

## HW 8

14.2

(12) Using the quadratic formula, we find the roots are  $\pm\sqrt{7\pm\sqrt{40}}$ .

Let  $\alpha = \sqrt{7+\sqrt{40}}$  and  $\beta = \sqrt{7-\sqrt{40}}$ . Then the roots are  $\pm\alpha, \pm\beta$ .

Since  $\frac{\alpha}{\beta} = 3$ , the splitting field is  $\mathbb{Q}(\alpha)$ . The Galois group thus has order 4, so is either  $\mathbb{Z}_4$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . Let's show it's not  $\mathbb{Z}_4$ .

The automorphism  $\alpha \mapsto -\alpha, \beta \mapsto -\beta$  has order 2. So it suffices to show that any other nonidentity automorphism doesn't have order 4. The Galois group is transitive on the roots so there's an automorphism taking  $\alpha \mapsto \beta$ .

The Galois group has order 4 and is transitive on the roots so there is a unique automorphism taking  $\beta \mapsto -\beta$ , namely the automorphism of order 2 above.

So the automorphism  $\alpha \mapsto \beta$  can't take  $\beta$  to  $-\beta$ . Also,  $\beta$  doesn't go to  $\alpha$ .  $\beta$  can't go to  $-\alpha$  since the automorphism wouldn't preserve the relation  $\alpha\beta = 3$ . Thus  $\beta \mapsto \alpha$ , so the automorphism has order 2. Therefore, the Galois group is  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

14.3

(8) If  $\alpha$  is a root of  $x^p - x - a$ , then  $(\alpha+1)^p - (\alpha+1) - a$

$= \alpha^p + 1^p - \alpha - 1 - a = \alpha^p - \alpha - a = 0$ , so  $\alpha+1$  is also a root. It

follows that the roots are  $\alpha, \alpha+1, \alpha+2, \dots, \alpha+p-1$  so the splitting field

is  $\mathbb{F}_p(\alpha)$ . Any automorphism  $\sigma$  taking  $\alpha$  to  $\alpha+c$  for some  $c \in \mathbb{F}_p^x$  has order

$p$  since  $\sigma^n(\alpha) = \alpha + nc$ . It follows that  $\alpha, \alpha+1, \dots, \alpha+p-1$  have the same

minimal polynomial (so that  $x^p - x - a$  is irreducible). Thus  $\mathbb{F}_p(\alpha)$  has degree  $p$  over

$\mathbb{F}_p$  so that  $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^p}$ . We've seen that any nonidentity element of the Galois group generates it, so the Galois group is  $\mathbb{Z}_p$ .

14,4

② Any automorphism of  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  over  $\mathbb{Q}$  is of the form  $\sqrt{2} \mapsto \pm\sqrt{2}$ ,  $\sqrt{3} \mapsto \pm\sqrt{3}$ ,  $\sqrt{5} \mapsto \pm\sqrt{5}$ . So  $\sqrt{2} + \sqrt{3} + \sqrt{5}$  isn't fixed by any nonidentity automorphism of  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ , so by the Fundamental Theorem of Galois Theory, the subfield  $\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$  must be the whole field  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ .