On Linear Independence of Characters

France Dacar, Jožef Stefan Institute

January 24, 2008

Let A be any set equipped with a binary operation, which is written multiplicatively. Let K be a field. We shall call a **character of A in K** any mapping $A \to K$ which preserves multiplication and is not identically zero; $\mathrm{Char}(A, K)$ will denote the set of all characters of A in K. The set of all maps $A \to K$ can be made into the vector space K^A over K, with the vector space operations defined pointwise.

Theorem 1 (Dedekind)**.** *Let A be a set with a (multiplicative) binary operation, and let K be a field. Then $\mathrm{Char}(A, K)$ is a linearly independent subset of the vector space K^A over K.*

Proof. Let us have distinct characters $\chi_1, \ldots, \chi_n \in \mathrm{Char}(A, K)$, $n \geqslant 1$, and suppose that

$$a_1\chi_1 + \cdots + a_n\chi_n \;=\; 0 \tag{1}$$

with $a_1, \ldots, a_n \in K$; we will show, by induction on n, that all coefficients $a_1, \ldots, a_n$ must be 0. For $n = 1$ choose $x \in A$ at which $\chi_1(x) \neq 0$ to see that $a_1\chi_1(x) = 0$ implies $a_1 = 0$. Now suppose that $n > 1$. Since $\chi_1 \neq \chi_n$, there exists $y \in A$ such that $\chi_1(y) \neq \chi_n(y)$. Evaluate (1) at x and yx, for an arbitrary $x \in A$:

$$\begin{aligned} a_1\chi_1(x) + \cdots + a_n\chi_n(x) \;&=\; 0\,, \\ a_1\chi_1(y)\chi_1(x) + \cdots + a_n\chi_n(y)\chi_n(x) \;&=\; 0\,. \end{aligned}$$

Subtracting the first equality multiplied by $\chi_n(y)$ from the second equality, and taking into account that x can be any element of A, we obtain

$$a_1(\chi_1(y) - \chi_n(y))\chi_1 + \cdots + a_{n-1}(\chi_{n-1}(y) - \chi_n(y))\chi_{n-1} \;=\; 0\,.$$

By induction hypothesis all coefficients of the linear combination on the left hand side must be 0; in particular, a_1 must be 0. But then the left hand side of (1) is a linear combination of $n - 1$ characters, hence $a_2 = \cdots = a_n = 0$ by induction hypothesis. □

In the proof above we did not need any properties of the operation on A whatsoever. However, the multiplicative structure of K is that of a commutative monoid; therefore, if $\approx$ is the least congruence on A that makes the operation of the quotient structure $A/\!\approx$ commutative and associative, then every character of A in K factors through $A \to A/\!\approx$ to give the correponding character of the commutative semigroup $A/\!\approx$ in K. Because of this we may always assume that A itself is already a commutative semigroup (but we do not need to). Usually, A will be a commutative monoid; in such a case every character of A in K will map the neutral element of A to 1 (i.e. it will be a homomorphism of monoids),

since the only other possibility is that the neutral element of A would map to 0, thus every element of A would map to 0, so we would have the zero mapping which is not a character.

Note that a character, as we have defined it, is not required to have only nonzero values, it suffices that it attains at least one nonzero value. For example, if A is a commutative monoid and U is the set of invertible elements of A, then the characteristic function $\chi_U\colon A \to K$, mapping elements of U to 1 and other elements of A to 0, is a character; in particular, the mapping $\chi_0\colon \mathbb{N} \to K : n \mapsto 0^n$ (where $0^0 = 1$) is a perfectly respectable character of the additive monoid $\mathbb{N}$ in K. However, every character of a monoid A in K maps invertible elements of A to nonzero elements of K; thus, if A is a group, then a character of A in K is a homomorphism of the group A into the multiplicative group $K^\times$ of all nonzero elements of the field K.

The Dedekind's theorem has well-known applications in Galois theory, and not only there. We will show how it can be used to determine the dimension of the vector space K^I over a field K (consisting of all maps $I \to K$) when I is an infinite set. If this result manages to infiltrate an algebra textbook at all, it finds itself tucked away out of sight as an exercise, without any clear indication that it can be obtained using Dedekind's theorem.

Proposition 2. *Let K be a field and I an infinite set. Then* $\dim_K(K^I) = \left|K^I\right| = |K|^{|I|}$.

Proof. Let $M = I \cdot \mathbb{N}$ be the coproduct of I copies of the additive monoid $\mathbb{N}$, in the category of commutative monoids. One of incarnations of M is the additive monoid of all formal linear combinations $\sum_{\iota\in I} n_\iota \cdot \iota$ with coefficients $n_\iota \in \mathbb{N}$ nonzero for only finitely many $\iota \in I$. The general form of a character of M in K is $\chi_x\colon \sum_\iota n_\iota \cdot \iota \mapsto \prod_\iota x_\iota^{n_\iota}$, for an arbitrary $x \in K^I$. The characters χ_x and χ_y corresponding to different $x, y \in K^I$ are distinct, since $x_\kappa \neq y_\kappa$ for some $\kappa \in I$, hence $\chi_x(1\cdot\kappa) = x_\kappa \neq y_\kappa = \chi_y(1\cdot\kappa)$. We know that $|M| = |I|$, so there is a bijection $\varphi\colon I \to M$; but then Dedekind's theorem tells us that $\chi_x \circ \varphi$, $x \in K^I$, are linearly independent elements of K^I. We have shown that $\dim_K(K^I) \geqslant \left|K^I\right|$; the other inequality, $\dim_K(K^I) \leqslant \left|K^I\right|$, is of course evident. □

Note that Proposition 2 is a theorem in ZFC: we have the equality of cardinals $|M| = |I|$, hence the existence of a bijection $M \to I$, courtesy of the axiom of choice.