

2. If  $f(x)$  is reducible over  $D$  then it factors as  $f(x) = g(x)h(x)$ . However it is irreducible over  $F$  which means one of  $g(x)$  or  $h(x)$  is a unit in  $F[x]$ , i.e. a constant polynomial. Thus the factorization over  $D$  has one polynomial constant. For example  $2x^2 - 4x$  where  $D$  is the integers factors as  $2(x^2 - 2)$ .

6. We know  $Z_p[x]/(f(x))$  is a field by Cor. 1, p.309. Let  $I = (f(x))$ . For any  $g(x) \in Z_p[x]$  we can use the division algorithm to write  $g(x) = q(x)f(x) + r(x)$  with degree of  $r(x) < n$ . But  $q(x)f(x) \in I$  so  $g(x) + I = r(x) + I$ . Thus every coset can be written in the form  $r(x) + I$  with  $r(x)$  having degree  $\leq n - 1$ . Two distinct such cosets are never equal because  $r_1(x) - r_2(x)$  would have to be divisible by  $f(x)$ , which has larger degree. Thus:

$$\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + I \mid a_i \in Z_p\}$$

is a complete set of elements in  $Z_p[x]/(f(x))$ . Since there are  $p$  choices for each  $a_i$ , there are  $p^n$  such elements.

7.  $Z_5[x]/(x^2 - 3)$  is a field since  $x^2 - 3$  is irreducible over  $Z_5$ . It has 25 elements by # 6.

8.  $Z_3[x]/(x^3 + 2x + 1)$  is a field of order 27.

13. See back.

14.  $x^3 + x^2 + x + 1 = (x + 1)^3$  over  $Z_2$ .

10. a. Irreducible by EC  $p = 3$ .

b. Consider  $x^4 + x + 1$  reduced mod 2. It has no roots, so does not have a linear factor. Suppose  $x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$  with  $a, b, c, d \in Z_2$ . Then  $b = d = 1$ . Considering the  $x$  coefficient we get  $bc + ad = 1$ , so  $c + a = 1$  so WLOG we have  $a = 1$  and  $c = 0$ . Check that  $(x^2 + x + 1)(x^2 + 1)$  has nonzero  $x^3$  coefficient. Thus this factorization cannot work.  $x^4 + x + 1$  is irreducible mod 2, and hence over  $Z$ .

c. Irreducible by EC  $p = 3$ .

d. Consider this polynomial mod 2, it is  $x^5 + x^2 + 1$ . This has no roots so no linear factors. Again suppose

$$x^5 + x^2 + 1 = (x^3 + ax^2 + bx + c)(x^2 + dx + e)$$

with  $a, b, c, d, e \in Z_2$ . Equating constant terms gives us  $c = e = 1$ . Then the  $x$  term gives  $b + d = 0$ , i.e.  $b = d$ . Turning to the  $x^2$  coefficient we get  $a + b^2 + 1 = 1$ , so  $a = b$ . Finally the  $x^3$  term is  $e + ad + b$  which is  $1 + a^2 + a$  which is always 1, giving a contradiction. Thus the polynomial is irreducible mod 2 and hence over  $Z$ .

e. Multiply by 14 then apply the EC with  $p = 3$ .

17.  $x^2 + x + 1$  is irreducible over  $Z_2$  so  $Z_2[x]/(x^2 + x + 1)$  is a field of order 4. For  $p > 2$  notice that  $a \neq -a$  for any  $a \neq 0$ . However  $a^2 = (-a)^2$ . Thus there are only  $1 + p/2$  perfect

squares, which is less than  $p$ . Thus choose  $c \in Z_p$  not a perfect square. Then  $x^2 - c$  is irreducible so  $Z_p[x]/(x^2 - c)$  is a field with  $p^2$  elements.

23. See back.

25. See back.

32. Consider  $Z[x]/(x^2 + 1)$ . Let  $I = (x^2 + 1)$ . Notice that  $x^2 + I = -1 + I$ . Thus any element  $p(x) + I$  is equal to  $ax + b + I$  for some  $a, b \in Z$  since terms of degree  $\geq 2$  can be reduced. Thus  $Z[x]/I = \{ax + b + I\}$ . Notice that

$$(ax + b + I)(cx + d + I) = acx^2 + (ad + bc)x + bd + I = (ad + bc)x + bd - ac + I.$$

This is exactly how complex numbers  $ai + b$  multiply. Similarly for addition. Thus the map taking  $a + bi$  to  $a + bx + I$  gives an isomorphism between  $Z[i]$  and  $Z[x]/I$ . We know  $Z[i]$  is an integral domain but not a field. Thus  $I$  is prime but not maximal.