

## SIMUW Theory of Equations: Quadratic extensions

A field  $F$  is called an extension of another field  $K$  if  $F$  contains  $K$  and the operations on  $F$  extend those on  $K$  (in other words, the sum or product in  $F$  of two elements of  $K$  are the same as the sum or product in  $K$ ). We also call  $K$  a subfield of  $F$ .

Every field is a subfield of itself, and there are many more interesting examples:  $\mathbb{R}$  is a subfield of  $\mathbb{C}$ , and  $\mathbb{Q}$  is a subfield of both  $\mathbb{R}$  and  $\mathbb{C}$ .

The simplest case is a quadratic extension. Suppose  $F$  contains an element  $\alpha$  such that  $\alpha^2 \in K$  but  $\alpha \notin K$ , and every element of  $F$  can be written as  $x + y\alpha$  with  $x, y \in K$ . Then  $F$  is called a quadratic extension of  $K$ . For example,  $\mathbb{C}$  is a quadratic extension of  $\mathbb{R}$ . (There's a slightly more general notion of quadratic extension, but we won't need it.)

We write  $F = K(\alpha)$  (" $F$  equals  $K$  adjoin  $\alpha$ "). I should insert a warning that " $K(\alpha)$ " has a meaning even for other sorts of extensions (where  $\alpha^2 \notin K$ ), but it's a little more subtle, and the meaning is generally not the set of all  $x + y\alpha$  with  $x, y \in K$ .

1. Prove that if  $x + y\alpha = w + z\alpha$  with  $x, y, w, z \in K$  and  $\alpha \notin K$ , then  $x = w$  and  $y = z$ .
2. Suppose  $F$  is any extension of  $K$  (not necessarily quadratic), and that  $\alpha \in F$  with  $\alpha^2 \in K$  but  $\alpha \notin K$ . Define

$$L = \{x + y\alpha : x, y \in K\}.$$

Prove that  $L$  is a field (with the field operations that come from  $F$ ). Pay particularly close attention to multiplicative inverses.

Suppose we have a quadratic extension  $F$  of  $K$  as above. We define the conjugate of  $x + y\alpha$  to be

$$\overline{x + y\alpha} = x - y\alpha.$$

This notation could be confusing, since it looks like the complex conjugate, but it's standard notation.

1. Prove that if  $K$  does not have characteristic 2, then a number  $z \in F$  is in  $K$  iff  $z = \bar{z}$ . (What goes wrong in characteristic 2?)
2. Prove that if  $z$  and  $w$  are elements of  $F$ , then  $\overline{z + w} = \bar{z} + \bar{w}$  and  $\overline{zw} = \bar{z} \cdot \bar{w}$ .
3. If  $p(z)$  is a polynomial with coefficients in  $K$ , then  $\overline{p(z)} = p(\bar{z})$  for all  $z \in F$ .
4. If  $p(z)$  is a polynomial with coefficients in  $K$ , and if  $z_0$  is a root of  $p(z)$ , then so is  $\bar{z}_0$ .
5. If  $p(z)$  is a cubic polynomial with coefficients in  $F$ , and it has two roots in  $F$ , then it has a third root in  $F$ . (This is just a problem about fields, not quadratic extensions specifically.)
6. If  $K$  does not have characteristic 2,  $p(z)$  is a cubic polynomial with coefficients in  $K$ , and  $p(z)$  has a root in  $F$ , then it has a root in  $K$ . What about quadratic polynomials? Fourth degree? Fifth degree?