SOLUTIONS TO FURTHER EXERCISES FOR

MATHEMATICS 144 — Part 4

Fall 2017

V. Number systems and set theory

V.2 : Finite induction and recursion

113. One basic property of the degree is that $\deg(f+g) = \deg(f) + \deg(g)$. The idea of the proof is to proceed by induction on the degree. If $\deg(f) = 1$ then it is not possible to write f as a product of two polynomials whose degrees are both positive (we cannot find two positive integers whose sum equals 1), so the result is true in that case. Assume now that the result is true whenever $\deg(f) < n$, where $n \geq 2$, and let p be a polynomial with degree n. If p is irreducible, then we are done. If not, then $p = q_1 q_2$ where $\deg(q_1)$ and $\deg(q_2)$ are both positive; clearly we must have $\deg(q_i) < n$ for $i = 1, 2$. Therefore by the Strong Principle of Finite Induction we know that q_1 and q_2 are products of irreducible polynomials. Therefore $p = q_1 q_2$ is also a product of irreducible polynomials.■

113. (*i*) If $c = a + b\sqrt{5}$ let $c^* = a - b\sqrt{5}$. Then $|N(a + b\sqrt{5})| = |cc^*|$. Direct calculation yields the identity

$$(c_1 c_2)^* \quad = \quad c_1^* \cdot c_2^*$$

(the same sort of derivation which proves the corresponding result for complex numbers) and therefore we have

$$|N(xy)| \;=\; |(xy)(xy)^*| \;=\; |xyx^*y^*| \;=\; |xx^*yy^*| \;=\; |xx^*| \cdot |yy^*| \;=\; |N(x)| \cdot |N(xy)|$$

which is what we wanted to prove.■

(*ii*) If $|N(x)| = 1$ then we have $x^* = x^{-1}$ by the given fact that $xx^* = 1$. Conversely, if $x^{-1} \in \mathbb{Z}[\sqrt{5}]$ then we have $1 = N(1) = |N(x)||N(x^{-1})|$. Since a product of two positive integers is 1 if and only if both factors are equal to 1, this implies $|N(x)| = 1$.■

(*iii*) As in Exercise 113, use the Strong Principle of Finite Induction, but start with $|N(x)| = 2$. In that case, if $x = yz$ then $2 = |N(x)| = |N(y)| \cdot |N(z)|$ implies that either $|N(x)| = 1$ or $|N(y)| = 1$. Suppose now that the result is known for all $k < n$, where $n \geq 3$. Suppose that $|N(x)| = n$. Then either x is irreducible or else $x = yz$ with $|N(x)| = |N(y)| \cdot |N(z)|$ and $1 < |N(y)|, |N(z)| < n$. In the first case the conclusion is automatically true, and in the seccond the conclusion follows because y and z are both products of irreducible elements by the Strong Principle of Finite Induction.■

VI. Infinite constructions in set theory

VI.2 : Infinite Cartesian products

101. By definition an element of the Cartesian product is a function $u : A \to \cup_\alpha X_\alpha$ such that $u_\alpha = X_\alpha$ for all α. If x lies in the product, then $x_\beta \in X_\beta$ is impossible because X_β is empty. Therefore the product must also be empty.■

VI.3 : Transfinite cardinal numbers

101. The defining condition uses nothing about $\mathcal{U}$ or $\mathcal{W}$; the existence of a 1–1 onto mapping does not change if we view the sets as members of one family or the other.■

102. We are given $|A| = |C|$, so we need only show $|B| = |C|$. But $|B| \leq |C| = |A|$ and $|A| \leq |B|$, so $|C| = |A| = |B|$ follows from the equivalence relation properties of cardinality and the Schröder-Bernstein Theorem.■

103. If $|A| \leq |B|$, then there is a 1–1 map $f : A \to B$. If $A' = f[A]$, then f defines a 1–1 correspondence between A and A', and consequently we have $|A| = |A'|$ where $A' \subset B$.■

VI.4 : Countable and uncountable sets

101. There should be a hypothesis that $A \neq \emptyset$ in this exercise.

Each of the sets $A^n \times \{n\}$ is finite, and hence we have 1–1 maps from A into $\mathbb{N} \times \{n\}$ for each n. We can merge them into a 1–1 map from **String** (A) into $\mathbb{N} \times \mathbb{N}$, and hence the set of strings has cardinality $\leq \aleph_0$. On the other hand, we have a 1–1 mapping from $\mathbb{N}$ into the set of strings by taking $a \in A$ and sending n to $(a, ..., a; n+1)$, where $(a, ..., a) \in A^{n+1}$ has a in each coordinate. We can now apply the Schröder-Bernstein Theorem to say that the cardinality of the set of strings is $\aleph_0$.

VII. The Axiom of Choice and related topics

VII.1 : Nonconstructive existence statements

NOTE. Throughout this section we assume that the Axiom of Choice is valid.

101. Let β be the cardinality of the set of irrational numbers, so that $2^{\aleph_0} = \beta + \aleph_0$. Now β must be infinite (otherwise the right hand side wouold be $\aleph_0$), so we know that $\beta = \beta + \aleph_0$. Since the right hand side equals $2^{\aleph_0}$, the same must be true for the left hand side.■

102. For each subset W pick a basis $b_1, \cdots, b_m$ of W, and define a mapping from $G_m(\mathbb{R}^n)$ to $(\mathbb{R}^n)^m = \mathbb{R}^{mn}$ sending W to $(b_1, \cdots, b_m)$. This shows that $|G_m(\mathbb{R}^n)| \leq |\mathbb{R}^{mn}| = |\mathbb{R}|$. To prove the reverse inequality, let $\mathbf{e}_1, ...(etc.)$ denote the standard unit vector basis of $\mathbb{R}^n$, and consider the map sending $t \in \mathbb{R}$ to the span of $\mathbf{e}_1 + t\mathbf{e}_2, \mathbf{e}_3, \cdots, \mathbf{e}_{m+1}$ in $\mathbb{R}^n$, with the convention that the list of unit vectors is empty if $m = 1$ (note that all the vectors lie in $\mathbb{R}^n$ because $m < n$ and hence $m+1 \leq n$).

The $m \times n$ matrices with these rows are in row reduced echelon forms, and no two of them are equal, so the subspaces spanned by different sets are distinct. This means that $|\mathbb{R}| \leq |G_m(\mathbb{R}^n)|$, so the result follows (once more) from the Schröder-Bernstein Theorem.∎

103. The polynomial in the statement should be assumed to be nonconstant.

Since and $(n-1)$-dimensional vector subspace of $\mathbb{R}^n$ is defined by a homogeneous linear equation, the preceding exercise shows that $|\mathbb{R}| \leq |\mathbf{H}|$.

To prove the reverse inequality, we start by verifying that the cardinality of the nonconstant polynomials in $\mathbb{R}[t]$ is equal to $|\mathbb{R}|$. There is a 1–1 mapping of $\mathbb{R}$ into $\mathbb{R}[t]$ given by sending $a \in \mathbb{R}$ to $t + a$. In each degree d there are $|(\mathbb{R} - \{0\}) \times \mathbb{R}^d|$ polynomials of degree d; the exceptional first factor is present because the term in the top degree is nonzero. Hence the number of polynomials of degree $d > 0$ is $|\mathbb{R}|$, so the number of polynomials of an arbitary positive degree is $\aleph_0 \times |\mathbb{R}| = |\mathbb{R}|$. Now the set of all nonconstant polynomials maps onto $\mathbf{H}$ by the map sending the polynomial f to the set $V(f) \subset \mathbb{R}^n$ of all points where $f = 0$. This map from polynomials to hypersurfaces is onto (but not 1–1!), and therefore $|\mathbf{H}|$ is less than or equal to the cardinality of the set of nonconstant polynomials. Since the latter cardinality is equal to $|\mathbb{R}|$, it follows that $|\mathbf{H}| \leq |\mathbb{R}|$. Once again we can apply the Schröder-Bernstein Theorem to conclude that $|\mathbb{R}| \leq |\mathbf{H}|$.∎