

Let's explore the connection between extension fields and quotient rings. We have seen that  $F[x]/\langle p(x) \rangle \cong F(\alpha)$ , where  $\alpha$  is a root of its minimal polynomial  $p(x)$ . The goal of this activity is to see how working in quotient rings help us realize  $E = F(\alpha)$  as a field.

We will start easy. For now, let  $E = \mathbb{Q}(\sqrt{2})$ .

1. What quotient ring is  $E$  isomorphic to?
  
  
  
  
  
  
  
  
  
  
2. One element in  $E$  is  $1 + 3\sqrt{2}$ . What element in the quotient ring does this correspond to?
  
  
  
  
  
  
  
  
  
  
3. What will  $\gcd(3x + 1, x^2 - 2)$  be? How do you know? Then verify you are correct using the Euclidean algorithm.

4. Bezout's identity says that for any polynomials  $a(x)$  and  $b(x)$ , there are polynomials  $s(x)$  and  $t(x)$  such that

$$\gcd(a(x), b(x)) = s(x)a(x) + t(x)b(x).$$

Find  $s(x)$  and  $t(x)$  in our case, by working backwards from the Euclidean algorithm above.

5. What does Bezout's identity have to do with the expression

$$1 + \langle x^2 - 2 \rangle = (3x + 1 + \langle x^2 - 2 \rangle)(t(x) + \langle x^2 - 2 \rangle)$$

and what does this have to do with finding inverses? In particular, what is  $(1 + 3\sqrt{2})^{-1}$  in  $E$ ?

6. Now let's try this again with a more complicated polynomial. As in the earlier activity, take  $p(x) = x^3 + 3x^2 - x + 2$  and let  $\varrho$  be a root. Use quotient rings to find the inverse of the element  $2 + 3\varrho^2$  in  $E = \mathbb{Q}(\varrho)$ .