Math 542 Exercises 18-19

Joe Timmerman

March 2, 2014

Exercise 18: Let $M \subset R$ be a maximal ideal. Suppose $ab = 0$. Prove $a \in M$ or $b \in M$.

Suppose $a, b \notin M$. By the theorem in class, we know that R/M is a field because M is maximal. First note that $(0+M) = M = 0 \in R/M$. Consider the element $(a+M)(b+M) \in R/M$. This is equal to $(ab+M) = (0+M) = 0$, by assumption. But since neither of these elements are in M, this means that one of $(a+M), (b+M)$ (both non-zero in R/M) is a zero divisor in R/M. But this is a contradiction, because fields can't have zero divisors. Thus, it must be that one of a, b is in M.

Exercise 19: Let α be a root of $p(x) = x^3 + x + 1$ in $\mathbb{Z}_2[x]$. Construct the multiplication table for $\mathbb{Z}_2[\alpha]$.

We know that $\alpha^3+\alpha+1 = 0$. We can arrange this to get the very helpful identity $\alpha^3 = 1+\alpha$. Also note that $\alpha^4 = \alpha^3\alpha = (1+\alpha)\alpha = \alpha + \alpha^2$. Using these identities, and the fact that any term with a coefficient of 2 is in fact 0, because our coefficients are in $\mathbb{Z}_2$, we get the following table:

	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	0	0	0	0	0	0	0
1	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
α	0	α	α^2	$\alpha+\alpha^2$	$1+\alpha$	1	$1+\alpha+\alpha^2$	$1+\alpha^2$
$1+\alpha$	0	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$	α^2	1	α
α^2	0	α^2	$1+\alpha$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	α	α^2+1	1
$1+\alpha^2$	0	$1+\alpha^2$	1	α^2	α	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$
$\alpha+\alpha^2$	0	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	1	α^2+1	$1+\alpha$	α	α^2
$1+\alpha+\alpha^2$	0	$1+\alpha+\alpha^2$	$1+\alpha^2$	α	1	$\alpha+\alpha^2$	α^2	$1+\alpha$

HW due Mar 3

Tao Ju

March 3, 2014

Problem 18
Let R be a commutative ring with 1. Let I be a maximal ideal in R. Suppose $ab = 0$. Prove that $a \in I$ or $b \in I$.

Proof:
Assume $a \notin I$.
Since I is the maximal ideal, we obtain $(a) + I = R$ from $I \subsetneq (a) + I$. Thus there exists some $r \in R$ and $x \in I$ s.t. $ar + x = 1$. Multiple it by b, we get $abr + xb = b \Rightarrow b = xb \in I$ since R is a commutative ring.
Therefore $a \in I$ or $b \in I$.

Problem 19
Consider $p(x) = x^3 + x + 1$ as a polynomial in $\mathbb{Z}_2[x]$. Suppose p has a root α is in some field extension. Construct the multiplication table for

$$\mathbb{Z}_2[\alpha] \stackrel{def}{=\!=} \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Z}_2\}$$

Solution:
We have $\alpha^3 + \alpha + 1 = 0$. Thus $\alpha \cdot \alpha^2 = \alpha + 1$ and $\alpha^2 \cdot \alpha^2 = \alpha^2 + \alpha$. Then, we can construct the multiplication table

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$