NAK and injectivity of surjections

Kazimierz Szymiczek

1. Vector spaces: injectivity equivalent to surjectivity

We propose to study analogs and generalizations of the following simple fact from linear algebra.

PROPOSITION 1. *Let V be a finite dimensional vector space over an arbitrary field K. If $h : V \to V$ is an endomorphism of V, then h is injective if and only if h is surjective.*

PROOF. h is injective if and only if $\dim \ker h = 0$, and h is surjective if and only if $\dim \operatorname{im} h = \dim V$. Since

$$\dim \ker h + \dim \operatorname{im} h = \dim V,$$

we see that $\dim \ker h = 0$ if and only if $\dim \operatorname{im} h = \dim V$. □

The finiteness of dimension of vector space is a decisive hypothesis. For infinite dimensional vector spaces surjectivity and injectivity of an endomorphism are independent properties.

EXAMPLE 1. For an arbitrary field K, the differentiation on the vector space $K[X]$ of polynomials over K is a surjective endomorphism $K[X] \to K[X]$ but it is not injective.
On the other hand multiplication by X is an injective endomorphism of the vector space $K[X]$ but it is not surjective.

2. Free modules: injectivity does not imply surjectivity

We want to generalize the setup and study relation between injectivity and surjectivity of an endomorphism of a module M over a ring A. To keep close to the case of vector spaces we first consider free modules. A free module M over A has a basis which is a linearly independent set spanning M. A vector space always has a basis and so is automatically a free module (over the underlying field). At the first sight, working with free modules, we are in almost the same situation as in vector spaces. However there are remarkable differences. First, for free modules of finite rank we cannot use the technique of the proof of Proposition 1, since for an endomorphism $h : A^n \to A^n$ of the free $A-$module A^n there does not exist any corresponding result to the theorem on the sum of dimensions of the kernel and of the image of an endomorphism of a (finite dimensional) vector space. Submodules $\ker h$ and $\operatorname{im} h$ of the module A^n are not, in general, free modules. For example, direct summands of A^n, that is, projective modules, are not in general free modules.
But this is not only the matter of proof. Simply injectivity of an endomorphism of a free module (of finite rank) does not imply its surjectivity. This is shown in the following example.

Talk at Ostrava University in April 2004.

EXAMPLE 2. Let A be an integral domain and let $a \in A$ be a non-invertible nonzero element of A. Then the principal ideal $(a) = aA$ is a proper ideal (that is $(a) \neq A$) and is an $A-$module isomorphic to A. The map

$$A \to aA, \quad x \mapsto ax$$

is an isomorphism. It can be viewed as an injective endomorphism of the free $A-$module A of rank 1. But it is not surjective. So injectivity does not imply surjectivity.

3. Finitely generated modules: surjectivity implies injectivity

The question that still makes sense is the following: does surjectivity of an endomorphism of an $A-$module imply injectivity of the endomorphism? The answer turns out to be yes for all finitely generated $A-$modules and for all rings A. Before going on we make the following remark on the image of an endomorphism of a f.g. module.

REMARK 1. Let $h : M \to M$ be an endomorphism of a f.g. $A-$module M. To be more specific assume that M is generated by the elements $x_1, \ldots, x_n$. Then we can write

$$h(x_i) = \sum_{j=1}^{n} a_{ij} x_j \quad \text{for some} \quad a_{ij} \in A.$$

Consider now the ideal

$$I = (a_{11}, \ldots, a_{ij}, \ldots, a_{nn}) = a_{11}A + \cdots + a_{ij}A + \cdots + a_{nn}A$$

of the ring A generated by all the coefficients a_{ij}. Then for any element $m = \sum c_i x_i \in M$, where $c_i \in A$, we have

$$h(m) = \sum_i c_i h(x_i) = \sum_i c_i \sum_j a_{ij} x_j = \sum_j (\sum_i c_i a_{ij}) x_j.$$

The coefficients $\sum_i c_i a_{ij}$ all belong to the ideal I and so $h(m)$ belongs to the submodule

$$IM = \left\{ \sum a_i m_i : a_i \in I, \quad m_i \in M \right\}$$

of the module M (here, of course, we consider only finite sums of elements of M). Thus $h(M) \subseteq IM$. We have shown that for each endomorphism $h : M \to M$ of an $A-$module M there always exists an ideal I of the ring A such that $h(M) \subseteq IM$. For example, if h is surjective, $I = A$ will do.

We now proceed to the proof of theorem saying that for finitely generated modules surjectivity of an endomorphism implies injectivity of the endomorphism. The proof is based on Nakayama Lemma and the proof of the latter uses the following lemma.

LEMMA 1. *Let M be a finitely generated $A-$module and suppose it is generated by $n < \infty$ elements. Let $h : M \to M$ be an endomorphism of M and let I be an ideal in A such that $h(M) \subseteq IM$. Then there are $a_i \in I$ satisfying*

$$h^n + a_1 h^{n-1} + \cdots + a_{n-1} h + a_n 1_M = 0_M, \tag{1}$$

where 1_M and 0_M are the identity and zero endomorphism, respectively.

PROOF. We give a typical proof taken from [**1**, Prop. 2.4] (see also [**2**, Theorem 2.1]). Let $x_1, \ldots, x_n$ be a set of generators for the module M. Since $h(M) \subseteq IM$, for each x_i there are elements $a_{ij} \in I$ such that

$$h(x_i) = \sum_{j=1}^{n} a_{ij} x_j.$$

Thus we get n equalities of the form

$$\sum_{j=1}^{n}(h\delta_{ij} - a_{ij})x_j = 0, \qquad 1 \leq i \leq n.$$

Here the entries of the matrix $H := [h\delta_{ij} - a_{ij}]$ are viewed as endomorphisms of the module M. They belong to the commutative subring $A[h]$ of the ring of all endomorphisms of M (here we identify the ring A with the ring of scalar endomorphisms $\{a1_M : a \in A\}$). Let H_{ij} be the cofactor of the entry $h\delta_{ij} - a_{ij}$ of the matrix H and let $d = \det H$. So d is an endomorphism of M. We shall show that d is the zero endomorphism. Fix k and multiply each of the above equalities by H_{ik}. On adding we get $dx_k = 0$. Hence the endomorphism d sends each generator of the module M to zero and so $d = 0$ is the zero endomorphism. Computing now $d = \det H$ using row and column expansions we get the equality (1). □

The main tool used in the solution of our *surjectivity-implies-injectivity-problem* is Nakayama Lemma. There are several versions of the Lemma and we reproduce here the following general version from [**2**, Theorem 2.2, p. 8]. Matsumura points out that Nakayama himself maintained that this result was earlier known to Azumaya and Krull. To acknowledge the priorities Matsumura uses the short form NAK for the result suggesting that he thinks of it as Nakayama-Azumaya-Krull Lemma. Alternatively, NAK is a short form of Nakayama's name as well.

LEMMA 2 (NAK Lemma). *Let M be a finitely generated $A-$module and let I be an ideal in A. If $M = IM$, then there is an $a \in A$ such that*

$$aM = 0 \quad \text{and} \quad a \equiv 1 \pmod{I}.$$

PROOF. Take $h = 1_M$ to be the identity endomorphism. Since $M = IM$ we have $h(M) = M \subseteq IM$ and so we can use Lemma 1. So we get the equality

$$1_M + a_1 1_M + \cdots + a_n 1_M = 0_M$$

with some $a_i \in I$. Put now

$$a := 1 + a_1 + \cdots + a_n \in A.$$

Then $aM = (a1_M)M = 0$ and $a \equiv 1 \pmod{I}$. □

Now we are ready to prove the following definitive result. This is proved in [**2**, Theorem 2.4, p. 9] and is ascribed there to Vasconcelos.

THEOREM 1. *Let M be a finitely generated $A-$module and let $h : M \to M$ be an endomorphism. If h is surjective, then h is injective.*

PROOF. M can be viewed as an $A[X]-$module when for $F(X) \in A[X]$ and $m \in M$ we define the product by setting

$$F(X) \cdot m = F(h)(m).$$

In particular $X \cdot m = h(m)$ and since h is assumed to be surjective we have $XM = M$, that is $(X) \cdot M = M$ for the principal ideal $I = (X) = X \cdot A[X]$. Clearly $A[X]-$module M is finitely generated hence by Nakayama Lemma there is an $a \in A[X]$ such that $aM = 0$ and $a \equiv 1 \pmod{X}$. Hence $a = 1 + XY$ for a certain polynomial $Y \in A[X]$ and $(1 + XY) \cdot M = 0$. If $u \in \ker h$, then

$$0 = (1 + XY)u = u + Y \cdot h(u) = u$$

because $h(u) = 0$. Hence $u = 0$, $\ker h = 0$ and so h is injective, as desired. □

We state the result in the particular case of $\mathbb{Z}-$modules, that is, abelian groups.

COROLLARY 1. *Let M be a finitely generated abelian group and let $h : M \to M$ be an endomorphism. If h is surjective, then h is injective.*

4. Noetherian rings: surjectivity implies injectivity

It turns out that a result similar to Theorem 1 can also be proved for rings. The following theorem is proposed as an exercise in Matsumura's book [**2**, Ex. 3.6, p. 19].

THEOREM 2. *Let A be a noetherian ring and let $h : A \to A$ be a ring homomorphism. If h is surjective, then h is injective.*

PROOF. Consider the iterates $h^1 = h, h^2 = h \circ h, \dots, h^{n+1} = h^n \circ h$ of the endomorphism h. It is easy to observe that, first, they are all surjective maps, and second, the kernels $\ker h^i$ form an ascending chain of ideals in the ring A:

$$\ker h \subseteq \ker h^2 \subseteq \cdots \subseteq \ker h^n \subseteq \cdots .$$

Since A is noetherian, there is a natural number n such that

$$\ker h^n = \ker h^{n+1}.$$

Take now an arbitrary element $a \in \ker h$. Since h^n is surjective, there is $b \in A$ such that $a = h^n(b)$. Then

$$0 = h(a) = h(h^n(b)) = h^{n+1}(b).$$

Hence $b \in \ker h^{n+1} = \ker h^n$ and so $a = h^n(b) = 0$. Thus $\ker h = 0$ and h is an injective homomorphism. □

REMARK 2. The ring A can be viewed as a free $A-$module of rank 1. One could expect that Theorem 2 should follow from Theorem 1. This is not so and the reason is that a ring endomorphism of A is not in general an endomorphism of the $A-$module A (and *vice versa*). For the ring endomorphism we have

$$h(ab) = h(a)h(b) \qquad \text{for} \quad a, b \in A$$

and for the $A-$module endomorphism we have

$$h(ab) = ah(b) \qquad \text{for} \quad a, b \in A$$

so that, in general, the two maps do not act in the same way on the products of elements in A.

References

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra.* Addison-Wesley, Reading, Mass. 1969.
[2] H. Matsumura, *Commutative ring theory.* Cambridge University Press, Cambridge 1986.

INSTYTUT MATEMATYKI, UNIWERSYTET ŚLĄSKI, KATOWICE
E-mail address: szymiczek@math.us.edu.pl