Ho Chi Minh University of Science HCMUS

Update: April 16, 2009

Finite fields: some applications

Michel Waldschmidt [1]

First course

April 8, 2009

References

[1] W. Chen – *Discrete Mathematics*, 201 pp. (web edition, 2008).
http://www.maths.mq.edu.au/∼wchen/ln.html/

[2] G.L. Mullen, C. Mummert – *Finite Fields and Applications*, Student mathematical library, **41**, AMS 2007.

[3] S. Lang – *Algèbre*, Dunod, 2004.

[4] R. Lidl & H. Niederreiter – *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1994.
http://www.amazon.com/gp/reader/0521460948/ref=sib_dp_ptu#reader-link

[5] V. Shoup – *A Computational Introduction to Number Theory and Algebra* (Version 2) second print editon, Fall 2008.
http://shoup.net/ntb/

[6] Zhe-Xian Wan – *Lectures on finite fields and Galois rings*, Word Scientific Publishing Co. Pte. Ltd. 2003.

1 Cyclotomic Polynomials

1.1 Cyclotomic Polynomials over Z

One of the equivalent definitions of the polynomials $\Phi_1, \Phi_2, \dots$ in $\mathbf{Z}[X]$ is by induction on n:

$$\Phi_1(X) = X - 1, \qquad \Phi_n(X) = \frac{X^n - 1}{\displaystyle\prod_{\substack{d|n\\ d\neq n}} \Phi_d(X)}\cdot$$

[1] This text is accessible on the author's web site
http://www.math.jussieu.fr/∼miw/coursVietnam2009.html

It follows that $\Phi_n(X) \in \mathbf{Z}[X]$ for all n. Let us recall why.

We shall work with groups, rings and fields. We shall use very often the properties of finite commutative groups (these are the same as $\mathbf{Z}$–modules), especially of cyclic groups.

An important result is that the order (number of elements) of a subgroup of a finite group G divides the order of G (*Lagrange's Theorem*). We shall need the definition and the properties of the order of an element (which is the order of the subgroup generated by this element). An element x in a multiplicative group G is *torsion* if it has finite order, that means if there exists $m \geq 1$ such that $x^m = 1$. In this case the order of x is the least of these m. The set of $m \in \mathbf{Z}$ with $x^m = 1$ is a subgroup of $\mathbf{Z}$ which is not 0, hence it has a unique positive generator d which is the order of x. Therefore for an element x of order d we have

$$x^m = 1 \Leftrightarrow d|m.$$

We stress that the condition $x^m = 1$ does not mean that x has order m, it means that the order of x divides m.

If x is an element in a multiplicative group G and m an integer such that $x^m = 1$, then for i and j in $\mathbf{Z}$ satisfying $i \equiv j \pmod{m}$ we have $x^i = x^j$. In other terms the kernel of the morphism

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & G \\ j & \mapsto & x^j \end{array}$$

contains $m\mathbf{Z}$. Hence this morphism factors to $\mathbf{Z}/m\mathbf{Z} \longrightarrow G$, which we denote again by $j \mapsto x^j$. This means that we define x^j for j a class modulo m by selecting any representative in $\mathbf{Z}$.

The subgroups and quotients of a cyclic group are cyclic. For any cyclic group of order n and for any divisor d of n there is a unique subgroup of G of order d; if ζ is a generator of the cyclic group G of order n and if d divides n, then $\zeta^{n/d}$ has order d, hence is a generator of the unique subgroup of G of order d.

A product $G_1 \times G_2$ of two finite groups is cyclic if and only if G_1 and G_2 are cyclic with relatively prime order.

The number of generators of a cyclic group of order n is given by Euler's function $\varphi(n)$.

All rings are supposed to have a unity 1 different from 0 (there is no ring structure on the set with only one element), they are supposed to be commutative. Unless we specify it, we shall further assume the rings to be without zero divisor (they are also called *integral domains* but we shall just say *rings*).

The units of a ring A are the invertible elements, they form a multiplicative group $A^\times$. A field is a ring F such that $F^\times = F \setminus \{0\}$. The torsion elements in the group $A^\times$ are the roots of unity in A. Their set

$$A^\times_{\text{tors}} = \{x \in A\ ;\ \text{ there exists } n \geq 1 \text{ such that } x^n = 1\}$$

is the torsion subgroup of the group of units $A^\times$.

We assume that the definitions of irreducible elements in a ring and of factorial rings are known.

When F is a field, the ring $F[X]$ of polynomials in one variable over F is a principal domain (since it is an Euclidean ring), and therefore a factorial ring.

The ring $\mathbf{Z}[X]$ is not an Euclidean ring - but if A and B are in $\mathbf{Z}[X]$ and B is monic, then both the quotient Q and the remainder R of the Euclidean division in $\mathbf{Q}[X]$ of A by B

$$A = BQ + R$$

are in $\mathbf{Z}[X]$. This proves that $\Phi_n(X) \in \mathbf{Z}[X]$.

First examples. From the very definition we derive

$$\Phi_2(X) = \frac{X^2-1}{X-1} = X+1, \quad \Phi_3(X) = \frac{X^3-1}{X-1} = X^2+X+1,$$

and more generally for p prime

$$\Phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

The next cyclotomic polynomials are

$$\Phi_4(X) = \frac{X^4-1}{X^2-1} = X^2+1 = \Phi_2(X^2),$$

$$\Phi_6(X) = \frac{X^6-1}{(X^3-1)(X+1)} = \frac{X^3+1}{X+1} = X^2-X+1 = \Phi_3(-X).$$

Definition. In a field F, an element ζ is a *n-th root of unity* if $\zeta^n = 1$. It is a *primitive n-th root of unity* if it is an element of order n in the multiplicative group $F^\times$.

For each positive integer n, the n–th roots of unity in F form a finite subgroup of $F^{\times}_{\text{tors}}$ having at most n elements. The union of all these subgroups of $F^{\times}_{\text{tors}}$ is just the torsion group $F^{\times}_{\text{tors}}$ itself. This group contains 1 and -1, but it could have just one element, like for $F = \mathbf{Z}/2\mathbf{Z}$. The torsion subgroup of $\mathbf{R}^{\times}$ is $\{\pm 1\}$, the torsion subgroup of $\mathbf{C}^{\times}$ has n elements.

Since the n roots of $X^n - 1$ in $\mathbf{C}$ are pairwise distinct, and since

$$X^n - 1 = \prod_{d|n} \Phi_d(X), \tag{1}$$

the roots of Φ_n in $\mathbf{C}$ are the complex numbers which are roots of $X^n - 1$ but not roots of $X^d - 1$ when d divides n, $d \neq n$. Hence in $\mathbf{C}[X]$ we have

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2i\pi k/n}), \qquad \Phi_n(X) = \prod_{\substack{0 \leq k \leq n-1 \\ \gcd(k,n)=1}} (X - e^{2\pi i k/n}). \tag{2}$$

Therefore:

Proposition 3. *The roots of $\Phi_n(X)$ in $\mathbf{C}$ are exactly the complex primitive n-th roots of unity.*

The name **cyclotomy** comes from the Greek and means *divide the circle*. The roots of $X^n - 1$ are the vertices of a regular polygon with n sides.

The second formula from (2) provides an alternative way of defining $\Phi_n \in \mathbf{C}[X]$. Starting from this definition, it is not plain that Φ_n has coefficients in $\mathbf{Z}$. One may recover this fact by using Galois theory, or more easily (as we did), by using the equivalence with the previous definition which rests on (1) and the Euclidean algorithm in $\mathbf{Z}[X]$.

The degree of Φ_n is the value at n of Euler's function

$$\varphi(n) = \#\{k \; ; \; 1 \leq k \leq n, \; \gcd(k,n) = 1\}.$$

This is the order of the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^{\times}$ of the ring $\mathbf{Z}/n\mathbf{Z}$.

Recall that φ is a multiplicative function: $\varphi(mn) = \varphi(m)\varphi(n)$ when m and n are relatively prime. This follows from the ring isomorphim between the ring product $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$ and the ring $(\mathbf{Z}/mn\mathbf{Z})$ when m and n are relatively prime.

Also $\varphi(p^a) = p^{a-1}(p-1)$ for p prime and $a \geq 1$. Hence the value of $\varphi(n)$ for n written as a product of powers of distinct prime numbers is

$$\varphi(p_1^{a_1} \cdots p_r^{a_r}) = p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1).$$

From (1) we deduce

Corollary 4.

$$n = \sum_{d|n} \varphi(d).$$

Exercise 5. *Let n be a positive integer. Check*

$$\varphi(2n) = \begin{cases} \varphi(n) & \text{if } n \text{ is odd,} \\ 2\varphi(n) & \text{if } n \text{ is even,} \end{cases} \qquad \Phi_{2n}(X) = \begin{cases} \Phi_n(-X) & \text{if } n \text{ is odd,} \\ \Phi_n(X^2) & \text{if } n \text{ is even.} \end{cases}$$

`Hint:` For a geometric proof, cut the circle in $2n$ pieces in place of n. Compare the positions on the unit circle of the roots of the two degree n polynomials $X^n - 1$ and $X^n + 1$.

For instance $\Phi_{2^\ell}(X) = X^{2^{\ell-1}} + 1$ for $\ell \geq 1$.

Exercise 6. *For p prime and $n \geq 1$, check*

$$\begin{cases} \Phi_n(X^p) = \Phi_{pn}(X) & \text{and} & \varphi(pn) = p\varphi(n) & \text{if } p|n, \\ \Phi_n(X^p) = \Phi_{pn}(X)\Phi_n(X) & \text{and} & \varphi(pn) = (p-1)\varphi(n) & \text{if } \gcd(p,n) = 1. \end{cases}$$

Check also

$$\Phi_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1$$

when p is a prime and $r \geq 1$.

Theorem 7. *For any $n \geq 1$, the polynomial Φ_n is irreducible in $\mathbf{Z}[X]$.*

Hence $[\mathbf{Q}(e^{2\pi i/n}) : \mathbf{Q}] = \varphi(n)$.

We postpone the proof of Theorem 7 to the next course. We give here the proof in the special case where n is prime.

Proof of Theorem 7 for $n = p$ prime. We set $X - 1 = Y$, so that

$$\Phi_p(Y+1) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{2} Y + p \in \mathbf{Z}[Y].$$

We observe that p divides all coefficients – but the leading one – of the monic polynomial $\Phi_p(Y+1)$ and that p^2 does not divide the constant term. We conclude by using the next result. □

Theorem 8 (Eisenstein criterion)**.** *Let*

$$h(X) = c_0 X^d + \cdots + c_d \in \mathbf{Z}[X]$$

and p a prime number. Assume h is product of two polynomials in $\mathbf{Z}[X]$ of positive degrees. Assume also that p divides c_i for $1 \leq i \leq d$ but that p does not divide c_0. Then p^2 divides c_d.

Proof. Let

$$f(X) = a_0 X^n + \cdots + a_n \quad \text{and} \quad g(X) = b_0 X^m + \cdots + b_m$$

be two polynomials of positive degrees m and n such that $h = fg$. Hence $d = m + n$, $c_0 = a_0 b_0$, $c_d = a_n b_m$. We use the reduction modulo p

$$\Psi_p : \mathbf{Z}[X] \longrightarrow \mathbf{F}_p[X] \tag{9}$$

which is the unique morphism of rings mapping X to X. Its kernel is the principal ideal $p\mathbf{Z}[X] = (p)$ generated by p.

Write $F = \Psi_p(f)$, $G = \Psi_p(g)$, $H = \Psi_p(h)$,

$$F(X) = \alpha_0 X^n + \cdots + \alpha_n, \quad G(X) = \beta_0 X^m + \cdots + \beta_m$$

and

$$H(X) = \gamma_0 X^d + \cdots + \gamma_d.$$

The greek letters α, β, γ denote the classes of the roman letters a, b, c modulo p. By assumption $\gamma_0 \neq 0$, $\gamma_1 = \cdots = \gamma_d = 0$, hence $H(X) = \gamma_0 X^d = F(X)G(X)$ with $\gamma_0 = \alpha_0 \beta_0 \neq 0$. Now F and G have positive degrees n and m, hence $\alpha_n = \beta_m = 0$, which means that p divides a_n and b_m, and therefore p^2 divides $c_d = a_n b_m$.. □

1.2 Cyclotomic Polynomials over any ring

The existence of Ψ_p in (9) is a special case of the following fact: *Any morphism of rings $f : A \to B$ extends in a unique way to a morphism of rings $A[X] \to B[X]$ mapping X to X.*

As a consequence, Φ_n makes sense in $A[X]$ over any ring A: indeed for any ring A there is a unique ring morphism $\mathbf{Z} \to A$. This morphism is used to give the definition of the characteristic of a ring. For an integral domain the characteristic is either 0 or a prime.

We shall use repeatedly the fact that in a ring of characteristic p, the map $x \mapsto x^p$ is ring homomorphism: $(x + y)^p = x^p + y^p$.

Let $n = p^r m$ with $r \geq 0$ and p does not divide m. If F is a field of characteristic p, we have in $F[X]$

$$X^n - 1 = (X^m - 1)^{p^r}.$$

For that reason when dealing with $X^n - 1$ and Φ_n we are going to assume most often that the characteristic of the field is not a prime divisor of n.

Exercise 10. *In characteristic p, for $r \geq 1$ and $m \geq 1$*

$$\Phi_{mp^r}(X) = \Phi_m(X)^{p^{r-1}(p-1)}.$$

`Hint:` *Use exercise 6.*

The proof we gave of proposition 3 extends to any field F, with the proviso that the characteristic of F is not a prime divisor of n:

Proposition 11. *Let F be a field and n an integer. We assume that either the characteristic of F is 0 or else that it is a prime number which does not divide n. Then roots of $\Phi_n(X)$ in F are exactly the primitive n-th roots of unity in F.*

For instance in any algebraically closed field Ω the number of primitive n-th roots of unity is $\varphi(n)$. These are the generators of the unique cyclic subgroup C_n of order n of $\Omega^\times$, which is the group of n-th roots of unity in Ω:

$$C_n = \{x \in \Omega\ ;\ x^n = 1\}.$$

Proposition 12. *Any finite subgroup of the multiplicative group of a field F is cyclic. If n is the order of G, then G is the set of roots of the polynomial $X^n - 1$ in F.*

Proof. Let F be a field and G a finite subgroup of $F^\times$. Denote by e the exponent of G: this is the smallest positive integer such that $x^e = 1$ for any $x \in G$. Equivalently, e is the lcm of the orders of the elements in G. By Lagrange's theorem e divides n. Any x in G is a root of the polynomial $X^e - 1$. Since G has order n, we get n roots in the field F of this polynomial $X^e - 1$ of degree $e \leq n$. Hence $e = n$. We conclude by using the fact that there exists in G an element of order e, hence G is cyclic and is the set of roots of the polynomial $X^n - 1$ in F.

The following alternative proof (not using the exponent) is instructive since it uses the properties of the cyclotomic polynomials. For any divisor d of n, denote by $N_G(d)$ the number of elements in G of order d. By Lagrange's Theorem

$$n = \sum_{d|n} N_G(d). \tag{13}$$

Let d be a divisor of n. If $N_G(d) > 0$, that is, if there exists an element ζ in G of order d, then the cyclic subgroup of G generated by ζ has order d, it has $\varphi(d)$ génerators. These $\varphi(d)$ elements in F are roots of Φ_d and therefore they are all the roots of Φ_d in F. It follows that there are exactly

$\varphi(d)$ elements of order d in G. This proves that $N_G(d)$ is either 0 or $\varphi(d)$. From (13) and Corollary 4 we deduce

$$n = \sum_{d|n} N_G(d) \leq \sum_{d|n} \varphi(d) = n,$$

hence $N_G(d) = \varphi(d)$ for all $d|n$. In particular $N_G(n) > 0$, which means that G is cyclic. □

1.3 Cyclotomic Polynomials over a finite field

Let F be finite field with q element. The characteristic of F is a finite prime p. The *prime field* of F (which is defined as the smallest subfield of F, that is the intersection of all subfields of F) is therefore $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, which is the unique field with p elements. Since F is a finite vector space over $\mathbf{F}_p$, we deduce $q = p^r$ where r is the dimension $[F : \mathbf{F}_p]$ of the $\mathbf{F}_p$–vector space F.

We shall use the definitions of algebraically closed fields and of the algebraic closure of a field. We take for granted that any field has an algebraic closure. We denote by $\overline{\mathbf{F}}_p$ an algebraic closure of $\mathbf{F}_p$. While dealing with finite fields of characteristic p, we shall always consider that they are subfield of $\overline{\mathbf{F}}_p$.

Given $q = p^r$, the unique subfield of $\overline{\mathbf{F}}_p$ with q elements is the set $\mathbf{F}_q$ of roots of $X^q - X$ in $\overline{\mathbf{F}}_p$:

$$X^q - X = \prod_{x \in \mathbf{F}_q} (X - x), \qquad X^{q-1} - 1 = \prod_{x \in \mathbf{F}_q^\times} (X - x). \tag{14}$$

See [5], Theorem 19.6. The set $\{X - x \ ; \ x \in \mathbf{F}_q\}$ is the set of all monic degree 1 polynomials with coefficients in $\mathbf{F}_q$. Hence (14) is the special case $n = 1$ of the next statement ([5], Theorem 19.10).

Proposition 15. *For any $n \geq 1$,*

$$X^{q^n} - X = \prod_{d|n} \prod_{f \in E_q(d)} f(X)$$

where $E_q(d)$ is the sel all monic irreducible polynomials in $\mathbf{F}_q[X]$ of degree d.

Denote by $N_q(d)$ the number of elements in $E_q(d)$, that is the number of monic irreducible polynomials of degree d in $\mathbf{F}_q[X]$. Proposition 15 yields, for $n \geq 1$,

$$q^n = \sum_{d|n} dN_q(d).$$

As a consequence ([5], Theorem 19.10),

$$\frac{1}{2n}q^n \leq N_q(n) \leq \frac{1}{n}q^n$$

for all $n \geq 1$.

From Möbius inversion formula one deduces ([5], Exercise 19.1):

$$N_q(n) = \sum_{d|n} \mu(d) q^{n/d}.$$

For instance when ℓ is a prime number not equal to the characteristic p of $\mathbf{F}_q$,

$$N_q(\ell) = \frac{q^\ell - q}{\ell}. \tag{16}$$

Remarks on Möbius inversion formula.

The *Möbius function* μ is the map from the positive integers to $\{0, 1, -1\}$ defined by the properties $\mu(1) = 1$, $\mu(p) = -1$ for p prime, $\mu(p^m) = 0$ for p prime and $m \geq 2$, and $\mu(ab) = \mu(a)\mu(b)$ if a and b are relatively prime. Hence $\mu(a) = 0$ if and only if a has a square factor, while for a squarefree number a which is a product of s distinct primes we have $\mu(a) = (-1)^s$:

$$\mu(p_1 \cdots p_s) = (-1)^s.$$

There are several variants of the Möbius inversion formula. The most classical one that we just used states that for f and g two maps defined on the set of positive integers with values in an additive group, the two following properties are equivalent:

(i) *For any integer* $n \geq 1$,

$$g(n) = \sum_{d|n} f(d).$$

(ii) *For any integer* $n \geq 1$,

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

For instance Corollary 4 is equivalent to

$$\varphi(n) = \sum_{d|n} \mu(n/d) d \quad \text{for all } n \geq 1$$

An equivalent statement of the Möbius inversion formula is the following multiplicative version which deals with two maps f, g from the positive integers into an abelian multiplicative group G. The two following properties are equivalent:
(i) *For any integer* $n \geq 1$,

$$g(n) = \prod_{d|n} f(d).$$

(ii) *For any integer* $n \geq 1$,

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

For instance take for G the multiplicative group $F(X)^\times$ where F is a field. The n–th cyclotomic polynomial Φ_n has been defined by induction using (1) Hence

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

A third form of the Möbius inversion formula (which we shall not use here) deals with two functions F and G from $[1, +\infty)$ to $\mathbf{C}$. The two following properties are equivalent:
(i) *For any real number* $x \geq 1$,

$$G(x) = \sum_{n \leq x} F(x/n).$$

(ii) *For any real number* $x \geq 1$,

$$F(x) = \sum_{n \leq x} \mu(n) G(x/n).$$

As an illustration take $F(x) = 1$ for all x and $G(x) = [x]$. Then

$$\sum_{n \leq x} \mu(n)[x/n] = 1$$

Denote by σ_q the $\mathbf{F}_q$–automorphism of $\overline{\mathbf{F}}_p$ (*Frobenius* automorphism: [5] Theorem 19.7):

$$\sigma_q(x) = x^q.$$

Let $x \in \overline{\mathbf{F}}_p$. The conjugates of x over $\mathbf{F}_q$ are the roots in $\overline{\mathbf{F}}_p$ of the minimal (=monic irreducible) polynomial of x over $\mathbf{F}_q$, and these are exactly the images of x by the iterated Frobenius:

$$\sigma_q^0 = 1,\ \sigma_q^\ell = \sigma_q^{\ell-1} \circ \sigma_q \quad (\ell \geq 1),$$

$$\sigma_q^0(x) = x,\ \sigma_q(x) = x^q,\ \sigma_q^2(x) = x^{q^2}, \qquad \sigma_q^\ell(x) = x^{q^\ell} \quad (\ell \geq 0).$$

We shall use repeatedly the following fact:

Lemma 17. *Let $\mathbf{F}_q$ be a finite field with q elements and $f \in \overline{\mathbf{F}}_p[X]$ a polynomial whose coefficients are algebraic over $\mathbf{F}_q$. Then f belongs to $\mathbf{F}_q[X]$ if and only if $f(X^q) = f(X)^q$.*

One of the main results of the theory of finite fields is the following ([5] Theorem 19.15):

Theorem 18. *Let $\alpha \in \overline{\mathbf{F}}_p$. Define $n = [\mathbf{F}_q(\alpha) : \mathbf{F}_q]$. Then*

$$n = \min\{\ell \geq 1\ ;\ \sigma_q^\ell(\alpha) = \alpha\}$$

and the minimal polynomial of α over $\mathbf{F}_q$ is

$$\prod_{\ell=0}^{n-1}\bigl(X - \sigma_q^\ell(\alpha)\bigr).$$

We apply this result to the cyclotomic polynomials ([5] Theorem 19.16):

Corollary 19. *Let $\mathbf{F}_q$ be a finite field with q elements and let n be a positive integer not divisible by the characteristic of $\mathbf{F}_q$. Then the cyclotomic polynomial Φ_n splits in $\mathbf{F}_q[X]$ into a product of irreducible factors, all of the same degree d, where d is the order of q modulo n.*

The order of q modulo n is by definition the order of the class of q in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ (hence it is defined if and only if n and q are relatively prime), it is the smallest integer ℓ such that q^ℓ is congruent to 1 modulo n.

Since an element $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$ if and only if ζ is a root of Φ_n, an equivalent statement to Corollary 19 is the following.

Corollary 20. *If $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$, then its degree $d = [\mathbf{F}_q(\zeta) : \mathbf{F}_q]$ over $\mathbf{F}_q$ is the order of q modulo n.*

Exercise 21. *Let F be a field, m and n two positive integers, a and b two integers ≥ 2. Check that the following conditions are equivalent.*
(i) n divides m.
(ii) In $F[X]$, the polynomial $X^n - 1$ divides $X^m - 1$.
(iii) $a^n - 1$ divides $a^m - 1$.
(ii') In $F[X]$, the polynomial $X^{a^n} - X$ divides $X^{a^m} - X$.
(iii') $b^{a^n} - b$ divides $b^{a^m} - b$.

`Hint` *Denote r the remainder of the Euclidean division of m by n. Check that $a^r - 1$ is the remainder of the Euclidean division of $a^m - 1$ by $a^n - 1$.* See also [5], Theorems 19.2, 19.3, 19.4.