

**FALL 2005 #6**

Construct a Galois extension  $F$  of the field  $\mathbb{Q}$  of rational numbers with Galois group  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  and determine explicitly a primitive element for  $F$ . (Hint: Look for a subfield of a cyclotomic field, i. e., a field obtained by adjoining a root of unity.)

*Solution:* Throughout, let  $\zeta_n$  denote a primitive  $n$ th root of unity. Note that the cyclotomic extensions  $\mathbb{Q}(\zeta_7)$  and  $\mathbb{Q}(\zeta_9)$  are Galois extensions of  $\mathbb{Q}$ , each with Galois group isomorphic to  $\mathbb{Z}/6\mathbb{Z}$ . The converse for Lagrange's theorem holds for abelian groups, and every subgroup of an abelian group is normal. Thus, by the Fundamental Theorem of Galois Theory, there exist intermediate Galois extensions  $E_1$  and  $E_2$  of  $\mathbb{Q}$ , with  $E_1 \subseteq \mathbb{Q}(\zeta_7)$  and  $E_2 \subseteq \mathbb{Q}(\zeta_9)$ , such that  $[E_1 : \mathbb{Q}] = [E_2 : \mathbb{Q}] = 3$ . In particular, we may take  $E_1 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  and  $E_2 = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ . It follows that these extensions  $E_1$  and  $E_2$  each have Galois group isomorphic to  $\mathbb{Z}/3\mathbb{Z}$  over  $\mathbb{Q}$ .

Since 7 and 9 are relatively prime, it follows that  $\mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\zeta_9) = \mathbb{Q}$ . Hence,  $\mathbb{Q} \subseteq E_1 \cap E_2 \subseteq \mathbb{Q}(\zeta_7) \cap \mathbb{Q}(\zeta_9) = \mathbb{Q}$ . Consequently, the composite field  $F = E_1 E_2$  is a Galois extension of  $\mathbb{Q}$  having Galois group  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . [Here, we are using the fact that if  $E_1$  and  $E_2$  are Galois extensions of a field  $K = E_1 \cap E_2$ , then the composite field  $E_1 E_2$  is a Galois extension of  $K$  having Galois group isomorphic to the direct product of the Galois groups of  $E_1$  and  $E_2$  over  $K$ . See, for example, Dummit and Foote *Abstract Algebra* (2nd edition) page 574.]

Note that  $F = E_1 E_2 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_9 + \zeta_9^{-1})$ . Since  $F$  is a finite dimensional extension of  $\mathbb{Q}$  (a field of characteristic zero), it follows that  $F$  is a simple extension of  $\mathbb{Q}$ . So there must exist a primitive element which generates  $F$  over  $\mathbb{Q}$ . One such primitive element is  $\zeta_7 + \zeta_7^{-1} + \zeta_9 + \zeta_9^{-1}$ .

□