

**Example 1.**  $\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\sqrt{2})) \cong \mathbf{Z}/2\mathbf{Z}$ .

*Sol.*: An automorphism  $\phi \in \text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\sqrt{2}))$  is completely determined once we fix the image of  $\sqrt{2}$ . The choice  $\phi(\sqrt{2}) = \sqrt{2}$  determines the identity element; the choice  $\phi(\sqrt{2}) = -\sqrt{2}$  determines the homomorphism

$$\phi: \mathbf{Q}(\sqrt{2}) \rightarrow \mathbf{Q}(\sqrt{2}), \quad \phi(m + \sqrt{2}n) = m - \sqrt{2}n. \quad (1)$$

Since  $\mathbf{Q}(\sqrt{2})$  is a finite degree extension of  $\mathbf{Q}$ , a  $\mathbf{Q}$ -homomorphism is also an isomorphism: it is injective because it is a field homomorphism; it is surjective because it is an injective  $\mathbf{Q}$ -linear map of a finite dimensional vector space into itself.

*Excercise.*

(a) Verify that  $\phi$  defined in (1) is a field homomorphism:

$$\phi((a + \sqrt{2}b)(c + \sqrt{2}d)) = \phi((a + \sqrt{2}b))\phi((c + \sqrt{2}d)), \quad \forall a, b, c, d \in \mathbf{Q}$$

(b) Verify that  $\phi \circ \phi = \text{Id}$ .

**Example 2.**  $\text{Aut}_{\mathbf{R}}(\mathbf{C}) \cong \mathbf{Z}/2\mathbf{Z}$ .

*Sol.*: An automorphism  $\phi \in \text{Aut}_{\mathbf{R}}(\mathbf{C})$  is completely determined once we fix the image of  $i$ . The choice  $\phi(i) = i$  determines the identity element; the choice  $\phi(i) = -i$  determines the homomorphism

$$\phi: \mathbf{C} \rightarrow \mathbf{C}, \quad \phi(x + iy) = x - iy, \quad (2)$$

which is the usual complex conjugation  $z \mapsto \bar{z}$ ,  $z = x + iy$ . Since  $\mathbf{C}$  is a finite degree extension of  $\mathbf{R}$ , then  $\phi$  is an isomorphism.

*Excercise.*

(a) Verify that  $\phi$  defined in (2) is a field homomorphism:

$$\phi((a + ib)(c + id)) = \phi((a + ib))\phi((c + id)), \quad \forall a, b, c, d \in \mathbf{R}$$

(b) Verify that  $\phi \circ \phi = \text{Id}$ .

**Example 3.** Let  $\xi$  be a primitive  $5^{\text{th}}$ -root of 1. Then  $\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi)) \cong \mathbf{Z}/5\mathbf{Z}^* \cong \mathbf{Z}/4\mathbf{Z}$ .

*Sol.*: As  $\mathbf{Q}(\xi)$  is a finite extension of  $\mathbf{Q}$ , we have

$$\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi)) = \text{Hom}_{\mathbf{Q}}(\mathbf{Q}(\xi), \mathbf{Q}(\xi)),$$

and the above set is in 1-1 correspondence with

$$Z(x^4 + x^3 + x^2 + x + 1) \cap \mathbf{Q}(\xi) = \{\xi, \xi^2, \xi^3, \xi^4\},$$

the zeroes of  $x^4 + x^3 + x^2 + x + 1$  contained in  $\mathbf{Q}(\xi)$ . Hence there are four automorphisms in  $\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$ , each determined by the image of  $\xi$ :

$$\phi_i(\xi) = \xi^i, \quad i = 1, \dots, 4.$$

This determines an isomorphism  $\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi)) \rightarrow \mathbf{Z}/5\mathbf{Z}^*$ ,  $\phi_i \mapsto i$ .

**Remark.** Note that  $\mathbf{Q}(\xi)$  is the splitting field of the polynomial  $f(x) = x^4 + x^3 + x^2 + x + 1$ . So, in principle,  $\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$  is a subgroup of  $S_4$ , the permutation group of 4 elements. In this case, the zeroes of  $f$  are very special, and  $\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi))$  is a much smaller subgroup than  $S_4$ .

**Remark.** In general, let  $\xi$  be a primitive  $n^{\text{th}}$ -root of 1. Then  $\text{Aut}_{\mathbf{Q}}(\mathbf{Q}(\xi)) \cong \mathbf{Z}/n\mathbf{Z}^*$ .

*Excercise.* Fix  $\xi = e^{2\pi i/5}$ . Verify that the automorphism determined by the condition  $\phi(\xi) = \xi^2$  has order 4, that is  $\phi \circ \phi \circ \phi \circ \phi = \text{Id}$ .