

## MATH 101A: HOMEWORK

### 9. ANSWERS TO HOMEWORK 9

9.1. (p. 320, #1 (b),(c),(d)) Find the Galois group of the polynomial

$$p(X) = X^3 - 10$$

over the fields: (b)  $\mathbb{Q}$ , (c)  $\mathbb{Q}(\sqrt{2})$ , (d)  $\mathbb{Q}(\sqrt{-3})$

$p(X)$  is irreducible over  $\mathbb{Q}$  by Eisenstein. Being a cubic, its roots do not lie in any quadratic extension. So  $p(X)$  is also irreducible over  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt{-3})$ . This implies that, in all three cases, the Galois group is either  $S_3$  or  $A_3$ .

Most students used the criterion that the Galois group is  $A_3 \cong \mathbb{Z}/3$  if and only if the discriminant is a square in the ground field. But  $\Delta = -2700 = -3(30^2) < 0$ . So, it is not a square in the real fields  $\mathbb{Q}$  or  $\mathbb{Q}(\sqrt{2})$ . It is a square in  $\mathbb{Q}(\sqrt{-3})$ . So, the answer is  $S_3, S_3, A_3$ .

Some students went further to try to find the elements of the Galois group:  $\tau =$  complex conjugation is an element of order 2 in the Galois groups  $Gal(L/\mathbb{Q})$  and  $Gal(LK/K)$  where  $K = \mathbb{Q}(\sqrt{2})$ .

$\mathbb{Q}(\sqrt{-3})$  contains the third root of unity:

$$\zeta = \frac{-1 + \sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3}).$$

So,  $E = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta)$ . If  $\alpha$  is the real cube root of 10 then the other two roots of the polynomial  $p(X)$  are the complex numbers  $\alpha\zeta$  and  $\alpha\zeta^2$ . This implies that the splitting field of  $p(X)$  is  $L = \mathbb{Q}(\alpha, \zeta)$  and it contains  $E$ .

Since  $Gal(L/E)$  acts transitively on the roots of  $p(X)$ , it contains an element  $\sigma$  so that  $\sigma(\alpha) = \alpha\zeta$ . Since  $Gal(L/E) \subseteq Gal(L/\mathbb{Q})$ ,  $\sigma$  is also an element of order 3 in  $Gal(L/\mathbb{Q}) = S_3$ . Since  $Gal(L/\mathbb{Q}) \cong Gal(LK/K)$ , the automorphism  $\sigma$  extends uniquely to an automorphism  $\bar{\sigma}$  of  $LK$  which fixes  $\sqrt{2}$ . So,  $Gal(L/\mathbb{Q}) = S_3 = \langle \sigma, \tau \rangle$ ,  $Gal(LK/K) = S_3 = \langle \bar{\sigma}, \tau \rangle$  and  $Gal(L/E) = A_3 = \langle \sigma \rangle$ .

**9.2.** (p. 254, #16) Let  $\text{char } K = p$ . Let  $\alpha$  be algebraic over  $K$ . Show that  $\alpha$  is separable if and only if  $K(\alpha) = K(\alpha^{p^n})$  for all positive integers  $n$ .

( $\Leftarrow$ ) Matt Graham gave the best explanation for this part: If  $\alpha$  is not separable over  $K$  then its irreducible polynomial  $f(X)$  has multiple roots. This happens if and only if it has a common factor with its derivative. Since  $f(X)$  is irreducible, this happens if and only if the powers of  $X$  which occur in  $f(X)$  are all multiples of  $p$ . I.e.,  $f(X) = g_1(X^p)$ . Since  $f$  is irreducible, so is  $g_1$ . If  $g_1$  has multiple roots then  $g_1(X^p) = g_2(X^{p^2})$ . This process cannot continue indefinitely since

$$\deg f > \deg g_1 > \deg g_2 > \dots$$

So, there is a maximal  $n$  for which  $f(X) = g_n(X^{p^n})$  and  $g_n$  does not have multiple roots. But  $\alpha$  is a root of  $f(X)$ . So,  $\alpha^{p^n}$  is a root of  $g_n$ . Since  $g_n$  does not have multiple roots,  $\alpha^{p^n}$  is separable over  $K$  and  $K(\alpha^{p^n})$  is a separable extension of  $K$ . If  $K(\alpha) = K(\alpha^{p^n})$  then  $\alpha$  is also separable (and  $n = 0$ ).

( $\Rightarrow$ ) Suppose by contradiction that  $\alpha$  is separable but  $K(\alpha) \neq K(\beta)$  where  $\beta = \alpha^{p^n}$ . Then  $\alpha$  is a root of the polynomial

$$g(X) = (X - \alpha)^{p^n} = X^{p^n} - \beta \in K(\beta)[X]$$

which has multiple roots. Let  $h(X) = \text{irr}(\alpha, K(\beta))$ . Then  $h(X)$  divides  $g(X)$  and therefore has multiple roots. This implies that  $f(X) = \text{irr}(\alpha, K)$  has multiple root since  $f(X)$  is a multiple of  $h(X)$  contradicting the assumption that  $\alpha$  is separable.

**9.3.** (p. 323, # 15) Let  $K/k$  be a Galois extension and let  $F$  be an intermediate field between  $k$  and  $K$ . Let  $H$  be the subgroup of  $\text{Gal}(K/k)$  mapping  $F$  into itself.

$$H = \{\sigma \in \text{Gal}(K/k) \mid \sigma(F) \subseteq F\}$$

Show that  $H$  is the normalizer of  $\text{Gal}(K/F)$  in  $\text{Gal}(K/k)$ .

Everyone got this. To show that  $H$  is contained in the normalizer of  $\text{Gal}(K/F)$ , suppose that  $\sigma \in H$  and  $\tau \in \text{Gal}(K/F)$ . Then we want to show that  $\sigma^{-1}\tau\sigma$  lies in  $\text{Gal}(K/F)$ . This is equivalent to saying that  $\sigma^{-1}\tau\sigma$  fixes  $F$  pointwise. So, let  $x \in F$ . Then  $\sigma(x) \in \sigma(F) \subseteq F$ . So,  $\tau(\sigma(x)) = \sigma(x)$  which implies  $\sigma^{-1}\tau\sigma(x) = x$  as claimed.

To show that  $H \supseteq N(\text{Gal}(K/F))$ , suppose that  $\sigma \in N(\text{Gal}(K/F))$ . Then I claim that  $\sigma(F) \subseteq F$  and therefore  $\sigma \in H$ . If not then there is some  $x \in F$  so that  $\sigma(x) \notin F$ . Since  $K$  is a Galois extension of  $k$  it is also a Galois extension of  $F$ . So, there is an element  $\tau \in \text{Gal}(K/F)$  so that  $\tau(\sigma(x)) \neq \sigma(x)$ . But then  $\sigma^{-1}\tau\sigma(x) \neq x$ . So,  $\sigma^{-1}\tau\sigma \notin \text{Gal}(K/F)$  which is a contradiction.