MATH 5590H HOMEWORK 9

BRENDAN WHITAKER

Exercise 7.1.14. *Let x be a nilpotent element of the commmutative ring R.*

(a) *Prove that x is either zero or a zero divisor.*

Proof. Since x is nilpotent, we know $\exists m \in \mathbb{Z}^+$ s.t. $x^m = 0$. If x is zero, we are done, so assume $x \neq 0$. We also assume m is the minimal such positive integer, since $0 \cdot 0 = 0$. Then we also know $x^{m-1} \neq 0$. So we have two nonzero elements, x, x^{m-1}, such that $xx^{m-1} = x^m = 0 \Rightarrow x$ is a zero divisor. □

(b) *Prove that rx is nilpotent $\forall r \in R$.*

Proof. Again we assume $x^m = 0$, where m is the least such positive integer where this holds true. Then we have

$$(rx)^m = r^m x^m = r^m \cdot 0 = 0,$$

since R is commutative. □

(c) *Prove that $1 + x$ is a unit in R.*

Proof. Note that $x^m + 1 = 1$. Then observe

$$(1 + x)(x^{m-1} - x^{m-2} + \cdots + (-1)^{m-2}x + (-1)^{m-1}) = x^m + 1 = 1.$$

Thus $(1 + x)$ has a multiplicative inverse and hence is a unit. □

(d) *Prove that the sum of a nilpotent element and a unit is a unit.*

Proof. Let x be nilpotent, so $x^m = 0$, where m is the minimial positive integer such that this is true, and let y be a unit. Then $\exists y^{-1} \in R$ s.t. $yy^{-1} = 1$. Suppose for contradiction that $x + y$ is not a unit. Then it has no multiplicative inverse, so $\forall z \in R$, $z(x + y) = r$ for some $r \in R$ s.t. $r \neq 1$. So let $z = y^{-1}$. Then we have

$$y^{-1}(x + y) = r$$

for some $r \in R$ s.t. $r \neq 1$. Thus

$$y^{-1}x + y^{-1}y = r.$$

We multiply by x^{m-1} on both sides

$$\begin{aligned} x^{m-1}xy^{-1} + x^{m-1}yy^{-1} &= x^{m-1}r, \\ x^{m-1} &= x^{m-1}r. \end{aligned} \tag{1}$$

Thus we must have that $r = 1$, and this is contradiction, hence $x + y$ must be a unit. □

Exercise 7.1.15. *Prove that every boolean ring is commutative.*

Proof. Let R be a boolean ring. Suppose $a, b \in R$ s.t. $a, b \neq 0$, $a \neq b$. Then observe

$$\begin{aligned} a + b = (a + b)^2 = a^2 + ab + ba + b^2 &= a + ab + ba + b \\ 0 &= ab + ba \\ -ba &= ab \end{aligned} \tag{2}$$

Date: AU17.

Also note for $a \neq 0$,

$$(-a) = (-a)(-a) = -(a)(-a) = -(-a^2) = a^2 = a,$$

which gives us $ab = ba$, hence R is commutative. $\square$

Exercise 7.1.21. *Let X be any nonempty set and let $\mathcal{P}(X)$ be the power set of X.*

(a) *Prove $\mathcal{P}(X)$ is a ring.*

Proof. We first prove that $\mathcal{P}(X)$ is an abelian group under the addition operation, where $\forall A, B \in \mathcal{P}(X)$, $A + B = (A \setminus B) \cup (B \setminus A)$. Let $A, B \subset X$, then $A \setminus B \subset A \subset X$ and $B \setminus A \subset B \subset X \Rightarrow A + B = (A \setminus B) \cup (B \setminus A) \subset X \Rightarrow$ we have closure under addition. Also $\varnothing$ is 0 since $\forall A \in \mathcal{P}(X)$, we have

$$\varnothing + A = (\varnothing \setminus A) \cup (A \setminus \varnothing) = (A \setminus \varnothing) \cup (\varnothing \setminus A) = \varnothing \cup A = A.$$

Now $\forall A \in \mathcal{P}(X)$, we have $-A = A$, since

$$A + A = (A \setminus A) \cup (A \setminus A) = \varnothing,$$

so we have inverses. Let $A, B, C \in \mathcal{P}(X)$. Then

$$\begin{aligned} A + (B + C) &= (A \setminus ((B \setminus C) \cup (C \setminus B))) \cup (((B \setminus C) \cup (C \setminus B)) \setminus A) \\ &= ((A \setminus (B \setminus C)) \cap (A \setminus (C \setminus B))) \cup (((B \setminus C) \setminus A) \cup ((C \setminus B) \setminus A)) \\ &= ((A \setminus (B \setminus C)) \cap (A \setminus (C \setminus B))) \cup (B \setminus (C \cup A)) \cup (C \setminus (B \cup A)) \\ &= (A \setminus (B \cup C)) \cup (A \cap B \cap C) \cup (B \setminus (C \cup A)) \cup (C \setminus (B \cup A)) \qquad (3) \\ (A + B) + C &= (((A \setminus B) \cup (B \setminus A)) \setminus C) \cup (C \setminus ((A \setminus B) \cup (B \setminus A))) \\ &= (((A \setminus B) \setminus C) \cup ((B \setminus A) \setminus C) \cup (C \setminus (A \setminus B)) \cap (C \setminus (B \setminus A))) \\ &= (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus (A \cup B)) \cup (A \cap B \cap C), \end{aligned}$$

thus we have associativity of addition. So $\mathcal{P}(X)$ is a group under addition. Additionally,

$$A + B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = (B + A),$$

because of commutativity of set unions, and thus we have that $\mathcal{P}(X)$ is abelian. We now check that multiplication, defined as $A \times B = A \cap B$, satisfies is associative and satisfies distributivity. Note associativity is immediate since set intersections are commutative, and

$$\begin{aligned} (A + B) \times C &= ((A \setminus B) \cup (B \setminus A)) \cap C \\ &= ((A \setminus B) \cap C) \cup ((B \setminus A) \cap C) \\ (A \times C) + (B \times C) &= ((A \cap C) \setminus (B \cap C)) \cup ((B \cap C) \setminus (A \cap C)) \\ &= ((A \setminus B) \cap C) \cup ((B \setminus A) \cap C). \end{aligned} \qquad (4)$$

Also $A \times (B + C) = (A \times B) + (A \times C)$ holds as well because of commutativity of set intersections. Thus $\mathcal{P}(X)$ is a ring. $\square$

(b) *Prove that this ring is commutative, has an identity, and is a Boolean ring.*

Proof. Recall from part (*a*) that multiplication is commutative because set intersections are commutative. Also, X is our identity since $\forall A \in \mathcal{P}(X)$, $A \subset X \Rightarrow A \times X = A \cap X = A$. Now let $A \in \mathcal{P}(X)$, then $A^2 = A \times A = A \cap A = A$, and thus $\mathcal{P}(X)$ is a Boolean ring. $\square$

Exercise 7.2.2. *Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$. Prove that $p(x)$ is a zero divisor in $R[x]$ if and only if there is a nonzero $b \in R$ s.t. $bp(x) = 0$.*

Proof. If there exists such a b, then $p(x)$ must be a zero divisor, so we need only prove that if $p(x)$ is a zero divisor, then there exists such a b. Let $g(x) = b_m x^m + \cdots b_1 x + b_0$ be a nonzero polynomial of minimal degree such that $g(x)p(x) = 0$. Then suppose $b_m a_n \neq 0$. Then we must have that $b_m \neq 0 \neq a_n$. But $g(x)p(x)$ contains the term $b_m a_n x^{n+m}$, so we must have that $g(x)p(x) \neq 0$, which is contradiction, so $b_m a_n = 0$. Thus $a_n g(x)$ is a polynomial of degree less than m such that $a_n g(x)p(x) = 0$. But we said $g(x)$ was the nonzero polynomial of minimal degree such that $g(x)p(x) = 0$, so we must have that $a_n g(x) = 0$. Now we show that $a_{n-i} g(x) = 0$ for $i = 0, 1, ..., n$. Let $i = 0$. We already know that $a_n g(x) = 0$, so the base case holds. Suppose $a_{n-i} g(x) = 0$. We wish to prove that $a_{n-(i+1)} g(x) = 0$. We claim $b_m a_{n-(i+1)} = 0$. Suppose $b_m a_{n-(i+1)} \neq 0$.

Then $b_m \neq 0 \neq a_{n-(i+1)}$. But again, since $g(x)p(x)$ contains a term $kb_m a_{n-(i+1)}x^{m+(n-(i+1))}$ for some nonzero $k \in R$, we must have that $g(x)p(x) \neq 0$, which again is a contradiction, so $b_m a_{n-(i+1)} = 0$. Then suppose $a_{n-(i+1)}g(x) \neq 0$. Then this polynomial has degree less than m, since $b_m a_{n-(i+1)} = 0$ and this contradicts the definition of $g(x)$, so we must have that $a_{n-(i+1)}g(x) = 0$. By induction, $a_{n-i}g(x) = 0$ for all $i \leq n$, and thus $b_m a_i = 0$ for all i, since otherwise $g(x)p(x) \neq 0$, so then we know b_m is our desired element b. $\square$

Exercise 7.2.10. *Consider the following elements of the integral group ring $\mathbb{Z}S_3$:*

$$\alpha = 3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3) \quad \textit{and} \quad \beta = 6(1) + 2(2\ 3) - 7(1\ 3\ 2),$$

where 1 *is the identity of S_3. Compute the following elements:*

(a) $\alpha + \beta = 6(1) - 3(2\ 3) + 14(1\ 2\ 3) - 7(1\ 2\ 3) + 3(1\ 2)$.

(b)

$$\begin{aligned}\alpha\beta &= 18(1\ 2) + 6(1\ 2\ 3) - 21(1\ 3) - 30(2\ 3) - 10(1) + 35(1\ 2) + 84(1\ 2\ 3) + 28(1\ 2) - 98(1) \\ &= 81(1\ 2) + 90(1\ 2\ 3) - 21(1\ 3) - 30(2\ 3) - 108(1)\end{aligned} \tag{5}$$