Math250aHw8

Trustin Nguyen

October 24, 2023

Exercise 1: Write out a careful proof of the "contravariant Yoneda embedding theorem":

Theorem 0.1: If F is a contravariant functor from a category C to the category of sets, and A is an object in C, then there is a natural isomorphism

$$((-, A), F) \cong F(A)$$

and its important consequence, the full embedding theorem:

Proof. We want to show:

$$\begin{tikzcd} ((-,A),F) \arrow[rr, bend right, "\delta"'] \arrow[rr, phantom, "\cong"] & & F(A) \arrow[ll, bend right, "\eta"'] \end{tikzcd}$$

where $\delta\eta = id$ and $id = \eta\delta$. We consider δ_A as

$$((A, A), F) \to F(A)$$

and since the functor is contravariant:

$$\begin{tikzcd} F(A) \arrow[r, "F(\varphi)"] & F(A) \\ A \arrow[u] & A \arrow[l, "\varphi"] \arrow[u] \end{tikzcd}$$

commutes. So if $\alpha_A \in ((A, A), F)$, then we send it by δ_A to an object in $F(A)$, which is the evaluation of α_A. We know that identities are sent to identities by isomorphism, so it must be that $\alpha_A \mapsto \alpha_A(1_A)$.

Now for $\eta_B(x)$, consider the diagram:

$$\begin{tikzcd} (A, A) \arrow[r] \arrow[d, "\varphi \circ f"] & F(A) \arrow[d, "F(\varphi \circ f)"] \\ (B, A) \arrow[r] & F(B) \end{tikzcd}$$

If we have $\varphi \in (A, A)$, then for some $f : B \to A$, we have that the morphism from $(A, A) \to (B, A)$ is composition shown above. Now if $x \in F(A)$, then it is sent to $F(B)$ by $F(\varphi \circ f)(x)$. Then there is a natural mapping from $(B, A) \to F(B)$:

$$\begin{tikzcd}
f \arrow[r] \arrow[d, "\varphi\circ f"] & x \arrow[d, "F(\varphi\circ f)"] \\
\varphi \circ f \arrow[r] & F(\varphi \circ f)(x)
\end{tikzcd}$$

Then if $\psi \in (B, A)$, we have the mapping from $\eta : x \mapsto (\psi \mapsto F(\psi)(x))$.

($\delta(\eta(x)) = x$) We have:

$$\begin{aligned}
\delta(\eta(x)) &= (\eta(x))_A(1_A) \\
&= F(\varphi)(x)(1_A \\
&= F(1_A)(x) \\
&= (1_A)(x) \\
&= x
\end{aligned}$$

which shows that $\delta\eta$ is the identity on $F(A)$.

($\eta(\delta(\alpha))_B = \alpha_B$) We have that

$$\begin{aligned}
\eta(\delta(\alpha))_B(\varphi) &= \eta(\alpha_A(1_A))_B(\varphi) \\
&= F(\varphi)(\alpha_A(1_A))
\end{aligned}$$

Now recall that we have the natural transformation:

$$\begin{tikzcd}
(A, A) \arrow[r, "\alpha_A"] \arrow[d, "\varphi"] & F(A) \arrow[d, "F(\varphi)"] \\
(B, A) \arrow[r, "\alpha_B"] & F(B)
\end{tikzcd}$$

So we have

$$F(\varphi)(\alpha_A(1_A)) = F(\varphi)(\alpha_A)(1_A) = \alpha_B(1_A)(\varphi) = \alpha_B(\varphi)$$

Therefore, we have that

$$\eta(\delta(\alpha))_B(\varphi) = \alpha_B(\varphi)$$

where φ was just a placeholder morphism. So $\eta(\delta(\alpha))_B = \alpha_B$, which shows that $\eta\delta$ is the identity. □

Corollary 0.2: The functor from C to the category of functors $C \to$ Sets taking an object A to the functor $(-, A)$ is one-to-one and onto on morphisms and takes non-isomorphic objects to non-isomorphic functors.

Proof. We will use the fact that for any A object of C, since $(-, A)$ is a contravariant functor, we have:

$$((-, A), \mathrm{id}) \cong A$$

Now we just map:

$$((-, A), \mathrm{id}) \mapsto (-, A)$$

This is one-to-one because if $F(((-, A), \mathrm{id})) = F(((-, B), \mathrm{id}))$, then $(-, A) \cong (-, B)$, which means that the identity morphism in (A, A) must map to the identity on (A, B) which is only possible if $A \cong B$ or $((-, A), \mathrm{id}) \cong ((-, B), \mathrm{id})$. The map is onto because if $(-, D) \in (C \to \text{Set})$, then we just have that $((-, D), \mathrm{id}) \cong D$ maps to it. We finally have that non-isomorphic objects are sent to non-isomorphic functors just by the contrapositive statement of the injectivity proved before. So we are done. □

Exercise 2: Read Lang, pp. 173-186 and do problems p.213, #1 – 3.

Exercise 3: Let k be a field and $f(X) \in k[X]$ a non-zero polynomial. Show that the following conditions are equivalent:

(a) The ideal $(f(X))$ is prime.

(b) The ideal $(f(X))$ is maximal.

(c) $f(X)$ is irreducible.

Proof. We will show that $a \to c$. This is because if $f(X) = g(X)h(X)$, then since $(f(X))$ is prime, we have that $g(X) \in (f(X))$ or $h(X) \in (f(X))$. So $g(X) \mid f(X)$ wlog. But since the ideal is generated by $f(X)$, we also have $f(X) \mid g(X)$. So:

$$f(X)u = g(X)$$

and

$$g(X)p = f(X)$$

so

$$g(X)up = g(X)$$

Therefore, p is a unit which means that $f(X)$ is irreducible.

We will now show that $c \to b$. Since k is a field, we have $k[X]$ is a Euclidean Domain and therefore a PID. So we have $(f(X), g(X)) = (h(X))$ for $g(X)$ not a multiple of $f(X)$. This means that $h(X) \mid f(X)$, $h(X) \mid g(X)$. Then $h(X)$ is a unit or differs from $f(X)$ by a unit. If $h(X)$ is a unit, we are done. If not, we have:

$$af(X) = h(X)$$

but

$$g(X) = bh(X)$$

so

$$g(X) = abf(X)$$

which shows that $f(X) \mid g(X)$ which contradicts our assumption. So if $(f(X))$ is contained in any ideal, that ideal must be the whole ring or itself.

Now for a proof of $b \to a$. Suppose $g(X)h(X) \in (f(X))$, $(f(X))$ a proper ideal of $k[X]$. Since $k[X]$ is a Euclidean Domain, we see wlog that $g(X)$ has the same degree as $f(X)$, otherwise, we perform the division algorithm on the degree of f and see that $(f(X)) = k[X]$. But:

$$\deg g + \deg h = \deg f$$

So

$$\deg h = 0$$

which means that h is a unit. So $g(X) \in f(X)$. □

Exercise 4:

(a) State and prove the analogue of Theorem 5.2 for the rational numbers.

Proof. We want to show that for any $\alpha \in \operatorname{Frac}\mathbb{Z}$, there is a unique decomposition such that if P is the set of primes in $\mathbb{Z}$, and $j(p)$ is 0 for almost all p,

$$\alpha = \sum_{p \in P} \frac{\alpha_p}{p^{j(p)}} + \beta$$

where $\alpha_p, \beta \in \mathbb{Z}$, $\alpha_p = 0$ if $j(p) = 0$, α_p is relatively prime to $p^{j(p)}$ if $j(p) \geqslant 1$, and $|\alpha_p| < |p^{j(p)}|$ if $j(p) > 0$. Furthermore, this decomposition is unique.

First, consider the primes $p_1, \dots, p_m$ where $j(p_i) \neq 0$. We will show that there are $a_1, \dots, a_m$ non-zero such that for any number of primes $p_1, \dots, p_m$ chosen, $m \geqslant 2$:

$$a_1 p_1^{j(p_1)} + a_2 p_2^{j(p_2)} + \cdots a_m p_m^{j(p_m)} = 1$$

Base Case: For $m = 2$, since $\mathbb{Z}$ is a PID, p_1, p_2 relatively prime, we have:

$$a_1 p_1^{j(p_1)} + a_2 p_2^{j(p_2)} = 1$$

Indeed neither a_1, a_2 are zero, because primes are not units by definition, so they cannot generate the ring.

Inductive Step: Suppose this is true for $p_1, \dots, p_m$. Then we have:

$$p' = a_1 p_1^{j(p_1)} + a_2 p_2^{j(p_2)} + \cdots + a_m p_m^{j(p_m)} = 1$$

Then p_{m+1} does not divide p', otherwise, (p_{m+1}) generates the entire ring. So p_{m+1}, p' are relatively prime. Now we have:

$$(1 - p_{m+1})p' + p_{m+1} = 1$$

so we have non-zero coefficients $a_1, \dots, a_{m+1}$ such that the linear combination equals 1. Now divide through

$$a_1 p_1^{j(p_1)} + a_2 p_2^{j(p_2)} + \cdots a_m p_m^{j(p_m)} = 1$$

by $p_1^{j(p_1)} p_2^{j(p_2)} \cdots p_m^{j(p_m)}$ to get:

$$\frac{1}{p_1^{j(p_1)} p_2^{j(p_2)} \cdots p_m^{j(p_m)}} = \sum_{i=1}^{m} \frac{a_i}{\prod_{k \neq i} p_k^{j(p_k)}}$$

We will use this to show that any element of $\operatorname{Frac} \mathbb{Z}$ with a denominator on m primes can be decomposed into a sum of elements of $\operatorname{Frac} \mathbb{Z}$ with each summand having one prime. For the case of where a summand has one prime in the denominator, that is the very most it can be decomposed. If there are two primes, we have:

$$a_1 p_1^{j(p_1)} + a_2 p_2^{j(p_2)} = 1$$

which means:

$$c a_1 \frac{p_1}{p_2^{j(p_2)}} + c a_2 \frac{p_2}{p_1^{j(p_1)}} = \frac{c}{p_1^{j(p_1)} p_2^{j(p_2)}}$$

So for any $c / p_1^{j(p_1)} p_2^{j(p_2)}$, it can be decomposed into denominators with only one prime factor. Now suppose we had $c / \prod_{i=1}^{m} p_m^{j(p_m)}$, where there are m prime factors in the denominator. By the fact that we have the decomposition:

$$\alpha = \frac{c}{p_1^{j(p_1)} p_2^{j(p_2)} \cdots p_m^{j(p_m)}} = c \sum_{i=1}^{m} \frac{a_i}{\prod_{k \neq i} p_k^{j(p_k)}}$$

the summands on the RHS have fewer primes in the denominator, and by induction, we can decompose those into sums of fractions with one prime in the denominator.

Now since α in the above equation is decomposed as such, if we have other summands with different primes p'_i in the denominator as already established, then if:

$$\alpha = c \sum_{i=1}^{m} \frac{a_i}{\prod_{k \neq i} p_k^{j(p_k)}} + \sum_{i \geqslant 0} \frac{c_i}{{p'_i}^{j(p'_i)}}$$

Then we know each of the c_i's are 0, if we also prove the unique decomposition. If any of the α_p in the numerator is greater than the denominator, we have the Euclidean algorithm such that the quotient gets added to β and the remainder replaces the numerator. α_p is relatively prime to $p^{j(p)}$ otherwise it belongs as a summand of β. Now we just need to show the decomposition is unique. Suppose that:

$$\sum_{p\in P} \frac{\alpha_p}{p^{j(p)}} + \beta = \sum_{q\in P} \frac{\alpha'_q}{q^{j(q)}} + \beta'$$

this means that:

$$\sum_{p\in P} \frac{\alpha_p}{p^{j(p)}} + \beta - \sum_{p\in P} \frac{\alpha'_p}{p^{i(p)}} - \beta' = 0$$

We have $\beta = \beta'$ because all the other summands are in $\operatorname{Frac}\mathbb{Z}$ and not in $\mathbb{Z}$. Now if for a fixed prime q, $j(1) = i(1)$, we have that

$$\frac{\alpha_q}{q^{j(q)}} - \frac{\alpha'_q}{q^{i(q)}} = 0$$

so indeed $\alpha_q = \alpha'_q$. Now suppose $j(q) < i(q)$ for some prime q. Then we clear denominators by multiplying by $dq^{i(q)}$ where d is the lcm of the prime powers not equal to q. So we are left with:

$$d(\alpha_q - \alpha'_q{}^{q^{i(q)-j(q)}}) = q^{i(q)}\eta$$

for some $\eta \in \mathbb{Z}$. But q does not divide either product parts on the LHS, which is a contradiction. So $i(q) = j(q)$ and the decomposition is unique. □

(b) State and prove the analogue of Theorem 5.3 for positive integers.

Proof. Let $p, q \in \mathbb{Z}_{\geqslant 0}$. Then there is a unique a_i such that:

$$p = a_0 + a_1 q + a_2 q^2 + \cdots + a_n q^n$$

such that $a_i < q$ where $q > 1$. If $q > p$, then we take $a_0 = p < q$. If $q = p$, we take $a_0 = 0$, $a_1 = 1$.

Otherwise, for $q < p$, we require the division algorithm, which will be proved at the end of this proof. Take the largest power of q such that $q^n < p$. Then perform the division algorithm:

$$p = a_n q^n + r_n$$

We know that $a_n < q$ because q^n is the largest power less than p. Furthermore, ,$r_n < q^n$. Now take the largest power of q such that $q^m < r_n$. We inductively repeat this process until $r_i < q$. So we have:

$$p = a_0 + a_1 q + a_2 q^2 + \cdots + a_n q^n$$

as desired. Suppose that we also had:

$$p = b_0 + b_1 q + b_2 q^2 + \cdots + b_n q^n$$

Then

$$0 = (a_0 - b_0) + (a_1 - b_1)q + \cdots + (a_n - b_n)q^n$$

So q divides $a_0 - b_0$ which we know are both less than q. So $a_0 - b_0 = 0$ and $a_0 = b_0$. But now we have:

$$0 = (a_1 - b_1)q + (a_2 - b_2)q^2 + \cdots + (a_n - b_n)q^n$$

which tells us that $q \mid (a_1 - b_1)$. So we can repeat this process inductively to show $a_i = b_i$.

(Division Algorithm) (Existence) Since $q > 1$, we know that for $d \geqslant p + 1$,

$$dq > p$$

So we have a finite number of possibilities for d: $1, \dots, p$. Choose the least of them such that $(d+1)q > p$. Then

$$dq < p \implies p - dq = r > o$$

But

$$(d+1)q > p \implies dq + q > p \implies q > p - dq = r$$

So we have found a d such that:

$$p = dq + r$$

and $r < q$.

(Uniqueness) Suppose that $p = d_1 q + r_1 = d_2 q + r_2$. Then

$$0 = q(d_1 - d_2) + r_1 - r_2$$

Then q divides $r_1 - r_2$ which means that $r_1 - r_2 = 0$ as $d > r_1, r_2 \geqslant 0$. So then:

$$0 = q(d_1 - d_2)$$

If $q = 0$, we have $p = r_1 = r_2$, so we are done. Otherwise, since there are no zero divisors in $\mathbb{Z}_{\geqslant 0}$, $d_1 - d_2 = 0$ which means $d_1 = d_2$. □

Exercise 5: Let f be a polynomial in one variable over a field k. Let X, Y be two variables. Show that in $k[X, Y]$ we have a "Taylor series" expansion

$$f(X+Y) = f(X) + \sum_{i=1}^{n} \varphi_i(X) Y^i,$$

where $\varphi_i(X)$ is a polynomial in X with coefficients in k. If k has characteristic 0, show that

$$\varphi_i(X) = \frac{D^i f(X)}{i!}.$$

Proof. Notice that we have for f as a polynomial in one variable:

$$f(z) = k_0 + k_1 z + k_2 z^2 + \cdots$$

where finitely many k_i are non-zero. Then

$$f(X+Y) = k_0 + k_1(X+Y) + k_2(X+Y)^2 + \cdots$$

By the binomial theorem, we have:

$$\begin{aligned}
f(X+Y) &= \sum_{i=0}^{m} k_i \sum_{j=0}^{i} \binom{i}{j} X^{i-j} Y^j \\
&= \sum_{i=1}^{m} k_i \sum_{j=1}^{i} \binom{i}{j} X^{i-j} Y^j + \sum_{i=0}^{m} k_i \binom{i}{0} X^i \\
&= \sum_{i=1}^{m} k_i \sum_{j=1}^{i} \binom{i}{j} X^{i-j} Y^j + f(X) \\
&= \sum_{i=1}^{m} \sum_{j=1}^{i} k_i \binom{i}{j} X^{i-j} Y^j + f(X)
\end{aligned}$$

Now for each $i = 1, \ldots, m$, we look at the instance of when $j = 1$. This gives us

$$k_i \binom{i}{1} X^{i-1} Y^1$$

So then the collection of terms with Y^1 is:

$$\sum_{i=1}^{m} k_i \binom{i}{1} X^{i-1} Y^1 = \left(\sum_{i=1}^{m} k_i \binom{i}{1} X^{i-1} \right) (Y^1)$$

and therefore,

$$\varphi_1 = \sum_{i=1}^{m} k_i \binom{i}{1} X^{i-1}$$

and in general:

$$\varphi_j = \sum_{i \geqslant j}^{m} k_i \binom{i}{j} X^{i-j}$$

which is a polynomial on X, and indeed,

$$\begin{aligned} f(X+Y) &= \sum_{i=1}^{m} \sum_{j=1}^{i} k_i \binom{i}{j} X^{i-j} Y^j + f(X) \\ &= \sum_{j=1}^{i} \sum_{i \geqslant j}^{m} k_i \binom{i}{j} X^{i-j} Y^j + f(X) \\ &= f(X) + \sum_{j=1}^{i} \varphi_j(X) Y^j \end{aligned}$$

Now for the second part, we recall

$$\varphi_j = \sum_{i \geqslant j}^{m} k_i \binom{i}{j} X^{i-j}$$

So we can factor out a j! from the bottom:

$$\begin{aligned} \varphi_j &= \frac{1}{j!} \sum_{i \geqslant j}^{m} k_i \frac{i!}{(i-j)!} X^{i-j} \\ &= \frac{1}{j!} \sum_{i \geqslant j}^{m} k_i (i)(i-1) \cdots (i-j+1) X^{i-j} \\ &= \frac{1}{j!} \sum_{i \geqslant j}^{m} k_i D^j X^i \\ &= \frac{1}{j!} D^j \sum_{i \geqslant j}^{m} k_i X^i \\ &= \frac{1}{j!} D^j f(X) \end{aligned}$$

which concludes the proof. □