

MATH 113, HOMEWORK 8 SOLUTIONS

ALLEN KNUTSON

Homework #8 (due Thursday 12/7).

p261 #14,15,19,41,46,47. Also, show $\text{End}(A)$ is a ring exactly if A is commutative.

#14. In \mathbb{Z} , only ± 1 have inverses.

#15. In $\mathbb{Z} \times \mathbb{Z} = \{(a, b) : a, b \in \mathbb{Z}\}$, there are four invertible elements: $(\pm 1, \pm 1)$.

#19. In $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, 2 is not invertible; only 1 and 3 are.

#41. (AKA "The Freshman's Dream".) In an arbitrary ring, you can compute $(a + b)^n$; expand using distributivity n times, and you get a sum of 2^n terms, each one a product $aabbabba$ etc. of n terms. You could call this the "noncommutative binomial theorem."

In a *commutative* ring, you can rearrange those so the a s come before the b s. Then the number of times $a^k b^{n-k}$ shows up is, by definition, $\binom{n}{k}$ (we're choose-ing the locations of the k a s). So we get the usual binomial theorem:

$$(a + b)^n = \sum_k \binom{n}{k} a^k b^{n-k}$$

To emphasize – here we're using Nr , $N \in \mathbb{Z}$, $r \in$ some ring R to mean $r + r + \dots + r$ added N times (or subtracted if $N < 0$). This notation makes sense even if the integers are not a subring of R .

We know a formula for $\binom{n}{k}$: it's $n!/k!(n-k)!$. (We actually derived this in class, thinking about the action of S_n on the set of 2^n noncommutative terms – the orbits were indexed by the number of a s, and the stabilizer was $S_k \times S_{n-k}$. We went on to derive the binomial theorem from there.)

Now take the case $n = p$ prime. Then the numerator of $\binom{p}{k}$ has a factor of p in it. If $k \notin \{0, p\}$ then the denominator is a product of many numbers less than p – so there will be no factors of p in the denominator. Consequently $p | \binom{p}{k}$ for $k \notin \{0, p\}$. And for those two extreme cases, $\binom{p}{k} = 1$.

So all those middle terms are something added to itself p times (and then that $\binom{p}{k}/p$ many more times), so are zero.

#46. Since a is nilpotent, pick $m \in \mathbb{N}$ such that $a^m = 0$. Likewise for b , pick n so $b^n = 0$. We need to show that there exists an N such that $(a + b)^N = 0$. Doesn't matter if it's really, really big; it just has to exist.

I claim that $m + n$ has the desired property. Apply the binomial theorem:

$$(a + b)^{m+n} = \sum_k \binom{m+n}{k} a^k b^{m+n-k} = \sum_j \binom{m+n}{m+j} a^{m+j} b^{n-j}$$

Date: December 11, 2000.

(here I'm doing the change of variable $j = k - m$ for convenience – it doesn't really matter though). In fact we'll prove the better statement – *every term* in this sum is zero. (It's not that they trickily cancel one another out.)

Look now at the j th term; it's some (irrelevant) number times $a^{m+j}b^{n-j}$. Two cases: if $j \geq 0$, then the a part is zero. Whereas if $j \leq 0$, then the b part is zero! So every term dies.

(See for yourself that $m+n-1$ would've worked too. But who cares. Once it's nilpotent, it's nilpotent, and we don't have to be efficient about it.)

Note: if you mentioned a^{-1} or b^{-1} , you've been too corrupted by groups. These elements for sure don't *have* inverses, unless we're in the zero ring. You should be thinking along the lines of noninvertible matrices here.

#47. Show R has interesting nilpotents $\iff R$ has interesting solutions to $x^2 = 0$. (Here "interesting" means "other than 0 itself.")

The right-to-left direction is totally stupid – x will serve as our interesting nilpotent.

The left-to-right has more to do. Let y be our interesting nilpotent. (Better not call it x – we don't know $y^2 = 0$!) Then there is some n such that $y^n = 0$. And $n > 1$, or else y would be uninteresting.

Choose n the smallest such; i.e. $y^n = 0$ but $y^{n-1} \neq 0$. Then let $x = y^{n-1}$. (Or if you like, $y^{n/2}$, but then you have to discuss n even and odd as separate cases.) Then $x^2 = y^{2n-2} = y^n y^{n-2}$. Note: we can only factor this way because we know $n \geq 2$! Otherwise we'd be afraid about taking negative powers.

Then the y^n kills that product, so we know x^2 is zero; also $x = y^{n-1} \neq 0$, so x is interesting.

Q. Show $\text{End}(A)$ is a ring only if A is commutative, where $\phi + \rho$ is defined as $(\phi + \rho)(g) = \phi(g)\rho(g)$.

If A commutative (writing its group structure as "+"). All I wanted here was distributivity. One,

$$\phi(a + b) = \phi(a) + \phi(b),$$

is just the definition of homomorphism. The other,

$$(\phi + \rho)(a) = \phi(a) + \rho(a),$$

is just how we defined the addition in our ring.

If A not commutative. Let $\phi = \rho = \mathbf{1}$ the identity endomorphism of A . Then $(\phi + \rho)(g) = \phi(g)\rho(g) = gg = g^2$ is the squaring map $G \rightarrow G$. We showed long ago in class that this is a group homomorphism if and only if G is commutative (by comparing $ghgh$ to $gghh$).

E-mail address: allenk@math.berkeley.edu