

# PS3

Sasha Redden

February 3, 2026

1. Let  $p$  be a prime and let  $K$  be a field of characteristic  $p$ . Define a map  $Fr_K : K \rightarrow K$  by  $Fr_K(a) = a^p$ . It is called **Frobenius**.
  - (a) Prove that  $Fr_k = id_K$  if and only if  $K = \mathbb{F}_p$ .
  - (b) Prove that  $Fr_K$  is a field homomorphism.
  - (c) Suppose that  $K$  is finite. Prove that  $Fr_K$  is surjective.
  - (d) Give an example of a field  $K$  where  $Fr_K$  is not surjective.

(a)  $\implies$  :  $Fr_k = id_k$  then  $Fr_K(a) = a^p = a \forall a \in K$ . Consider  $f(x) = x^p - x$ , every element in  $K$  is a solution to this equation, and since  $deg(f(x)) = p$  there are at most  $p$  solutions in  $K$ , then  $|K| = p$  so  $K = \mathbb{F}_p$ .  
 $\impliedby$  :  $K = \mathbb{F}_p$ , then  $\forall a \in K$ ,  $Fr_K(a) = a^p = a$  thus  $Fr_k = id_K$ .

(b) Field hom:  $Fr_K(1) = 1$ ,  $Fr_K(0) = 0$  and for any  $a, b \in K$ ,  $Fr_K(a + b) = (a + b)^p = a^p + b^p = Fr_K(a) + Fr_K(b)$  because  $K$  has characteristic  $p$ , and  $Fr_K(ab) = (ab)^p = a^p b^p = Fr_K(a)Fr_K(b)$  so  $Fr_K$  is a field homomorphism.

(c)  $K$  is finite,  $Fr_K$  is a field homomorphism so it is injective, then  $|Fr_K(K)| = |K|$  so  $Fr_K$  is surjective.

(d)  $\mathbb{F}_p[x]$ ,  $\nexists a \in \mathbb{F}_p[x] : Fr_k(a) = x$ .
2. Let  $f \in K[x]$  be an irreducible inseparable polynomial. In class, we proved that this implies that  $f' = 0$ .
  - (a) Prove that there exists a prime  $p$  such that  $K$  has characteristic  $p$  and another polynomial  $g \in K[x]$  such that  $f(x) = g(x^p)$ .
  - (b) Suppose that  $Fr_K$  is surjective. Prove that no such  $f$  can exist.

(a) Since  $f(x) \in K[x]$  is irreducible and inseparable,  $K$  must have positive characteristic  $p$  such that  $p$  is prime. Since  $f'(x) = 0$  we have  $f(x) = g(x^p)$  (or  $f(x)$  is a constant and then  $f(x) = f(x^p)$ ) for some  $g(x) \in K[x]$  because then  $g'(x) = 0 = f'(x)$ .

- (b) Assume  $Fr_K$  is surjective, then for all  $b \in K, \exists a \in K$  such that  $Fr_K(a) = a^p = b$ , so for any irreducible inseparable polynomial  $f(x) \in K[x]$ , from a) there is a polynomial  $g(x) \in K[x]$  such that  $f(x) = g(x^p)$  but then  $f(a) \neq g(b) = g(a^p)$ , so no such  $f$  can exist.
3. A field  $K$  is called **perfect** if every irreducible polynomial in  $K[x]$  is separable.
- (a) Prove that every field of characteristic 0 is perfect. (Just repeat the argument from class.)
- (b) Prove that a field  $K$  of characteristic  $p$  is perfect if and only if  $Fr_K$  is surjective.
- (a) We know that if  $F$  has characteristic 0 then every irreducible polynomial in  $K[x]$  is separable, and thus  $K$  is perfect.
- (b) Let  $K$  be a perfect field. Let  $\alpha \in F$ , any field extension of  $K$  such that  $f(x) \in K[x]$  is the minimal polynomial of  $\alpha$ , then  $f(x)$  can be factored into distinct linear factors in  $F[x]$ ...
4. A field  $K$  is called **algebraically closed** if every polynomial  $f \in K[x]$  has a root in  $K$ .
- (a) Assume that  $K$  is algebraically closed. Prove that if  $F/K$  is an algebraic extension, then  $F = K$ .
- (b) Suppose that  $F/K$  is an algebraic extension and every polynomial in  $K[x]$  splits in  $F$ . Prove that  $F$  is algebraically closed.
- (a) Every polynomial  $f(x) \in K[x]$  has a root in  $K$ , and  $F/K$  is an algebraic extension, so every element of  $c \in F$  is algebraic over  $K$ , then  $\exists p(x) \in K[x] : p(c) = 0$ , and we can assume  $p(x) = m_c(x)$ , so  $c \in K$  and thus  $F = K$ .
- (b) Every element of  $c \in F$  is algebraic over  $K$ , i.e.  $\exists p(x) \in K[x] : p(c) = 0$  and every polynomial  $k(x) \in K[x]$  can be factored into linear factors in  $F[x]$  (all of the roots of  $k(x)$  lie in  $F$ ). Let  $f(x) \in F[x] \setminus K[x]$  be an arbitrary polynomial, then there exists  $k(x) \in K[x]$  such that  $f(x)|k(x)$  i.e.  $f(x)$  is a factor of  $k(x)$ , and all of the roots of  $k(x)$  lie in  $F$ , thus all of the roots of  $f(x)$  must also lie in  $F$ , so  $F$  is algebraically closed.
5. Let  $F/K$  be a normal extension. Let  $L$  be another field containing  $F$  (so we have  $K \subseteq F \subseteq L$ ). Let  $\phi : L \rightarrow L$  be an automorphism such that  $\phi|_K = id_K$ . Then  $\phi(F) = F$ .  
 Let  $f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$ , then  $\phi(f(x)) = a_0 + a_1\phi(x) + \dots + a_n\phi(x)^n = f(\phi(x))$ .  
 First show  $F \subseteq \phi(F)$ : let  $a \in F$  and let  $b \in L$  such that  $\phi(b) = a$ . Then let  $f(x) \in K[x]$  be such that  $f(a) = 0$ ,  $\phi(f(b)) = f(\phi(b)) = f(a) = 0$ , so  $b$  must be a root of  $f(x)$ , and since  $F/K$  is a normal extension, all of the roots of  $f(x)$  must be in  $F$ , thus  $b \in F$ . And since  $\phi(b) = a \in \phi(F)$ ,  $F \subseteq \phi(F)$ .  
 $\phi(F) \subseteq F$ : Let  $a \in F$ ,  $\phi(a) = b \in L$ , then consider  $f(x) \in K[x]$  such that  $f(a) = 0$ , then  $\phi(f(a)) = f(\phi(a)) = f(b) = 0$ , thus  $b \in F$  and  $\phi(F) \subseteq F$ .
6. Let  $F/L$  and  $L/K$  be field extensions. Prove or give a counterexample:
- (a) If  $F/K$  is normal, then  $F/L$  is normal.
- (b) If  $F/K$  is normal, then  $L/K$  is normal.
- (c) If  $F/L$  and  $L/K$  are normal, then  $F/K$  is normal.

- (a) Let  $p(x) \in L[x]$  be irreducible and let  $\alpha \in F$  be a root of  $p(x)$ . Let  $f(x)$  be the minimal polynomial of  $\alpha$  over  $K$ , then  $p(x) \mid f(x)$  and  $f(x)$  splits over  $F$ , thus  $p(x)$  splits over  $F$  so  $F/L$  is normal.
- (b) Consider  $K = \mathbb{Q} \subset L = \mathbb{Q}(\sqrt[4]{2}) \subset F = \mathbb{Q}(\sqrt[4]{2}, i)$ , then  $F/K$  is normal because  $F$  is the splitting field of  $f(x) = x^4 - 2 \in K[x]$ , but  $L/K$  is not normal because  $L$  has two roots of  $f(x)$ ,  $\pm\sqrt[4]{2}$ , but it does not contain all of the roots, thus  $f(x)$  does not split over  $L$ .
- (c) Let  $f(x) \in K[x] \subseteq L[x]$  such that  $f(c) = 0$  for some  $c \in L \subseteq F$ , then  $f(x)$  splits over  $L \subseteq F$ , then  $f(x)$  splits over  $F$ . Now consider  $f(c) = 0$  for  $c \in F \setminus L$ , then since  $f(x) \in L[x]$ ,  $f(x)$  splits over  $F$  so  $F/K$  is a normal extension.