

7.5

$$x^9 - x = x(x+1)(x+2)(x^2+1)(x^2+x-1)(x^2-x-1)$$

7.7 Suppose  $K$  is a finite field, and that there exists a prime  $p$  and  $r \in \mathbb{N}$  such that  $|K| = p^r$ .

We must consider  $\pi = \prod_{k \in K^*} k$ . Note that for each element  $k \in K^*$  which doesn't satisfy  $x^2 - 1 = 0$  has a unique inverse other than itself. Therefore  $\prod_{k \in K^*, k^2 \neq 1} k = 1$ . Note that if we multiply the previous product by  $(-1)(1)$  we get  $\pi$ . Thus  $\pi = -1$ .

7.8 Let  $f(x) = x^3 + x + 1, g(x) = x^3 + x^2 + 1, f(\alpha) = 0, g(\beta) = 0, \mathbb{F}_2(\alpha) = K, \mathbb{F}_2(\beta) = L$ .

We want to construct  $\sigma : K \rightarrow L$  such that  $\sigma$  is an isomorphism. Note that

$$(\alpha + 1)^3 + (\alpha + 1)^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + 1 + 1 = \alpha^3 + \alpha + 1 = 0.$$

Therefore  $g(\alpha + 1) = 0$ , thus we know by the textbook that  $\sigma(\alpha + 1) = \beta$  is an isomorphism since  $\alpha + 1, \beta$  are both roots of the irreducible polynomial of  $g$ . Furthermore since both  $K, L$  are isomorphic to  $\mathbb{F}_8$  then we only need to ask the number of automorphisms of  $\mathbb{F}_8$ . If we consider the basis of  $\mathbb{F}_8$  to be  $(1, \alpha, \alpha^2)$ , then we just have the isomorphisms of (1) doing nothing, (2), multiplying by  $\alpha$  yielding  $(\alpha, \alpha^2, \alpha + 1)$ , and (3) multiplying by  $\alpha^2$  yielding  $(\alpha^2, \alpha + 1, \alpha^2 + \alpha)$ . Note that we must maintain at least one root, and since there are 3 roots, and that all cases are covered by swapping the roots which in turn swaps the other implies that there are 3 automorphisms.

Bonus Let  $P(x) = \prod_{i=1}^n (x - \alpha_i)$ . By the definition of the formal derivative we have by the product rule that  $P'(x) = \sum_{i=1}^n \prod_{j=1, j \neq i}^n (x - \alpha_j)$ . Note that  $P'(\alpha_i) = \prod_{j=1, j \neq i}^n (\alpha_i - \alpha_j)$ , since all of the other  $n-1$  terms in the series contain  $(x - \alpha_i)$ , thus going to 0. Therefore  $\prod_{i=1}^n P'(\alpha_i) = \prod_{i=1}^n \prod_{j=1, j \neq i}^n (\alpha_i - \alpha_j)$ . Note that the normal discriminant is strictly positive, therefore for each  $(\alpha_i - \alpha_j)$  there exists  $(\alpha_j - \alpha_i)$  with a negative sign. Since there are  $nC2 = \frac{n(n+1)}{2}$  pairings one must multiply by  $(-1)^{\frac{n(n+1)}{2}}$  to counteract the signs of the negative pairings. Note that additionally once the sign issue is taken care of that we now have paired every  $(\alpha_i - \alpha_j)$  with  $(\alpha_j - \alpha_i)$ , thus we have eliminated nearly half of the terms in the product therefore the formulation above is equivalent to  $\prod_{i < j}^n (\alpha_i - \alpha_j)^2$ .