Idempotent lifting

Idempotent lifting is the following statement:

Theorem 0.1. *Let $R \to S$ be a surjection of rings with nilpotent kernel, and let $e \in S$ be an idempotent. Then there exists an antecedent $\tilde{e} \in R$ which is also an idempotent.*

The usual proofs rely on some calculational trick, and do not really clarify the situation. Here is one proof that I learned from Eric Wofsey on MSE, in the commutative case :

Proof. Because the kernel is nilpotent, the induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is a homeomorphism.

If $S \cong S_0 \times S_1$ through some nilpotent e, then this yields a clopen decomposition $\mathrm{Spec}(S) \cong \mathrm{Spec}(S_0) \sqcup \mathrm{Spec}(S_1)$, and thus we get a compatible clopen decomposition $\mathrm{Spec}(R) = U \sqcup V$ which, because $\mathcal{O}_{\mathrm{Spec}(R)}$ is a sheaf, yields $R \cong \mathcal{O}(U) \times \mathcal{O}(V)$ which is compatible with the previous one, in other words it yields an idempotent lift. □

Let me make a few remarks about that proof:

- It is geometric, and we get a sense of *why* this happens. In particular, it is rather clear that it happens because of *idempotents*, and so, as opposed to calculational tricks, it is clear why this works for $x^2 = x$, and not other natural variations such as $x^n = x$ (see the end of the document for a counterexample)
- The difficulty is not completely removed though, it is hidden in the fact that $\mathcal{O}_{\mathrm{Spec}(R)}$ is a sheaf, where the same type of calculations appear.
- It only works in the commutative case. Of course, because of the general nature of the claim, the general case follows from the commutative case (fix one lift r of the idempotent e, then $\mathbb{Z}[r] \to \mathbb{Z}[e]$ are commutative rings and they satisfy the assumptions - where I abuse notation by writing $\mathbb{Z}[x]$ for the subring generated by x), but it feels weird to use commutative techniques for a general statement.

The proof I want to explain now keeps the first bullet point, which I find to be a positive point, while removing the two other bullet points, which I was unsatisfied with.

Of course, one has to change what one means with "geometry" in the noncommutative case, as schemes do not work so well. I take the Kontsevich school's point of view here, that noncommutative geometry is about categories of modules, which are themselves the geometric object.

First recall, from Morita theory:

Lemma 0.2. *Let R be a ring, and $U : \mathbf{Mod}_R \to \mathbf{Ab}$ the forgetful functor. Then there is an isomorphism of rings $\mathrm{End}(U) \cong R$, given by sending η to $\eta_R(1)$, and where the converse is $r \mapsto (r \cdot - : M \to M)_M$.*

Proof. This is just a classical Yoneda-type statement. □

Then, observe:

Proposition 0.3. *Let R be a ring and e an idempotent. Then it corresponds to a decomposition $U \cong eU \oplus (1-e)U$.*

Conversely a decomposition $U \cong A \oplus B$ comes from an idempotent $e \in R$.

Proof. The first part is standard. Now let $U \cong A \oplus B$, and consider the decomposition $R \cong A(R) \oplus B(R)$ as abelian groups. Then $1 \mapsto (a, b)$. I claim that the image e of $(a, 0)$ is an idempotent, and that this determines the decomposition.

Indeed, $R \cong \mathrm{End}(U) \cong \begin{pmatrix} \mathrm{End}(A) & \hom(B, A) \\ \hom(A, B) & \mathrm{End}(B) \end{pmatrix}$, and the endomorphism $U \to A \to U$ corresponds to the matrix $\begin{pmatrix} \mathrm{id}_A & 0 \\ 0 & 0 \end{pmatrix}$, which is indeed an idempotent. By the previous lemma, the image of 1 (which is precisely e) is an idempotent in R.

Now suppose M is an R-module. Then $e \cdot - : M \to M$ corresponds to $M \to A(M) \to M$, again by the previous lemma, and similarly $(1-e) \cdot - : M \to M$ corresponds to $M \to B(M) \to M$, which proves that $(A, B) \cong (eU, (1-e)U)$. □

The main observation is then that this kind of decomposition for S gives rise to one for R.

Proof of the theorem. We start by doing the usual reduction, namely that we may assume $\ker^2 = 0$. Indeed, letting $I := \ker$, we have the following composite, where n is the smallest such that $I^n = 0$: $R = R/I^n \to R/I^{n-1} \to ... \to R/I^2 \to R/I \cong S$ and if we can deal with the square-zero case, we can lift e along each of these morphisms.

So we now assume $I^2 = 0$. Let e be an idempotent in S, and fix an arbitrary lift $r \in R$ of e.

Consider the natural morphism of abelian groups $M \to S \otimes_R M \cong e(S \otimes_R M) \oplus (1-e)(S \otimes_R M)$.

Call M_e the preimage of $e(S \otimes_R M)$ and $M_{\overline{e}}$ the preimage of the complement $(1-e)(S \otimes_R M)$. We have $M_e \cap M_{\overline{e}} = \ker(M \to S \otimes_R M) = IM$.

Now observe that IM itself is an R-submodule of M, but where I acts as 0 (because $I^2 = 0$), so that it is in fact canonically an S-module. It follows that $IM = r(IM) \oplus (1-r)IM$.

We now claim that the inclusion of abelian groups $(1-r)IM \subset M_e \cap M_{\overline{e}} \subset M_e$ is canonically split.

Indeed, if $x \in M_e$, then $(1-r)x \in IM$ and so $(1-r)^2 x \in (1-r)IM$. Furthermore, if $x \in (1-r)IM$, then $(1-r)^2 x = x$, precisely because $1-e$ is an idempotent, and IM is an S-module.

In particular, we can write $M_e = M(e) \oplus (1-r)IM$, and similarly $M_{\overline{e}} = M(\overline{e}) \oplus rIM$. The claim is that $M \cong M(e) \oplus M(\overline{e})$.

Remark 0.4. The point here is that $M = M_e + M_{\overline{e}}$, with intersection $IM = rIM \oplus (1-r)IM$, and one can actually write each one as $M_e = M(\overline{e}) \oplus (1-r)IM$, $M_{\overline{e}} = M(\overline{e}) \oplus rIM$, so that now there is no overlap but we still cover everything. We now prove this in detail.

So first of all, they are in direct sum. Indeed, suppose $x \in M(e) \cap M(\overline{e})$. Then $x \in M_e \cap M_{\overline{e}} = IM$, and $0 = (1-r)^2 x = (1-e)x$, and $0 = r^2 x = ex$ (where we again use the S-module structure on IM), so that $x = ex + (1-e)x = 0$.

Second, let $x \in M$. Then $x = y + z$ for some $y \in M_e, z \in M_{\overline{e}}$. Further write $y = y' + y'', y' \in M(e), y'' \in (1-r)IM, z = z' + z'', z' \in M(\overline{e}), z'' \in rIM$, and one finds $x = y' + z'' + z' + y''$. Now $z'' \in rIM$, which implies $(1-r)z'' = 0$, so $z'' \in M(e)$, and similarly $y'' \in M(\overline{e})$.

This proves the claim, and thus $U_R \cong U_R(e) \oplus U_R(\overline{e})$, lying over the corresponding decomposition $U_S \cong eU_S \oplus (1-e)U_S$. This provides an idempotent for R which lies over e. □

Remark 0.5. In this proof, we basically replaced $\mathrm{Spec}(R)$ by $U : \mathbf{Mod}_R \to \mathbf{Ab}$, and treated the (dual of the) latter as a geometric object.

This proves the claim, but also allows us to find the corresponding calculations.

Indeed, take the case $M = R$. Then it suffices for us to find the decomposition associated to 1, by simply following the above proof.

We start by writing $1 = r + (1-r)$, then write r as $r(1-r)^2 + r(1-(1-r)^2)$ and $1-r$ as $(1-r)r^2 + (1-r)(1-r^2)$.

This should give us the $R(e)$-term (our idempotent lift) as $r(1-(1-r)^2) + (1-r)r^2 = r - r(1-r)^2 + r^2 - r^3 = r - r(1-2r+r^2) + r^2 - r^3 = r - r + 2r^2 - r^3 + r^2 - r^3 = 3r^2 - 2r^3$.

But now one may first observe that $3r^2 - 2r^3$ is indeed a lift of e, but also if we write $r^2 = r + i$ with $i \in I$, we find $r^3 = r^2 + ri = r + i + ri$, and so $3r^2 - 2r^3 = 3r + 3i - 2r - 2i - 2ri = r + i - 2ri$, and $(r + i - 2ri)^2 = (r+i)^2 - 4(ri)(r+i)$ (as $I^2 = 0$), and this is further $r^2 + 2ri - 4rir = r + i + 2ri - 4(r+i)i = r + i + 2ri - 4ri = r + i - 2ri$ (observe that $i = r^2 - r$ commutes with r).

It follows that $3r^2 - 2r^3 = r + i - 2ri$ is indeed an idempotent, which of course one could have found beforehand, if one were into calculational tricks.

The above proof hides *nothing*, but is still able to recover this calculation without getting into it, or having to guess it somehow.

Furthermore, if one were just presented with the calculational proof, it would not be clear a priori that one could not find similar tricks for things like $x^n = x$ that sound like reasonable generalizations of $x^2 = x$, whereas the above proof clearly only works for idempotents.

And here is a counterexample for $n = 4$: consider $\mathbb{Z}[x]/(x^3-1)^2 \to \mathbb{Z}[x]/(x^3-1)$.

In the quotient, $x^3 = 1$ and so $x^4 = x$. In particular, a lift y of x should exist, and because x is a unit and the kernel is nilpotent, y would have to be a unit too, so actually satisfy $y^3 = 1$. But then if we write $y = x + (x^3-1)P$ for some integer coefficients P, we find that we need $(x + (x^3-1)P)^3 - 1 = 0$, and so (because $(x^3-1)^2 = 0$) $x^3 - 1 + 3(x^3-1)P^2 = 0$, and so $1 + 3P^2$ would be divisible by $x^3 - 1$.

Evaluating at 1 gives a contradiction, as $1 + 3n = 0$ cannot happen for integer n.

In fact, inverting 3 is enough for this to work, and this is related to $\mathbb{Z}[\frac{1}{(n-1)}] \to \mathbb{Z}[\frac{1}{(n-1)}][x]/(x^n - x)$ being (formally) étale, but let us not get into this.

References