

# Math 230B Final Exam

Joshua Hill

March 16, 2009

1) Show that the following polynomials are irreducible.

(a)  $X^6 + X^3 + 1$  over  $\mathbb{Q}$

Note that  $f(X + 1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$ , which is irreducible over  $\mathbb{Q}$  by the Eisenstein criterion (with  $p = 3$ ). If  $f(X)$  was not irreducible over  $\mathbb{Q}$ , then its factorization would produce a non-trivial factorization for  $f(X + 1)$ , which we have seen does not exist. Thus  $f(X)$  is irreducible.

(b)  $X^2 + Y^2 + 1$  over  $\mathbb{C}(Y)$

Let  $f(X) = X^2 + (Y^2 + 1) \in \mathbb{C}(Y)[X]$ .  $f(X)$  is degree 2 over  $X$ , so it is irreducible if and only if it has no linear divisors in  $\mathbb{C}(Y)[X]$ . Otherwise stated  $f(X)$  is reducible if and only if there exist  $\alpha_1, \alpha_2 \in \mathbb{C}(Y)$  such that  $f(X) = (X - \alpha_1)(X - \alpha_2) = X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2$ . As there is no  $X^1$  term in  $f(X)$ , we immediately see that  $\alpha_1 = -\alpha_2$ , thus  $f(X) = (X - \alpha_1)(X + \alpha_1) = X^2 - \alpha_1^2$ . As such,  $\alpha_1^2 = -(Y^2 + 1)$ . Thus  $f(X)$  is reducible if and only if there is an element  $\beta \in \mathbb{C}(Y)$  such that  $\beta^2 = Y^2 + 1$ .  $\beta = \frac{g(Y)}{h(Y)}$  where  $g, h \in \mathbb{C}[Y]$ , so  $\beta^2 = \frac{g(Y)^2}{h(Y)^2} = Y^2 + 1$  so  $g(Y)^2 = h(Y)^2(Y^2 + 1)$ . The existence of such an element finally hinges on the existence of an element  $\zeta(Y) \in \mathbb{C}[Y]$  such that  $\zeta(Y)^2 = Y^2 + 1$ . There is no such  $\zeta(X)$ . If there were, then  $\zeta(Y)$  would have to be degree 1, thus  $\zeta = (aY + b)$  for some  $a, b \in \mathbb{C}$  and  $\zeta^2 = (aY + b)^2 = a^2Y^2 + (a+b)Y + b^2 = Y^2 + 1$ , whence  $a = -b = 1$ , so  $\zeta(Y) = Y - 1$ , but  $\zeta(Y)^2$  would then be  $Y^2 - 2Y + 1$ , which is not  $Y^2 + 1$ . Thus, there is no such  $\zeta(Y)$ , so there is no such  $\beta$ , so there is no such  $\alpha_1$ , so  $f(X)$  is irreducible.

2) Compute the Galois groups of the following polynomials.

(a)  $f(X) = \underbrace{(X^2 - p_1)}_{f_1(X)} \cdots \underbrace{(X^2 - p_n)}_{f_n(X)}$  over  $\mathbb{Q}$  where  $p_i$ 's are distinct primes.

Each  $f_j(X)$  is irreducible over  $\mathbb{Q}$  by the Eisenstein criterion ( $p = p_j$ ). Each  $f_j(X) = (x - \sqrt{p_j})(x + \sqrt{p_j})$ , so  $f_j(X)$  is irreducible over any field that doesn't contain  $\sqrt{p_j}$  as an element. As each  $\sqrt{p_j}$  can not be represented using a product of other primes, we see that we have the extension tower

$$\begin{aligned} [\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] &= \underbrace{[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})]}_{\text{degree 2}} \cdots \underbrace{[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) : \mathbb{Q}(\sqrt{p_1})]}_{\text{degree 2}} \underbrace{[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}]}_{\text{degree 2}} \\ &= 2^n \\ &= |G_f| \end{aligned}$$

Each extension is normal (as each field extension is the splitting field for some number of the  $f_j(X)$ s), and separable (as the extension is over a field of characteristic 0) so each extension is Galois. Each  $f_j(X)$  has exactly 2 roots so  $G_f$  must contain  $n$  automorphisms fixing  $\mathbb{Q}$  that are the  $\mathbb{Q}$ -linear extension that maps one conjugate to the other ( $\psi(\sqrt{p_j}) = -\sqrt{p_j}$ ). As any selection of these automorphisms can be composed with each other (yielding a distinct automorphism also fixing  $\mathbb{Q}$ ), we have a total of

$2^n$  distinct automorphisms fixing  $\mathbb{Q}$ . This is the total number of automorphisms, so these are all of the automorphisms of  $G_f$ .

Now, as each automorphism is order 2 within  $G_f$ ,  $G_f \cong (\mathbb{Z}/2\mathbb{Z})^n$ .

(b)  $f(X) = X^5 - 4X + 2$  over  $\mathbb{Q}$ .

$f(X)$  is irreducible over  $\mathbb{Q}$  (by Eisenstein,  $p = 2$ ).  $f'(X) = 5X^4 - 4$ , so  $f'(X) = 0$  when  $X = \pm \sqrt[4]{\frac{4}{5}}$ . Using calculus to examine the behavior of this function over  $\mathbb{R}$ ,  $f(X)$  is increasing on  $(-\infty, -\sqrt[4]{\frac{4}{5}})$ , decreasing on  $(-\sqrt[4]{\frac{4}{5}}, \sqrt[4]{\frac{4}{5}})$ , and then increasing on  $(\sqrt[4]{\frac{4}{5}}, \infty)$ .  $f(-2) = -22$ ,  $f(-\sqrt[4]{\frac{4}{5}}) \approx 5.02 > 0$ ,  $f(\sqrt[4]{\frac{4}{5}}) \approx -1.03 < 0$ , and  $f(2) = 26$ . So  $f(X)$  has exactly 3 real roots (by the intermediate value theorem), one each in the intervals  $(-2, -\sqrt[4]{\frac{4}{5}})$ ,  $(-\sqrt[4]{\frac{4}{5}}, \sqrt[4]{\frac{4}{5}})$ , and  $(\sqrt[4]{\frac{4}{5}}, 2)$ .  $f'(X)$  shares none of these roots, so  $f(X)$  has no multiple roots. Thus,  $f(X)$  has exactly two complex roots.

$f(X)$  has degree 5 (so  $f(X)$  has prime degree), is over  $\mathbb{Q}$ , and has exactly two complex roots so by a theorem presented in Lang (example 6, page 273)  $G_f \cong S_5$ .

(c)  $f(X) = \frac{X^p-1}{X-1} - t$  over  $\mathbb{Q}(t)$ , where  $p$  is prime.

We will show that  $\frac{X^p-1}{X-1} = \Phi_p(X)$  is Morse, thus by a theorem of Hilbert  $G_f \cong S_{deg \Phi_p(X)} = S_{p-1}$ .

Claim:  $\Phi_p(X)$  is irreducible over  $\mathbb{Q}$ . This will proceed in a similar way as Lang's proof that the  $p$ -th cyclotomic polynomial is irreducible: we will apply Eisenstein's criterion (using the prime  $p$ ) to the shifted polynomial  $\Phi_p'(X+1)$ .

First, examine the two standard ways of representing the  $p$ th-cyclotomic polynomial

$$\begin{aligned}\Phi_p(X) &= X^{p-1} + X^{p-2} + \dots + X + 1 \\ &= \frac{X^p - 1}{X - 1}\end{aligned}$$

$$\begin{aligned}\Phi_p'(X) &= (p-1)X^{p-2} + (p-2)X^{p-3} + \dots + 1 \\ &= \frac{d}{dx} \left[ \frac{X^p - 1}{X - 1} \right] \\ &= \frac{pX^{p-1}(X-1) - (X^p - 1)}{(X-1)^2} \\ &= \frac{pX^{p-1} - \Phi_p(X)}{X-1}\end{aligned}$$

By plugging in  $X+1$  and expanding this last form we get:

$$\begin{aligned}\Phi_p'(X+1) &= \frac{p(X+1)^{p-1} - \Phi_p(X+1)}{(X+1) - 1} \\ &= \frac{p(X+1)^{p-1} - ((X+1)^{p-1} + (X+1)^{p-2} + \dots + (X+1) + 1)}{X} \\ &= \frac{p(X+1)^{p-1} - (X+1)^{p-1} - (X+1)^{p-2} - \dots - (X+1) - 1}{X}\end{aligned}$$

Applying the binomial theorem for each term we can quickly dispense with the constant terms: the first term contributes  $p$  and every one of the following  $p$  terms contribute a  $-1$ , so the constant terms cancel (which we knew a priori, as we know that this is a polynomial, not a rational expression!)

The non-constant terms are somewhat more of a chore. Examine the  $X^j$  term, where  $j \in \{1, 2, \dots, p-1\}$ . By the binomial theorem, the first term contributes a  $p\binom{p-1}{j}$  and then the  $k$ th term further right contributes  $-\binom{p-1-k}{j}$ . If  $p(x)$  is a polynomial, let  $p(x)|_{x^j}$  be the coefficient of the  $x^j$ th term of the polynomial.

$$\begin{aligned}
(X\Phi'_p(X+1))|_{x^j} &= \\
&= [p(X+1)^{p-1} - (X+1)^{p-1} - (X+1)^{p-2} - \dots - (X+1) - 1] |_{x^j} \\
&= p\binom{p-1}{j} - \binom{p-1}{j} - \binom{p-2}{j} - \dots - \binom{j}{j} \\
&= p\binom{p-1}{j} - \sum_{k=j}^{p-1} \binom{k}{j} \\
&= p\binom{p-1}{j} - \binom{p}{j+1}
\end{aligned}$$

The  $(p-1)$ st term is  $(p-1)$ , and  $p \nmid (p-1)$ .

$p$  does divide the  $j$ th term where  $j \in \{1, 2, \dots, p-2\}$ .

Finally, the 1st term (which is the constant term after division by  $X$ ) is  $(p)(p-1) - \frac{(p)(p-1)}{2}$ , so  $p$  divides this 1st term (as we had earlier observed) but  $p^2$  does not divide this 1st term. So, finally,  $\Phi'_p(X)$  is irreducible by the Eisenstein criterion (using  $p$ ).

Because  $\Phi'_p(X)$  is irreducible, and we are operating over a field of characteristic 0,  $\Phi'(X)$  is separable, thus has no repeated roots.

Claim: the roots of  $\Phi'(X)$  have distinct values in  $\Phi(X)$ .

Let  $\beta_1, \dots, \beta_{p-1}$  be the distinct roots of  $\Phi'(X)$ . Note that 1 is not one of these roots, as  $\Phi'_p(1) = (p-1) + (p-2) + \dots + 1 = \binom{p}{2} > 0$ .

Let  $\beta_i$  and  $\beta_j$  be arbitrary roots of  $\Phi'(X)$ .  $\Phi'(\beta_i) = \Phi'(\beta_j) = 0$ , so  $p\beta_i^{p-1} - \Phi_p(\beta_i) = p\beta_j^{p-1} - \Phi_p(\beta_j) = 0$ .

If  $\Phi_p(\beta_i) = \Phi_p(\beta_j)$ , then we have  $p\beta_i^{p-1} = p\beta_j^{p-1}$ , and thus  $\left(\frac{\beta_i}{\beta_j}\right)^{p-1} = 1$ . So, we have found that  $\frac{\beta_i}{\beta_j} = \xi$  (where  $\xi$  is a  $(p-1)$ th root of unity), and thus  $\beta_i = \beta_j\xi$ .

As we are operating under the assumption that  $\Phi_p(\beta_i) = \Phi_p(\beta_j)$ , by the above we additionally have  $\Phi_p(\beta_j\xi) = \Phi_p(\beta_j)$ , so it follows that

$$\Phi_p(\beta_j\xi) = \frac{(\beta_j\xi)^p - 1}{(\beta_j\xi) - 1} = \frac{(\beta_j)^p - 1}{(\beta_j) - 1} = \Phi_p(\beta_j)$$

Repeated manipulation of the middle terms gives us:

$$\begin{aligned}
\frac{(\beta_j \xi)^p - 1}{(\beta_j \xi) - 1} &= \frac{\beta_j^p - 1}{\beta_j - 1} \\
\frac{\beta_j^p \xi - 1}{(\beta_j \xi) - 1} &= \frac{\beta_j^p - 1}{\beta_j - 1} \\
(\beta_j^p \xi - 1)(\beta_j - 1) &= (\beta_j^p - 1)(\beta_j \xi - 1) \\
\beta_j^{p+1} \xi - \beta_j^p \xi - \beta_j + 1 &= \beta_j^{p+1} \xi - \beta_j^p - \beta_j \xi + 1 \\
\beta_j^p \xi + \beta_j &= \beta_j^p + \beta_j \xi \\
\beta_j^{p-1} \xi - \xi &= \beta_j^{p-1} - 1 \\
(\beta_j^{p-1} - 1)\xi &= \beta_j^{p-1} - 1
\end{aligned}$$

So, either  $\xi = 1$ , whence we have  $\beta_i = \beta_j$ , or  $\beta_j^{p-1} = 1$ .

Examining this second possibility for a moment, we quickly arrive at a contradiction. Recall that  $\beta_j \neq 1$ , so if  $\beta_j^{p-1} = 1$  (that is, if  $\beta_j$  is a  $(p-1)$ th root of unity), we find that

$$\Phi_p(\beta_j) = \frac{\beta_j^p - 1}{\beta_j - 1} = \frac{\beta_j - 1}{\beta_j - 1} = 1$$

and thus

$$\Phi'_p(\beta_j) = \frac{p\beta_j^{p-1} - \Phi_p(\beta_j)}{\beta_j - 1} = \frac{p-1}{\beta_j - 1} = 0$$

As  $\beta_j \neq 1$ , this implies that  $p = 1$ , a contradiction, as  $p$  was assumed to be prime. Thus  $\Phi_p(\beta_i) = \Phi_p(\beta_j)$  implies that  $\beta_i = \beta_j$ . Thus, the roots of  $\Phi'(X)$  have distinct values in  $\Phi(X)$ .

So,  $\Phi_p(X)$  is Morse, and as noted at the start, we have  $G_f \cong S_{deg \Phi_p(X)} = S_{p-1}$ .

- 3) Let  $F$  be a finite field, and let  $K$  be a finite extension of  $F$ . Show that both the norm map and the trace map from  $K$  to  $F$  are surjective. Is the same statement true if  $K$  and  $F$  are number fields?

For the finite field case, let  $p = \text{char}(F)$ ,  $q = |F|$ ,  $n$  such that  $q = p^n$ , and  $m = [K : F]$ .  $F = \mathbb{F}_q = \mathbb{F}_{p^n}$  and  $K = \mathbb{F}_{q^m} = \mathbb{F}_{p^{nm}}$ .

This extension  $K/F$  is always Galois, so the set of automorphisms fixing  $F$  is quite well behaved: in particular every automorphism fixing  $F$   $\sigma_j \in \text{Gal}(K/F)$  is of the form  $\sigma_j(\alpha) = \alpha^{q^j}$  where  $j \in \{0, 1, \dots, m-1\}$ .

Examining

$$\text{Tr}_{K/F}(\alpha) = \text{Tr}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{m-1}}$$

The Trace is  $F$ -linear, so  $\text{Tr}(0) = 0$ . To show that the rest of  $F$  is in the image of  $\text{Tr}$  requires only that we show that there is at least one  $\alpha \in K$  such that  $\text{Tr}(\alpha) \neq 0$ . We can then scale this element by any value in  $F$ , and can thus arrive at any value in  $F$ .

By the above formula for  $\text{Tr}(\alpha)$  it is clear that  $\text{Tr}(\alpha) = 0$  if and only if  $\alpha$  is a root of the polynomial  $X + X^q + X^{q^2} + \dots + X^{q^{m-1}}$ . This polynomial has at most  $q^{m-1}$  roots, but  $K$  has  $q^m$  values, so there must be some values in  $K$  that are not roots of the above polynomial, thus there are some values in  $F$  that have a non-zero trace. Thus Trace is onto.

Examining

$$N_{K/F}(\alpha) = N(\alpha) = \alpha \alpha^q \dots \alpha^{q^{m-1}} = \alpha^{1+q+q^2+\dots+q^{m-1}} = \alpha^{\frac{q^m-1}{q-1}}$$

$N(0) = 0$ . Further note that by construction,  $N(\alpha\beta) = N(\alpha)N(\beta)$  so  $N$  is a group homomorphism under multiplication.

There are at most  $\frac{q^m-1}{q-1}$  roots for  $N$ , so  $|\text{Ker}(N)| \leq \frac{q^m-1}{q-1}$ .  $N$  maps elements in  $K^*$  to  $F^*$ , as each automorphism has a trivial kernel.  $|\text{Im}(N)| = \frac{q^m-1}{|\text{Ker}(N)|}$  so  $|\text{Im}(N)| \geq \frac{q^m-1}{\frac{q^m-1}{q-1}} = q-1$ . Thus  $N$  maps  $K^*$  onto  $F^*$ , so  $N$  maps  $K$  onto  $F$ .

For the non-finite field case, again let  $m = [K : F]$ . The trace continues to be onto, due to the fact that it is a linear transformation. If  $\alpha \in F$   $Tr(\alpha) = m\alpha$ , so we can scale this to any value in  $F$ .

The norm isn't quite so well behaved. For an example, note that in  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ , the extension is order 2 so the only automorphisms fixing  $\mathbb{Q}$  are the identity and the automorphism such that  $\sigma(\sqrt{2}) = -\sqrt{2}$  extended by linearity. Thus, for  $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ,  $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 > 0$ , so any negative number is not in the image of the norm. Thus, the Norm operator is not onto in the non-finite field case.

- 4) Let  $\zeta_n$  be a primitive  $n$ -th root of unity, where  $n > 1$ . Let  $K = \mathbb{Q}(\zeta_n)$  be the  $n$ -th cyclotomic field. Show that the norm  $N_{K/\mathbb{Q}}(1 - \zeta_n)$  is  $p$  when  $n$  is a power of a prime  $p$ , and the norm  $N_{K/\mathbb{Q}}(1 - \zeta_n)$  is 1 is not a power of a prime.

In the case where  $n$  is a prime power, let  $r$  be such that  $n = p^r$ .

To examine the norm of  $N_{K/\mathbb{Q}}(1 - \zeta_n)$  we first find the minimal polynomial for this element, and use the fact that the norm of this element is simply the constant term of this polynomial (possibly with a sign change).

$\zeta_n$  is a primitive  $n$ th root of unity, so it is a root of  $\Phi_n(X)$ .  $\Phi_n(X)$  is irreducible, so  $\hat{\Phi}_n(X) = \Phi_n(1 - X)$  is similarly irreducible.  $\hat{\Phi}_n(1 - \zeta_n) = \Phi_n(1 - (1 - \zeta_n)) = \Phi_n(\zeta_n) = 0$ . As  $\hat{\Phi}_n(X)$  is irreducible and has  $1 - \zeta_n$  as a root,  $\hat{\Phi}_n(X)$  is the minimal polynomial for  $1 - \zeta_n$ .

$$\begin{aligned} \hat{\Phi}_n(X) &= \Phi_n(1 - X) = \Phi_{p^r}(1 - X) = \Phi_p((1 - X)^r) \\ &= ((1 - X)^r)^{p-1} + ((1 - X)^r)^{p-2} + \dots + ((1 - X)^r) + 1 \\ &= (1 - X)^{r(p-1)} + (1 - X)^{r(p-2)} + \dots + (1 - X)^r + 1 \end{aligned}$$

From the binomial theorem, we see that each term contributes 1 to the constant term. There are  $p$  terms total, so the constant term from the expanded polynomial is  $p$ . The degree of this polynomial is  $\varphi(n)$ , which is even (for  $n > 2$ ), so  $N_{K/\mathbb{Q}}(1 - \zeta_n) = (-1)^{\varphi(n)}p = p$ . For the case where  $n = 2$ ,  $\zeta_2 = -1$ , so  $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ , so the only automorphism fixing  $\mathbb{Q}$  is the identity, so  $N_{K/\mathbb{Q}}(1 + 1) = 2 = p$ .

In the instance where  $n$  is not a power of a prime, we perform induction on the number of distinct primes that divide  $n$ . The two prime case is our base case.

In the case where  $n = p_1^{r_1} p_2^{r_2}$

$$\begin{aligned} \Phi_{p_1^{r_1} p_2^{r_2}}(X) &= \Phi_{p_1 p_2}(X^{p_1^{r_1-1} p_2^{r_2-1}}) \\ &= \frac{\Phi_{p_2}\left(\left(X^{p_1^{r_1-1} p_2^{r_2-1}}\right)^{p_1}\right)}{\Phi_{p_2}\left(X^{p_1^{r_1-1} p_2^{r_2-1}}\right)} \\ &= \frac{\Phi_{p_2}\left(X^{p_1^{r_1} p_2^{r_2-1}}\right)}{\Phi_{p_2}\left(X^{p_1^{r_1-1} p_2^{r_2-1}}\right)} \end{aligned}$$

We are (sadly) interested in  $\Phi_n(1 - X)$ . Happily, we can restrict our analysis to the constant term of  $\Phi_{p_2}(1 - X)$ . There are  $p_2$  terms in  $\Phi_{p_2}(1 - X)$  (and thus in  $\Phi_{p_2}((1 - X)^{p_1^{r_1} p_2^{r_2 - 1}})$  and  $\Phi_{p_2}((1 - X)^{p_1^{r_1 - 1} p_2^{r_2 - 1}})$ ). By the binomial theorem, each one will contribute 1, so the constant term for both the numerator and denominator is  $p_2$ .

Interpreting the above equality as a statement about norms, we see that the constant term for  $\Phi_{p_1^{r_1} p_2^{r_2}}(X)$  is an integer such that when it is multiplied by  $p_2$  the result is  $p_2$ . Thus, the constant term for  $\Phi_{p_1^{r_1} p_2^{r_2}}(X)$  is 1, and  $N_{K/\mathbb{Q}}(1 - \zeta_n) = (-1)^{\varphi(n)} 1 = 1$ .

So, the base case is proven. Now, assume that the norm is 1 for all composite values of  $n$  with up to  $m - 1$  distinct primes. Now examine the case where  $n$  is divisible by  $m$  distinct primes.

In this instance  $n = \underbrace{p_1^{r_1} \dots p_{m-1}^{r_{m-1}}}_l p_m^{r_m}$ .

$$\begin{aligned} \Phi_n(X) &= \Phi_{lp_m}(X^{p_m^{r_m - 1}}) \\ &= \frac{\Phi_l(X^{p_m^{r_m}})}{\Phi_l(X^{p_m^{r_m - 1}})} \end{aligned}$$

By the induction hypothesis both the numerator and denominator of this expression have a constant term of 1. By the same argument above, the constant term of  $\Phi_n(X)$  is an integer such that multiplying it by 1 yields 1; clearly 1. Thus  $N_{K/\mathbb{Q}}(1 - \zeta_n) = (-1)^{\varphi(n)} = 1$ . This completes our induction, so we have that when two or more distinct primes divide  $n$ ,  $N_{K/\mathbb{Q}}(1 - \zeta_n) = 1$ .

5) Let  $k$  be a field of characteristic  $p > 0$ , and let  $t$  and  $u$  be algebraically independent over  $k$ . Prove the following:

(a)  $k(t, u)$  has degree  $p^2$  over  $k(t^p, u^p)$ .

$t, u$  are algebraically independent over  $k$ , so there is no polynomial  $f \in k[X_1, X_2]$  (with  $f \neq 0$ ) such that  $f(t, u) = 0$ . As a direct consequence both  $t$  and  $u$  are transcendental over  $k$ ,  $t$  is transcendental over  $k(u)$  and  $u$  is transcendental over  $k(t)$ .

We'll first prove the parallel fact that  $[k(t) : k(t^p)] = p$ .

$x^p - t^p = (x - t)^p$  is irreducible over  $k(t^p)$  as the only root of this polynomial is  $t$ , so  $[k(t) : k(t^p)] = p$ . Further note that this minimal polynomial has multiple roots, so this extension is not separable (indeed, as there are no non-trivial divisors of  $p$  and the inseparable component is not degree 1, this extension is purely inseparable).

In diagrams, we have

$$\begin{array}{c} k(t) \\ \left| \begin{array}{l} p \text{ (purely inseparable)} \end{array} \right. \\ k(t^p) \end{array}$$

To address the original question, it suffices to note that we can break our extension from  $k(t^p, u^p)$  into two subextensions that both behave as the extension from  $k(t^p)$  to  $k(t)$  extension above. In diagrams, we have:

$$\begin{array}{c}
k(t, u) \\
\left| \begin{array}{l} p \text{ (purely inseparable)} \end{array} \right. \\
k(t, u^p) \\
\left| \begin{array}{l} p \text{ (purely inseparable)} \end{array} \right. \\
k(t^p, u^p)
\end{array}$$

Where in our lowest extension, we note that  $k(u^p)$  is a field with characteristic  $p > 0$  and  $t$  is transcendental over  $k(u^p)$ , so the extension of  $k(u^p)(t^p) = k(t^p, u^p)$  to  $k(u^p)(t) = k(t, u^p)$  is a purely inseparable extension of degree  $p$  by the above argument. We then exchange elements and note that  $k(t)$  is a field with characteristic  $p > 0$  and  $u$  is transcendental over  $k(t)$ , so the extension of  $k(t)(u^p) = k(t, u^p)$  to  $k(t)(u) = k(t, u)$  is a purely inseparable extension of degree  $p$  by the same argument.

So, finally we have

$$[k(t, u) : k(t^p, u^p)] = \underbrace{[k(t, u) : k(t, u^p)]}_{\text{degree } p} \underbrace{[k(t, u^p) : k(t^p, u^p)]}_{\text{degree } p} = p^2$$

- (b) There are infinitely many fields between  $k(t, u)$  and  $k(t^p, u^p)$ .

By the primitive element theorem, it suffices to show that there is no primitive element for the extension  $k(t^p, u^p)$  to  $k(t, u)$ . If there were such an element, then there would be an  $\alpha \in k(t, u)$  such that  $k(t^p, u^p)(\alpha) \cong k(t, u)$ . By the above, adjoining  $\alpha$  would have to yield an extension of exactly degree  $p^2$ . Any element in  $k(t, u)$  can be thought of as a quotient field of polynomials in  $t$  and  $u$ , so any such rational expression when raised to the  $p$  is then an element of  $k(t^p, u^p)$  (as the exponent  $p$  distributes in a field of characteristic  $p$ ), so adjoining any element in  $k(t, u)$  to  $k(t^p, u^p)$  yields an extension of at most degree  $p$ . So, there is no primitive element  $\alpha \in k(t, u)$  such that  $k(t^p, u^p)(\alpha) \cong k(t, u)$ .

So, by the primitive element theorem there are an infinite number of fields between  $k(t^p, u^p)$  and  $k(t, u)$ .

- 6) Prove the Chevalley-Warning theorem: Let  $f(X_1, \dots, X_n)$  be a polynomial in  $n$  variables of total degree at most  $d$  over a finite field  $\mathbb{F}_q$  of  $q$  elements, where  $q = p^r$ . Let  $N_q(f)$  be the number of solutions of  $f(x_1, \dots, x_n) = 0$  with  $x_i \in \mathbb{F}_q$ . Assume  $n > d$ . Show  $N_q(f)$  is divisible by  $p$ .

For all  $x \in \mathbb{F}_q$  we have:

$$x^{q-1} = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

so

$$(1 - f^{q-1})(x_1, \dots, x_n) = \begin{cases} 1 & (x_1, \dots, x_n) \text{ is a zero of } f \\ 0 & \text{otherwise} \end{cases}$$

As such, the number of zeros of  $f$ :

$$N_q(f) \equiv_p \sum_{(x_1, \dots, x_n) \in \mathbb{F}_q} (1 - f^{q-1})(X_1, \dots, X_n) = - \sum_{(x_1, \dots, x_n) \in \mathbb{F}_q} f^{q-1}(X_1, \dots, X_n)$$

As  $f$  was of total degree  $d$ ,  $f^{q-1}$  is of total degree at most  $(q-1)d$ , thus we can treat  $f^{q-1}$  as a sum of monomials, each of total degree at most  $(q-1)d$ . Split the sum for  $N_q(f)$  across these monomials. For the  $l$ th monomial term of  $f^{q-1}$ , we have (for some  $a_l \in \mathbb{F}_q$ )

$$-a_l \sum_{(x_1, \dots, x_n) \in \mathbb{F}_q} x^{u_1} \dots x^{u_n} = -a_l \prod_{i=1}^n \sum_{x_i \in \mathbb{F}_q} x_i^{u_i}$$

This last equality is a consequence of the fact that summing over all possible products is combinatorially equivalent to taking the product of sums.

For the sum  $\sum_{x_i \in \mathbb{F}_q} x_i^{u_i}$ , we simplify this sum depending on the value  $u_i$ :

$$\sum_{x_i \in \mathbb{F}_q} x_i^{u_i} = \begin{cases} -1 & (q-1) \mid u_i \\ 0 & \text{otherwise} \end{cases}$$

As  $d < n$  there must be at least one  $u_i$  non-divisor of  $q-1$  in each monomial term, so each monomial term sums to identically zero in  $F_q$ . So

$$N_q(f) \equiv_p 0$$

Or otherwise stated,  $p$  divides  $N_q(f)$ .