{m}_a) = A$, hence there is some $m \in M$ and $y \in A$ such that $1 = m + ay$, so $m = 1 - ay \in \mathfrak{m}$. But since $\mathfrak{m}$ is maximal and hence a proper ideal of A, $1 - ay$ is not a unit in A. Therefore, if $1 - ax \in A^\times$ for all $x \in A$ then $a \in \mathcal{R}(A)$. □

With reference to [1] and [6].

6 Spectra

Q1. Spectrum of $k[[x]]$

Let k be a field and let $k[[x]]$ denote the ring of formal power series with coefficients in k,

$$k[[x]] = \{a_0 + a_1 x + a_2 x^2 + \cdots : a_i \in k\}\,. \tag{6.1.1}$$

We first remind ourselves that since k is a field, hence an integral domain, $k[[x]]$ is also an integral domain. Let $a(x) = \sum_{i=0}^{\infty} a_i x^i$ and $b(x) = \sum_{j=0}^{\infty} b_j x^j$ be non-zero polynomials in $k[[x]]$. Let i' and j' be the smallest indices such that $a_{i'}$ and $b_{j'}$ are non-zero coefficients in $a(x)$ and $b(x)$ respectively. Then

$$a(x)b(x) = a_{i'} b_{j'} x^{i'+j'} + \{\text{higher order terms}\} \neq 0 \tag{6.1.2}$$

since both $a_{i'}, b_{j'} \neq 0$. Hence $k[[x]]$ is also an integral domain.

We then want to show that (0), the principal ideal generated by $0 \in k[[x]]$, is a prime ideal. Suppose $p(x), q(x) \in k[[x]]$ are such that $p(x)q(x) = 0$. Then since $k[[x]]$ is an integral domain from above, we have that either $p(x) = 0$ or $q(x) = 0$, hence (0) is a prime ideal.

We can also show that (x) is a prime ideal. Suppose $p(x), q(x) \in k[[x]]$ are such that $p(x)q(x) = a(x) \in (x)$, so we can write

$$p(x)q(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} p_k q_{n-k} \right) x^n = \sum_{n=1}^{\infty} a_n x^n\,, \tag{6.1.3}$$

specifically noting the sum on the right starts at $n = 1$ since $a(x) \in (x)$. By comparison of terms (which uniquely defines a power series), this implies that the first term $p_0 q_0$ of $p(x)q(x)$ must be 0, hence either $p_0 = 0$ or $q_0 = 0$ since k is a field. In either case, this implies one of $p(x)$ or $q(x)$ is in (x), hence (x) is a prime ideal.

But are there any other prime ideals? We note that $k[[x]]$ is a principal ideal domain, so we only need to investigate other possible principal ideals. There are two obvious choices, and neither are prime ideals. An ideal of the form (x^n) for $n \geq 2$ is not prime, with the trivial counterexample being: suppose $p(x)q(x) = x^n \in (x^n)$, then we could have $p(x) = x$ and $q(x) = x^{n-1}$ in $k[[x]]$, neither of which is in (x^n) hence showing it is not prime - indeed, $(x^n) \subset (x)$.

We could also feasibly have ideals of the form $(x - a)$ for some $a \in k$, but by Rings Q9 we know that if a_0 is a unit in its underlying ring then the formal power series $x - 1$ is a unit. Clearly in our case $a_0 = -a \in k$ is a unit since k is a field, meaning we just have $(x - a) = k[[x]]$, hence it is also not prime. Combining these two facts we see that there are no other prime ideals, thus

$$\text{Spec}\, k[[x]] = \{(0), (x)\}. \tag{6.1.4}$$

□

With reference to [3].

Q3. Direct product to disjoint union

Let A_1, A_2 be rings. Considering the direct product ring $A_1 \times A_2$, we can write down the canonical projections

$$\begin{aligned} \pi_1 : A_1 \times A_2 &\to A_1 & \pi_2 : A_1 \times A_2 &\to A_2 \\ (a_1, a_2) &\mapsto a_1 & (a_1, a_2) &\mapsto a_2 \,. \end{aligned} \tag{6.3.1}$$

Clearly both of these maps are surjective which gives us an indication to analyse an induced map between spectra, which we can define as

$$\begin{gathered} \beta^* : \operatorname{Spec} A_1 \amalg \operatorname{Spec} A_2 \to \operatorname{Spec}(A_1 \times A_2) \\ \beta^*((\mathfrak{p}, i)) = \begin{cases} \pi_1^{-1}(\mathfrak{p}) & \text{if } i = 1 \\ \pi_2^{-1}(\mathfrak{p}) & \text{if } i = 2 \end{cases} . \end{gathered} \tag{6.3.2}$$

That β^* is a bijection largely comes down to determining what the elements of $\operatorname{Spec}(A_1 \times A_2)$ are. We claim that these elements are of the form $\mathfrak{p}_1 \times A_2$ or $A_1 \times \mathfrak{p}_2$ for some prime ideals $\mathfrak{p}_1 \in A_1$ or $\mathfrak{p}_2 \in A_2$. Certainly these elements are indeed prime ideals: suppose $a_1, b_1 \in \mathfrak{p}_1$ and $a_2, b_2 \in A_2$ are such that

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2) \in \mathfrak{p}_1 \times A_2 \,. \tag{6.3.3}$$

Then $a_1 \in \mathfrak{p}_1$ or $b_1 \in \mathfrak{p}_1$, so either $(a_1, a_2) \in \mathfrak{p}_1 \times A_2$ or $(b_1, b_2) \in \mathfrak{p}_1 \times A_2$, hence $\mathfrak{p}_1 \times A_2$ is a prime ideal (and obviously symmetry gives the alternative stated above).

Are there any others? Suppose $P \subset A_1 \times A_2$ is a prime ideal. Let $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Since P is a proper ideal, there is some nonzero element in P - suppose we have $e_1 \notin P$. Then we have $e_1 e_2 = (0, 0) \in P$ since P is a subgroup, but since P is prime, we must have $e_2 \in P$. Since 1 is a unit in A_2, hence generates the whole ring A_2, we see that $0 \times A_2 \subseteq P$ (since $(0, 0) = 0$ must be a subset of any prime ideal). Finally, it is obvious that $\pi_1(P)$ must be a prime ideal of A_1, say $\pi_1(P) = \mathfrak{p}_1 \in A_1$, but also we must have $P = \pi_1(P) \times A_2$. Therefore $P = \mathfrak{p}_1 \times A_2$ or $P = A_1 \times \mathfrak{p}_2$ are the prime ideals of $A_1 \times A_2$.

Suppose $\beta^*((\mathfrak{p}, i)) = \beta^*((\mathfrak{p}', i'))$ for prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ in, say, A_1 (which is clearly symmetric for A_2). Note that in order for this equality to make sense we must have $i = i'$. Then

$$\pi_1^{-1}(\mathfrak{p}) = \pi_1^{-1}(\mathfrak{p}') \,, \quad \text{so } \mathfrak{p} \times A_2 = \mathfrak{p}' \times A_2 \,, \quad \text{so } \mathfrak{p} = \mathfrak{p}' \,, \tag{6.3.4}$$

so β^* is injective. Then let $\mathfrak{p} \in \operatorname{Spec}(A_1 \times A_2)$. Thanks to our painstaking effort above, we know that $\mathfrak{p} = \mathfrak{p}_1 \times A_2$ for some prime ideal $\mathfrak{p}_1 \in A_1$ (and, as always, symmetric for the $i = 2$ case). Then we can just take $\mathfrak{p}_1 \in \operatorname{Spec}(A_1)$ as our element in the domain, hence

$$\beta^*((\mathfrak{p}_1, 1)) = \pi_1^{-1}(\mathfrak{p}_1) = \mathfrak{p}_1 \times A_2 = \mathfrak{p} \,, \tag{6.3.5}$$

and so β^* is also surjective, hence we have a well defined bijection and we are done. □

With reference to [4].

References

[1] *Abstract Algebra - Every non-unit is in some maximal ideal.* URL: https://math.stackexchange.com/questions/938777/every-non-unit-is-in-some-maximal-ideal (visited on 08/20/2020).

[2] *Abstract Algebra - Every prime ideal of height 1 in a UFD is principal.* URL: https://math.stackexchange.com/questions/2548309/every-prime-ideal-of-height-1-in-a-ufd-is-principal (visited on 08/20/2020).

[3] *Abstract Algebra - If R is an integral domain, then $R[[x]]$ is an integral domain.* URL: https://math.stackexchange.com/questions/457447/if-r-is-an-integral-domain-then-rx-is-an-integral-domain (visited on 08/20/2020).

[4] *Abstract Algebra - Prime ideals in a finite direct product of rings.* URL: https://math.stackexchange.com/questions/1216203/prime-ideals-in-a-finite-direct-product-of-rings (visited on 08/20/2020).

[5] *Category Theory - Morphism epimorphism if and only if surjective.* URL: https://math.stackexchange.com/questions/1691666/morphism-epimorphism-if-and-only-if-surjective (visited on 08/20/2020).

[6] *Comm. Algebra - The Jacobson Radical.* URL: https://crypto.stanford.edu/pbc/notes/commalg/jacobson.html (visited on 08/20/2020).

[7] *Exact sequence.* en. Page Version ID: 970013709. July 2020. URL: https://en.wikipedia.org/w/index.php?title=Exact_sequence&oldid=970013709 (visited on 08/20/2020).

[8] *Galois Theory - Homework 11 Solutions.* 2012. URL: http://palmer.wellesley.edu/~ivolic/pdf/Classes/MATH306GaloisTheorySpring12/Solutions/306Homework11Solutions.pdf.

[9] *Height of an ideal - Encyclopedia of Mathematics.* URL: https://encyclopediaofmath.org/wiki/Height_of_an_ideal (visited on 08/20/2020).

[10] *Nilradical is an ideal - Commalg.* URL: https://commalg.subwiki.org/wiki/Nilradical_is_an_ideal (visited on 08/20/2020).

[11] *Unique factorization domain.* en. Page Version ID: 971664567. Aug. 2020. URL: https://en.wikipedia.org/w/index.php?title=Unique_factorization_domain&oldid=971664567 (visited on 08/20/2020).

Acknowledgement

With thanks to Spencer Wong and Caleb Smith for their useful discussions and helpful pointers along the way.