

Reading: §§4.4, 5.1, 5.2.

*Very early in our mathematical education – in fact in junior high school or in high school itself – we are introduced to polynomials. For a seemingly endless amount of time we are drilled, to the point of utter boredom, in factoring them, multiplying them, dividing them, simplifying them. Facility in factoring a quadratic becomes confused with genuine mathematical talent.* I. Herstein

1. (Quadratic roots)

a) There are two roots of  $T^2 + 3T + 1$  in  $\mathbf{R}$ :  $(-3 \pm \sqrt{5})/2$ . Let  $\alpha = (-3 + \sqrt{5})/2$ . For rational  $a$  and  $b$ , write

$$\frac{1}{a + b\alpha} = a' + b'\alpha$$

for some rational  $a'$  and  $b'$  in terms of  $a$  and  $b$ . Notice  $\alpha$  is not a pure square root (like  $\sqrt{5}$ ), so  $(a + b\alpha)(a - b\alpha) = a^2 - b^2\alpha^2$  is *not* generally rational. (Hint: Write  $a + b\alpha$  in the form  $x + y\sqrt{5}$  by writing  $\alpha$  in  $a + b\alpha$  as  $\frac{-3 + \sqrt{5}}{2}$  and collecting like terms, invert  $x + y\sqrt{5}$ , and then write the answer in the form  $a' + b'\alpha$  by writing  $\sqrt{5}$  as  $2\alpha + 3$  and collecting like terms.)

b) Let  $F$  be a field and  $Q(T) = T^2 + c_1T + c_0$  be an irreducible quadratic in  $F[T]$ . We know there is a field  $E \supset F$  in which  $Q(T)$  has a root, say  $\alpha$ . Show  $\beta := -c_1 - \alpha$  is also a root by directly computing that  $Q(-c_1 - \alpha) = 0$ . Then show

$$F[\alpha] := \{a + b\alpha : a, b \in F\}$$

is closed under multiplication and write an *explicit* inverse formula

$$\frac{1}{a + b\alpha} = a' + b'\alpha$$

in  $F[\alpha]$ , where  $a'$  and  $b'$  in  $F$  depend on  $a$  and  $b$ , so  $F[\alpha]$  is a field. Finally, show the function  $\sigma: F[\alpha] \rightarrow F[\alpha]$  given by  $\sigma(a + b\alpha) = a + b\beta$ , which replaces  $\alpha$  with  $\beta$ , is a field homomorphism and  $\sigma(\sigma(x)) = x$  for all  $x$  in  $F[\alpha]$ . (Note: To show  $\sigma$  is multiplicative you need to have shown first that  $F[\alpha]$  is closed under multiplication.)

2. The polynomial  $T^3 + T + 1$  is irreducible in  $\mathbf{F}_2[T]$ . Let  $\alpha$  be a root of  $T^3 + T + 1$  in some field extension of  $\mathbf{F}_2$ , so  $\alpha^3 + \alpha + 1 = 0$ .

a) Find the other roots of  $T^3 + T + 1$  in the ring  $\mathbf{F}_2[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbf{F}_2\}$  by explicitly substituting the 8 elements of  $\mathbf{F}_2[\alpha]$  into  $T^3 + T + 1$  and seeing when you get the value 0.

b) The polynomial  $T^3 + T^2 + 1$  is irreducible in  $\mathbf{F}_2[T]$ . What are its roots in  $\mathbf{F}_2[\alpha]$ ? (Note  $\alpha$  is *not* a root of this, so you don't have any roots of the polynomial to start off with.)

3. (Irreducibility tests)

a) Use reduction mod  $p$  or the Eisenstein criterion to show each of the following three polynomials is irreducible in  $\mathbf{Q}[T]$ :

$$T^4 + 3T^3 + 6T^2 - 9, \quad T^4 - T^3 + 17T^2 - 101T + 9, \quad T^5 - 6T + 12.$$

b) Show  $f(T) = T^4 - 10T^2 + 1$  has no Eisenstein translate: for no  $c \in \mathbf{Z}$  is  $f(T + c)$  an Eisenstein polynomial with respect to a prime number.

4. Let  $F$  be a field and  $E$  be an extension field. For  $f(T)$  and  $g(T)$  in  $F[T]$ , show  $f|g$  in  $F[T]$  if and only if  $f|g$  in  $E[T]$ . (The interesting direction is  $\Leftarrow$ , since a weaker condition seems to imply a stronger one. For that, use uniqueness of quotient and remainder in the division theorem for polynomials, comparing  $F[T]$  with  $E[T]$ .)
5. Determine which of the following functions are ring homomorphisms:
- a)  $\varphi: \mathbf{Z}[i] \rightarrow \mathbf{F}_3[T]/(T^2 + 1)$  by  $\varphi(a + bi) = \bar{a} + \bar{b}T \pmod{T^2 + 1}$ ,
  - b)  $\varphi: \mathbf{Z} \rightarrow \mathbf{Z}$  by  $\varphi(a) = 3a$ ,
  - c)  $\varphi: \mathbf{Q}[T] \rightarrow \mathbf{R}$  by  $\varphi(f(T)) = f(\sqrt{5})$ ,
  - d)  $\varphi: \mathbf{Q}[T] \rightarrow \mathbf{Q}[T]$  by  $\varphi(f(T)) = f(T^2)$ ,
  - e)  $\varphi: \mathbf{F}_2[T] \rightarrow \mathbf{F}_2[T]$  by  $\varphi(f(T)) = f(T)^2$ ,
  - f)  $\varphi: \mathbf{F}_3[T] \rightarrow \mathbf{F}_3[T]$  by  $\varphi(f(T)) = f(T)^2$ .