CHM: A.7

Po-Shen Loh

24 March 2001

Problem 1 (A.6) *Let R be a finite commutative ring. Prove that R has a multiplicative identity element (1) if and only if the annihilator of R is 0 (that is, $aR = 0$, $a \in R$ imply $a = 0$).*

First, observe that there exist elements $e, x \in R$ such that $xe = x$: we can do the following "chain multiplication." Start with an element $a_1 \in R$. By the given information, there exists another element $a_2 \in R$ such that $a_1 a_2 \neq 0$. Now by a similar argument there exists $a_3 \in R$ such that $a_1 a_2 a_3 \neq 0$. Repeating this process, we can get arbitrarily long chains. For a given chain, let us define the partial products $\pi_n = \Pi_1^n a_i$. We have a finite ring R, so at some point our partial products will repeat; therefore, we have the form $\pi_n \alpha = \pi_n$ where α is a substring of the chain. Therefore, the opening claim is true.

Now we use an extremal argument. Let us select the $e \in R$ for which the ideal $I = \{x | xe = x\}$ is maximal. Proceed by indirect proof; suppose, for the sake of contradiction, that $I \neq R$. We show that we can choose $r, s \in R$ such that $rs \neq 0$, $rI = 0$, and $se = 0$. Observe that there exists some element $y \in R$ for which $ye \neq y$. Let $r = ye - y \neq 0$. But for any $x \in I$, $yex = yx \to rx = (ye - y)x = 0$, so r annihilates I. Use indirect proof to show that we can find our r, s as claimed: suppose that for all r found above, $rs = 0$ for all s that satisfy $se = 0$. This is equivalent to the statement $R - I \subset \text{Ann}(\text{Ann}(e))$.

We have finite rings, so by Lagrange's theorem applied to the additive groups, $|R - I| \geq |R|/2$ and $|\text{Ann}(\text{Ann}(e))| \leq |R|/2$; therefore, the inclusion above must be exact, so $R - I = \text{Ann}(\text{Ann}(e))$. This is not true, however, because $0 \in I \to 0 \notin R - I$ but $0 \in \text{Ann}(\text{Ann}(e))$. Our supposition is false, so our claim is indeed true.

We return to chain multiplication. Start with r and s, and build the chain as above, but this time start with $a_0 = r$, $a_1 = s$ and maintain the definition of $\pi_n = \Pi_1^n a_i$. By the same argument as above, we will be able to find a form $r\pi_n\alpha = \pi_n$. This translates into a relation $ye' = y$, where $y = \pi_n$ and $e' = r\alpha$. Since $r | e'$, we find that e' annihilates all of I, and similarly $s | y \to ey = 0$. Also, since $rI = 0$, by construction π_n is not contained in I. Observe that we have discovered that for all $x \in I$, $(e + e')x = ex + e'x = x + 0 = x$ and for all z in the ideal generated by y, $(e + e')z = ez + e'z = 0 + z$.

Therefore, the element $(e + e')$ is a better identity than e; it acts trivially on both I and the ideal generated by y. This violates our maximality condition, so our assumption that $I \neq R$ is false, and we are done. The identity is e.