

For example, if  $d \geq 2$  is square-free, then the map  $c: \mathbb{Q}(\sqrt{d}) \rightarrow \mathbb{Q}(\sqrt{d})$  given by

$$c(a + b\sqrt{d}) = a - b\sqrt{d}$$

is an automorphism of  $\mathbb{Q}(\sqrt{d})$ , and  $\text{Fix}(c) = \mathbb{Q}$ .

If  $K$  is a field, we have the ring homomorphism  $h: \mathbb{Z} \rightarrow K$  given by  $h(n) = n \cdot 1$ . If  $h$  is injective, then  $K$  contains a copy of  $\mathbb{Z}$ , and since it is a field, it contains a copy of  $\mathbb{Q}$ . In this case, we say that  $K$  has *characteristic 0*. If  $h$  is not injective, then  $h(\mathbb{Z})$  is a subring of  $K$ , and thus an integral domain, the kernel of  $h$  is a subgroup of  $\mathbb{Z}$ , which by Proposition 2.15 must be of the form  $p\mathbb{Z}$  for some  $p \geq 1$ . By the first isomorphism theorem,  $h(\mathbb{Z})$  is isomorphic to  $\mathbb{Z}/p\mathbb{Z}$  for some  $p \geq 1$ . But then,  $p$  must be prime since  $\mathbb{Z}/p\mathbb{Z}$  is an integral domain iff it is a field iff  $p$  is prime. The prime  $p$  is called the *characteristic* of  $K$ , and we also say that  $K$  is of *finite characteristic*.

**Definition 2.28.** If  $K$  is a field, then either

- (1)  $n \cdot 1 \neq 0$  for all integer  $n \geq 1$ , in which case we say that  $K$  has *characteristic 0*, or
- (2) There is some smallest prime number  $p$  such that  $p \cdot 1 = 0$  called the *characteristic* of  $K$ , and we say  $K$  is of *finite characteristic*.

A field  $K$  of characteristic 0 contains a copy of  $\mathbb{Q}$ , thus is infinite. As we will see in Section 8.10, a finite field has nonzero characteristic  $p$ . However, there are infinite fields of nonzero characteristic.