

Re: 2 rings with a special property

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-06/2176.html>

From: Robert Israel (israel_at_math.ubc.ca)

Date: 06/30/04

Date: 30 Jun 2004 05:45:29 GMT

In article <ce759023.0406291754.4e1bb810@posting.google.com>, Bessel <crypto_170@hotmail.com> wrote:

>I want to find two rings R_1 , R_2 and a homomorphism $f: R_1 \rightarrow R_2$ between
>the two rings. I need some special properties:

- >1. R_1 should have many ideals
- >2. Kernel of f should not look too "special" in any way.
- >I.e. for example if we are dealing with matrices and the kernel of
>homomorphism is such that last column or last row is all zeroes, then
>it's not quite satisfactory because then it looks "special" as opposed
>to other regular elements which don't have this 0s property.
- >3. I also would like $|\ker f|/|R_1|$ to be fairly small.

I assume $|\cdot|$ is cardinality, so you're dealing with finite rings.
ker f of course will be an ideal. So I'd start with a large ring
with many small ideals, let J be a randomly-chosen small ideal, and
let f be the quotient map $R_1 \rightarrow R_1/J$. So $\ker f = J$, and its elements
won't be any more "special" than the elements of any other small ideal.

For example, let $R_1 = (\mathbb{Z}_2)^n$ with coordinatewise operations (so
 $(xy)_j = x_j y_j$), S a nonempty subset of $\{1, \dots, n\}$ (typically
with $|S|$ about $n/2$), $J = \{x \text{ in } R_1: x_k = 0 \text{ for } k \text{ in } S\}$. You can
also identify f as the restriction map of R_1 to
 $(\mathbb{Z}_2)^{\text{complement of } S}$. Then $|\ker f|/|R_1| = 2^{-|S|}$.

Robert Israel israel@math.ubc.ca
Department of Mathematics <http://www.math.ubc.ca/~israel>
University of British Columbia
Vancouver, BC, Canada V6T 1Z2