

---

620-321 Algebra, Semester 1, 2008  
**Answers to Problem Sheet 10**

---

2. 2, 6, 4
3. There is only the identity automorphism.
5. Galois group is  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .
7. We know  $[K : F] = [K : F(u)][F(u) : F]$ . Since  $u \notin F$  we know  $[F(u) : F] > 1$ . Therefore, since  $[K : F]$  is prime  $[K : F(u)] = 1$  and hence  $K = F(u)$ .
8. We know  $[F(u, v) : F] = [F(u, v) : F(u)][F(u) : F] = [F(u, v) : F(u)] \times \deg(p(x))$  and  $[F(u, v) : F] = [F(u, v) : F(v)][F(v) : F] = [F(u, v) : F(v)] \times \deg(q(x))$ . But clearly  $[F(u, v) : F(u)] \leq \deg(q(x))$  and  $[F(u, v) : F(v)] \leq \deg(p(x))$ , so  $[F(u, v) : F] \leq \deg(p(x)) \times \deg(q(x))$ . Since the degrees are co-prime and each divides  $[F(u, v) : F]$  we must have  $[F(u, v) : F] = \deg(p(x)) \times \deg(q(x))$ .
9. For any element  $u \in K \setminus \mathbb{Q}$  we must have  $[\mathbb{Q}(u) : \mathbb{Q}] = 2$  and so  $K = \mathbb{Q}(u)$ . Fix such an element  $u_0$ . The minimal polynomial of  $u_0$  must be quadratic and after clearing denominators will have the form  $ax^2 + bx + c \in \mathbb{Z}[x]$ . The quadratic formula shows  $\mathbb{Q}(u_0) = \mathbb{Q}(\sqrt{b^2 - 4ac})$ . Since  $u_0 \notin \mathbb{Q}$ , we know  $b^2 - 4ac$  is not a square, so  $b^2 - 4ac = e^2d$  where  $d$  is a square free integer. Then  $K = \mathbb{Q}(u_0) = \mathbb{Q}(\sqrt{d})$  as required.
10. Both polynomials are irreducible by Eisenstein, for instance. The quadratic formula shows both splitting fields are  $\mathbb{Q}(\sqrt{3})$ .
11. (a) The dimension is 6 and the field is  $\mathbb{Q}(\omega, 2^{\frac{1}{3}})$  where  $\omega = e^{2\pi i/3}$ .  
(b) The dimension is 4 and the field is  $\mathbb{Q}(\sqrt{5}, i)$ .
12. Observe that  $f(x) = x^3 + x + 1$  is irreducible over  $\mathbb{Z}_2$  since it has degree 3 but no root. Let  $K = \mathbb{Z}_2[x]/(f(x))$ . Let  $u = x + (f(x))$  be the coset of  $x$  in this quotient, so  $u$  is a root of  $f(x)$  in  $K$ . Now  $a \mapsto a^2$  is an isomorphism of  $K$  (see problem sheet 9, question 5) leaving  $\mathbb{Z}_2$  fixed. If  $u^2 = u$  then  $x^2 - x \in (f(x))$  which is impossible. Thus  $u^2 \neq u$  and we have two different roots of  $f(x)$ . Thus, since  $f(x)$  has degree 3, it must split into linear factors in  $K[x]$ . Since  $K = \mathbb{Z}_2(u)$ ,  $K$  is a splitting field of  $f(x)$  over  $\mathbb{Z}_2$ . The dimension is  $[K : \mathbb{Z}_2] = \deg(u, \mathbb{Z}_2) = 3$ .
13. The minimal polynomial of  $5^{\frac{1}{3}}$  over  $\mathbb{Q}$  is  $x^3 - 5$ . If  $\sigma \in G(\mathbb{Q}(5^{\frac{1}{3}})/\mathbb{Q})$  then  $\sigma$  must permute the roots of  $x^3 - 5$ . But  $5^{\frac{1}{3}}$  is the only root in  $\mathbb{Q}(5^{\frac{1}{3}})$ , so  $\sigma$  fixes  $5^{\frac{1}{3}}$  and thus  $\sigma = 1$ . The Galois group  $G(\mathbb{Q}(5^{\frac{1}{3}})/\mathbb{Q})$  is the trivial group. Hence, since  $[\mathbb{Q}(5^{\frac{1}{3}}) : \mathbb{Q}] = 3$ ,  $\mathbb{Q}(5^{\frac{1}{3}})$  is not a Galois extension, and so is not the splitting field of any polynomial over  $\mathbb{Q}$ .