

# Homework 6

Madilyn Simons

1. To prove that “is an associate of” is an equivalence relation on  $R$ , we must show that it is reflexive, symmetric, and transitive.

First, since  $R$  is a commutative ring, there exists some identity element in  $R$ ,  $1_R$ , such that  $a1_R = a$ . We can say that  $1_R$  is a unit since  $(1_R)(1_R) = 1_R$ . Since  $a1_R = a$ ,  $a$  is an associate of  $a$  and “is an associate of” is reflexive.

Next, let  $a, b \in R$  such that  $a$  is an associate of  $b$ . Therefore, there exist some unit,  $u$ , in  $R$  such that  $a = bu$ . Since  $u$  is a unit, there also exists some unit  $v \in R$  such that  $uv = 1_R$ .

If  $a = bu$ , then

$$av = buv = b1_R = b$$

Therefore,  $b$  is an associate of  $a$  and “is an associate of” is reflexive.

Finally, let  $a$  be an associate of  $b$  and let  $b$  be an associate of  $c$  for some elements  $a, b, c \in R$ . Therefore,  $a = bu$  and  $b = cv$  for some units  $u, v \in R$ .

We notice that

$$a = bu = cvu$$

We know that  $vu$  is a unit because there exists some  $v^{-1}, u^{-1} \in R$  such that  $vv^{-1} = 1_R$  and  $uu^{-1} = 1_R$  since  $v$  and  $u$  are units. Thus,  $(vu)(v^{-1}u^{-1}) = (vv^{-1})(uu^{-1}) = 1_R$  and so  $vu$  is a unit. Since  $vu$  is a unit,  $a$  is an associate of  $c$  and “is an associate of” is transitive.

2. (a) There are 4 different quadratic polynomial in  $(\mathbb{Z}/2\mathbb{Z})[x]$ :

$$x^2$$

$$x^2 + 1$$

$$x^2 + x$$

$$x^2 + x + 1$$

Let  $f(x)$  be any quadratic polynomial in  $(\mathbb{Z}/2\mathbb{Z})[x]$ . We know that if  $f(x) = x^2$ , then  $f(x)$  is reducible because 0 is a root. If  $f(x) = x^2 + 1$ ,

then  $f(x)$  is reducible because 1 is a root. If  $f(x) = x^2 + x$ , then  $f(x)$  is reducible because 1 is a root.

If  $f(x) = x^2 + x + 1$ , then  $f(x)$  is irreducible because  $f(x)$  has no roots in  $(\mathbb{Z}/2\mathbb{Z})[x]$ :

$$f(0) = 0^2 + 0 + 1 = 1$$

$$f(1) = 1^2 + 1 + 1 = 3 = 1$$

Therefore the only irreducible quadratic polynomial in  $(\mathbb{Z}/2\mathbb{Z})[x]$  is  $x^2 + x + 1$ .

- (b) No, because  $f(1) = 0$ .
  - (c) No, because  $g(x) = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 - x + 1)$ .
  - (d) Yes. Since  $h(x)$  does not have any roots, it is not divisible by a polynomial with degree 1. Therefore, it can only be the product of an irreducible polynomial with degree 2 and an irreducible polynomial of degree 3. The only irreducible polynomial with degree 2 in  $\mathbb{Z}/2\mathbb{Z}$  is  $x^2 + x + 1$ . Therefore, if  $h(x)$  is reducible, then it is divisible by  $\mathbb{Z}/2\mathbb{Z}$  in  $x^2 + x + 1$ . However,  $h(x)$  is NOT divisible by  $\mathbb{Z}/2\mathbb{Z}$ , so it must be irreducible.
3. By Eisenstein's Criterion,  $p(x)$  is irreducible. Let  $q = 2$ . Since  $q$  is a prime that divides all of the coefficients except for the leading coefficient and  $q^2$  does not divide 34,  $p(x)$  is irreducible.
  4. Let  $p = 11$ . Then  $\bar{q}(x) = x^4 + 7x + 5$ . Since  $\bar{q}(x)$  is irreducible in  $(\mathbb{Z}/p\mathbb{Z})[x]$  and  $p$  does not divide the leading coefficient of  $q(x)$ ,  $q(x)$  is irreducible.