Math 254B: Number theory.

H.W. Lenstra, Jr. (office 879, tel. 643.7857, office hours MF 3:15–4),

Spring 1988, MWF 2-3, 6 Evans.

This course is a continuation of **Math 254A** (Number theory), which was taught in the fall of 1987. The contents of the latter course are supposed to be known.

The main subject of the course will be *class field theory*, which classifies the abelian extensions of an algebraic number field. Other subjects have not yet been decided upon, but they will probably be taken from the following: local class field theory; power reciprocity laws; quadratic fields; L-series and distribution of prime ideals; the Riemann hypothesis for curves over finite fields.

Every one or two weeks some homework problems will be handed out, to accommodate students that wish to get credit for the course. There will not be a final examination.

The main theorems of class field theory were obtained by Teiji Takagi (Japanese mathematician, 1875-1960) and Emil Artin (German mathematician, 1898-1962) in the period 1920–1926. For the history of class field theory, see Chapter XI by H. Hasse in the book by Cassels and Fröhlich mentioned below. The proofs of Takagi and Artin depended partly on analytic techniques (Dirichlet L-series); see H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, I, Ia, II, *Jber. dt. Mat. Verein.* **35** (1926), 1–55; **36** (1927), 233–311; *Erg. Bd.* **6** (1930), 1–204; reprint: Physica-Verlag, Würzburg, 1965.

A modern exposition of the treatment depending on L-series is contained in S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, 1970; reprint: Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1986.

After the war, an approach to the main theorems of class field theory was found that does not depend on analysis but on *cohomology of groups*. The basic reference is E. Artin, J. Tate, *Class field theory*, Benjamin, New York, 1967. For a more accessible treatment, see J.W.S. Cassels, A. Fröhlich (eds), *Algebraic number theory*, Academic Press, London–New York, 1967; paperback reprint, 1986.

In the course no particular textbook will be followed. We shall adopt an approach that avoids both the L-functions and the cohomological techniques. It goes back to C. Chevalley, *La théorie des corps de classes, Ann. Math.* **41** (1940), 394-417.

Other approaches to class field theory can be found in A. Weil, *Basic number theory*, Springer-Verlag, Berlin, 1967, and in J. Neukirch, *Class field theory*, Springer-Verlag, Berlin, 1986.

Exercise 1. In class it was shown how to deduce the quadratic reciprocity law

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

(for odd primes p, q) from the inclusion $\mathbf{Q}(\sqrt{\left(\frac{-1}{q}\right)q}) \subset \mathbf{Q}(\zeta_q)$ and properties of the Artin symbol. Give a similar proof for the supplementary law

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8, \\ -1 & \text{if } p \equiv \pm 3 \bmod 8, \end{cases}$$

where p denotes an odd prime.

Exercise 2. Let L be a field extension of $\mathbf{Q}$ with $[L : \mathbf{Q}] \leq 2$, and denote by Δ the absolute value of the discriminant of L over $\mathbf{Q}$. For a positive integer m, let ζ_m denote a primitive m-th root of unity in an extension field of $\mathbf{Q}$.

(a) Prove that L is isomorphic to a subfield of $\mathbf{Q}(\zeta_\Delta)$.

(b) (This is harder.) Prove that Δ is the minimum of all positive integers m for which L is isomorphic to a subfield of $\mathbf{Q}(\zeta_m)$.

In Exercises 3–5 we let $f = X^3 - X - 1$, which is an irreducible polynomial in $\mathbf{Z}[X]$ with discriminant -23. We let α be a zero of f in an algebraic closure of $\mathbf{Q}$, and we write $K = \mathbf{Q}(\sqrt{-23})$, $L = K(\alpha)$.

In Exercises 4 and 5, the theorems stated (but not yet proved) in class may be used.

Exercise 3. (a) Prove that L is the Galois closure of $\mathbf{Q}(\alpha)$ over $\mathbf{Q}$, and that $K \subset L$ is an abelian extension of degree 3.

(b) Prove that exactly two primes of $\mathbf{Q}(\alpha)$ are ramified over $\mathbf{Q}$, and that they lie over 23 and ∞. Prove that in both cases the ramification index equals 2.

(c) Prove that $K \subset L$ is totally unramified.

Exercise 4. Prove that L is the Hilbert class field of K.

Exercise 5. Let p be a prime number, and let m be the number of distinct zeros of $(f \bmod p)$ in $\mathbf{F}_p$. Prove the following:

(a) $m = 0$ if and only if $\left(\frac{p}{23}\right) = 1$ and p cannot be written as $p = a^2 + 23b^2$ with a, $b \in \mathbf{Z}$.

(b) $m = 1$ if and only if $\left(\frac{p}{23}\right) = -1$.

(c) $m = 2$ if and only if $p = 23$.

(d) $m = 3$ if and only if p can be written as $p = a^2 + 23b^2$ with a, $b \in \mathbf{Z}$, $a \neq 0$.

In Exercises 6 and 7, we let K be an algebraic number field and L a finite abelian extension of K. Further we let $\mathfrak{p}$ be a prime of K.

Let $\mathfrak{f}(L/K)$ be the *conductor* of L over K; so this is the greatest common divisor of all cycles $\mathfrak{m}$ of K for which L is contained in the ray class field modulo $\mathfrak{m}$ of K. Denote by m the exponent to which $\mathfrak{p}$ appears in $\mathfrak{f}$. It is part of the main theorem of class field theory that $m \geq 1$ if and only if $\mathfrak{p}$ is ramified in L, and that $m \geq 2$ if and only if $\mathfrak{p}$ is finite and *wildly* ramified in L.

In these exercises we shall find an *upper* bound for m. We may and do assume that $\mathfrak{p}$ is *finite*. Denote by p be the prime of $\mathbf{Q}$ over which $\mathfrak{p}$ is lying, and let $e = e(\mathfrak{p}/p)$ be the ramification index of $\mathfrak{p}$ over p.

For exercise 7, the theorems stated (but not yet proved) in class may be used.

Exercise 6. For an integer $i > 0$, denote by U_i the open subgroup $1 + \mathfrak{p}^i$ of $K_\mathfrak{p}^*$. Prove the following assertions.

(a) If i, j are positive integers with $j \not\equiv 0 \bmod p$, then the map $U_i \to U_i$ sending every x to x^j is an isomorphism.

(b) If $i > e/(p-1)$, then there is an isomorphism $U_i \to U_{i+e}$ sending every x to x^p.

(c) If j is a positive integer, then $(K_\mathfrak{p}^*)^j$ is an *open* subgroup of $K_\mathfrak{p}^*$, and it contains $U_{e'+ke}$, where e' denotes the least integer $> e/(p-1)$ and k is the number of factors p in j.

(d) If $K_\mathfrak{p} \subset E$ is a finite extension, then $N_{E/K_\mathfrak{p}}[E^*]$ is an open subgroup of $K_\mathfrak{p}^*$, and it contains $U_{e'+ke}$, with e' as in (c) and k the number of factors p in $[E : K_\mathfrak{p}]$.

Exercise 7. (a) Prove that $m \leq e' + ke$, where e' denotes the least integer $> e/(p-1)$ and k is the number of factors p in $[L : K]$.

(b) More precisely, prove that $m \leq e' + ke$, with e' as before, but with k now equal to the number of factors p in the exponent of the inertia group of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$.

Exercises 8–10 are devoted to the extension $K \subset L$, where $K = \mathbf{Q}(\sqrt{-3})$ and $L = K(2^{1/3})$. We write ζ_3 for the cube root of unity $(-1 + \sqrt{-3})/2$ in K, and μ_3 for the subgroup of K^* generated by ζ_3. The unique primes of K lying over 2 and 3 are denoted by 2 and $\mathfrak{t}$, respectively.

The theorems stated (but not yet proved) in class may be used.

Exercise 8. (a) Prove that $K \subset L$ is cyclic of degree 3, and that the map $\epsilon\colon \mathrm{Gal}(L/K) \to$

μ_3 sending σ to $\sigma(2^{1/3})/2^{1/3}$ is a group isomorphism.

(b) Show that the conductor $\mathfrak{f}(L/K)$ divides $2\mathfrak{t}^4$.

(c) Let $\mathfrak{p}$ be a finite prime of K not dividing $2\mathfrak{t}$, and let $\mathfrak{N}\mathfrak{p}$ be the cardinality of its residue class field. Prove that $\epsilon((\mathfrak{p}, L/K))$ is the unique element of μ_3 that is congruent to $2^{(\mathfrak{N}\mathfrak{p}-1)/3}$ modulo $\mathfrak{p}$.

Exercise 9. Show that L is the ray class field of K with modulus 6 $(= 2 \cdot \mathfrak{t}^2)$.

Exercise 10. Let p be a prime number, and let m be the number of distinct cube roots of $(2 \bmod p)$ in $\mathbf{F}_p$. Prove the following:

(a) $m = 0$ if and only if $p \equiv 1 \bmod 3$ and p cannot be written as $p = a^2 + 27b^2$ with a, $b \in \mathbf{Z}$.

(b) $m = 1$ if and only if $p \not\equiv 1 \bmod 3$.

(c) $m \neq 2$.

(d) $m = 3$ if and only if p can be written as $p = a^2 + 27b^2$ with a, $b \in \mathbf{Z}$.

Exercise 11. Let G be a finite cyclic group, m the order of G, and A a G-module.

(a) Prove that m annihilates $H^i(G, A)$ for $i = 0$, 1.

(b) Suppose that for each $a \in A$ there is a unique $b \in A$ with $ma = b$. Prove that $H^i(G, A) = 0$ for $i = 0$, 1.

(c) Suppose that the Herbrand quotient $h(G, A)$ is defined. Prove that every prime number dividing the numerator or denominator of $h(G, A)$ divides m. Can you prove that conversely every positive rational number with this property occurs as $h(G, A)$, for suitable A?

Exercise 12. Let $K \subset L$ be a finite Galois extension of algebraic number fields, and suppose that the Galois group G is cyclic. Let J_L be the group of idèles of L. Prove that $H^1(G, J_L) = \{1\}$.

Exercise 13. Let $K \subset L$ be a finite Galois extension of algebraic number fields, with Galois group G. Denote by C_K and C_L the idèle class groups of K and L. Prove that $C_K = C_L^G$. [*Hint.* In class this was shown for *cyclic* G. Either generalize this proof, or reduce the general case to the cyclic case.]

In Exercises 14–16, let K be an algebraic number field, Cl_K its ideal class group, and $h_K = \#\mathrm{Cl}_K$ its class number. We let $\bar{K}$ be an algebraic closure of K, and $H(K)$ the

Hilbert class field of K, which is the maximal abelian totally unramified extension of K inside $\bar{K}$.

In class it was shown, as a consequence of the main theorem of class field theory, that $H(K)$ is a finite abelian extension of K of degree h_K, and that the Artin symbol induces a group isomorphism $\mathrm{Cl}_K \to \mathrm{Gal}(H(K)/K)$.

The exercises illustrate how properties of the Hilbert class field can be used to obtain information about the class number.

The theorems stated (but not yet proved) in class may be used.

Exercise 14. (a) Let E be a finite extension of K. Prove that $H(K) \subset H(E)$, and that h_K divides $h_E \cdot [E : K]$.
(b) Let E, F be two finite extensions of $\mathbf{Q}$ inside $\bar{\mathbf{Q}}$. Prove: if $h_E = h_F = 1$, then $h_{E \cap F} = 1$.

Exercise 15. (a) Let E be a finite extension of K, and denote by L the maximal abelian totally unramified extension of K inside E. Show that the cokernel of the norm map $N_{E/K} \colon \mathrm{Cl}_E \to \mathrm{Cl}_K$ is isomorphic to $\mathrm{Gal}(L/K)$.
(b) Let n be a positive integer, and denote by ζ_n a primitive n-th root of unity. Prove that the class number of $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ divides the class number of $\mathbf{Q}(\zeta_n)$.

Exercise 16. The *Hilbert class field tower* of K is the sequence of fields $H^{(0)}(K) = K \subset H^{(1)}(K) = H(K) \subset H^{(2)}(K) = H(H(K)) \subset \ldots \subset H^{(i)}(K) \subset \ldots$, where each $H^{(i)}(K)$ is the Hilbert class field of $H^{(i-1)}(K)$. The Hilbert class field tower is said to be *finite* if $H^{(i+1)}(K) = H^{(i)}(K)$ for some i.

Prove that the Hilbert class field tower of K is finite if and only if there is a finite extension E of K with $h_E = 1$.

Exercises 17–19 concern the following result, which was proved in class as a consequence of the first inequality:

(A) *if $K \subset L$ is a finite Galois extension of algebraic number fields, and S is a finite set of primes of L containing the infinite ones and the primes that ramify over K, then* $\mathrm{Gal}(L/K)$ *is generated by* $\{[\mathfrak{q}, L/K] : \mathfrak{q}$ *is a prime of* L, $\mathfrak{q} \notin S\}$.

Actually a stronger theorem is valid:

(B) *let the hypotheses be the same; then for every element* $\sigma \in \mathrm{Gal}(L/K)$ *there exist infinitely many finite primes* $\mathfrak{q}$ *of* L, *unramified over* K, *such that* $\sigma = [\mathfrak{q}, L/K]$.

Statement (B) is a consequence of Čebotarev's density theorem (Nikolai Gregorovič

Čebotarev, Russian mathematician, 1894-1947), and its only known proof employs complex L-functions; see S. Lang, *Algebraic number theory*, Ch. VIII, §4, Theorem 10. (Čebotarev's density theorem itself asserts a bit more, in that it makes "infinitely many" more precise.)

Exercise 17. (a) Dirichlet's theorem on primes in arithmetic progression asserts that for any two positive integers a, m with $\gcd(a, m) = 1$ there exist infinitely many prime numbers p with $p \equiv a \bmod m$ (Peter Gustav Lejeune Dirichlet, German mathematician, 1805–1859). Show how to deduce this theorem from (B).
(b) Show how to deduce the special case $m = 24$, $a \not\equiv 1 \bmod 24$ of Dirichlet's theorem from (A).

Exercise 18. Let $f \in \mathbf{Z}[X]$ be a non-zero polynomial with the property that the polynomial $(f \bmod p) \in \mathbf{F}_p[X]$ splits completely into linear factors in $\mathbf{F}_p[X]$, for all but finitely many prime numbers p. Prove that f splits completely into linear factors in $\mathbf{Q}[X]$. (Don't use (B).)

Exercise 19. (a) Let G be a group acting transitively on a finite set Ω with $\#\Omega > 1$. Prove that there exists $\sigma \in G$ such that for all $\omega \in \Omega$ one has $\sigma\omega \neq \omega$.
(b) Let $f \in \mathbf{Z}[X]$ be an irreducible polynomial with the property that $(f \bmod p)$ has a zero in $\mathbf{F}_p$, for all but finitely many primes p. Use (B) to show that f has degree 1.
(c) The classification of finite simple groups can be used to show that, for *finite* G, the element σ in (a) can be chosen to be of prime power order (see B. Fein, W. M. Kantor, M. Schacher, *J. Reine Angew. Math.* **328** (1981), 159-173). Prove that now (A) suffices to deduce the statement in (b).

Exercise 20. Let m be a positive integer, K an algebraic number field that contains a primitive m-th root of unity, and J its group of idèles. For a finite set S of primes of K we write

$$J_S = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}},$$

$$K_S = K^* \cap J_S,$$

$$E_S = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^{*m} \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}.$$

(a) Let S be a finite set of primes of K containing all infinite primes and all primes dividing m, and suppose that $J = K^* J_S$. Prove that the image of K_S in J_S/E_S is a group of order $m^{\#S}$ isomorphic to K_S/K_S^m, and that the quotient $J_S/(K_S E_S)$ is also of order $m^{\#S}$.

(b) Let J/J^m have the quotient topology from J. Prove that the image of K^* in J/J^m is a *discrete* subgroup, isomorphic to K^*/K^{*m}. Prove that it can be identified with the injective limit of the groups K_S/K_S^m, with S ranging over all finite sets of primes of K.
(c) Prove that the quotient group $J/(K^*J^m)$ is *compact*, and that it can be identified with the projective limit of the groups $J_S/(K_S E_S)$, with S ranging over all finite sets of primes of K for which $J = K^* J_S$.

Exercise 21. Let K be an algebraic number field, and α, β, $\gamma \in K$.
(a) Prove that there exist x, $y \in K$ with $\alpha x^2 + \beta y^2 = \gamma$ if and only if for each prime $\mathfrak{p}$ of K there exist x, $y \in K_\mathfrak{p}$ with $\alpha x^2 + \beta y^2 = \gamma$.
(b) Suppose that α, β and γ are non-zero. Prove that for all but finitely many primes $\mathfrak{p}$ of K there exist x, $y \in K_\mathfrak{p}$ with $\alpha x^2 + \beta y^2 = \gamma$.

Exercise 22. (a) Prove that the field $\mathbf{Q}(\sqrt{5})$ has class number 1, and that the group of units of its ring of integers is generated by -1 and $(1+\sqrt{5})/2$.
(b) Let p be a prime number. Prove that there exists a field K satisfying

$$[K : \mathbf{Q}] = 4, \qquad \sqrt{5} \in K, \qquad |\Delta_{K/\mathbf{Q}}| = 25p$$

if and only if $p \not\equiv 2, 3 \bmod 5$. Prove also that if such a field exists, it is uniquely determined by p, up to isomorphism. We denote this field by $K_{(p)}$.
(c) Prove that among all fields $K_{(p)}$, the only one that is Galois over $\mathbf{Q}$ is the field $K_{(5)}$. Can you embed $K_{(5)}$ in a cyclotomic extension of $\mathbf{Q}$?

Exercise 23. A number field is called *totally real* if it has no complex primes, *totally complex* if it has no real primes, and *mixed* if it is neither totally real nor totally complex. The *Fibonacci sequence* $(F_n)_{n=0}^\infty$ is inductively defined by $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$.
Let p be a prime number with $p \equiv 1$ or $4 \bmod 5$, and let $K_{(p)}$ be as in Exercise 22.
(a) Prove that $K_{(p)}$ is mixed if and only if $p \equiv 3 \bmod 4$.
(b) Suppose that $p \equiv 1 \bmod 8$. Prove that $K_{(p)}$ is totally real if p divides $F_{(p-1)/4}$, and totally complex otherwise.
(c) Suppose that $p \equiv 5 \bmod 8$. Prove that $K_{(p)}$ is totally complex if p divides $F_{(p-1)/4}$, and totally real otherwise.

Exercise 24. Let p be a prime number with $p \equiv 11$ or $19 \bmod 20$, and let $K_{(p)}$ be as in Exercise 22. Prove that the field $K_{(p)}$ has exactly one prime lying over 5 if $p \equiv 11 \bmod 20$, and exactly two primes lying over 5 if $p \equiv 19 \bmod 20$.

Let L be an algebraic number field of discriminant Δ over $\mathbf{Q}$. *Stickelberger's theorem* asserts that $\Delta \equiv 0$ or $1 \bmod 4$ (Ludwig Stickelberger, Swiss mathematician, 1850-1936). If s denotes the number of complex primes of L, then the sign of Δ is $(-1)^s$, so one can reformulate Stickelberger's theorem by saying that $|\Delta| \equiv 0$ or $(-1)^s \bmod 4$. In the Exercises 25–27 Stickelberger's theorem is generalized to *relative* discriminants.

Exercise 25. Let E be a finite extension of $\mathbf{Q}_2$, with ring of integers A. Let $x \in E^*$. Prove that $E(\sqrt{x})$ is unramified over E if and only if $x = (1+4y)z^2$ for some $y \in A$ and $z \in E^*$.

Exercise 26. Let $K \subset L$ be a quadratic extension of algebraic number fields, and write $\mathrm{Gal}(L/K) = \{\mathrm{id}_L, \sigma\}$. If $\mathfrak{a}$ is a non-zero ideal of the ring of integers A_K of K, we write $\mathfrak{N}\mathfrak{a} = \#(A_K/\mathfrak{a})$.
(a) Let $\mathfrak{p}$ be a prime of K, and let $(-1)_\mathfrak{p} \in J_K$ be the idèle that has coordinate -1 at $\mathfrak{p}$ and coordinate 1 at all other primes. Prove that the image of $(-1)_\mathfrak{p}$ under the Artin map $J_K \to \mathrm{Gal}(L/K)$ equals

id_L	if $\mathfrak{p}$ is unramified in L,
σ	if $\mathfrak{p}$ is an infinite prime that ramifies in L,
$\sigma^{(\mathfrak{N}\mathfrak{p}-1)/2}$	if $\mathfrak{p}$ is ramified in L and $\lvert 2\rvert_\mathfrak{p} = 1$.

(b) Let $\mathfrak{d}_{L/K}$ denote the discriminant of L over K, and s the number of infinite primes of L that ramify over K. Prove that $\mathfrak{N}\mathfrak{d}_{L/K} \equiv 0$ or $(-1)^s \bmod 4$.

Exercise 27. Let $K \subset L$ be a finite extension of algebraic number fields, and let $\mathfrak{d}_{L/K}$ denote the discriminant of L over K. Denote by s the number of infinite primes of L that ramify over K. Prove that $\mathfrak{N}\mathfrak{d}_{L/K} \equiv 0$ or $(-1)^s \bmod 4$.

Exercise 28. Let K be a number field, and r the number of real primes of K. Denote by Cl the class group of K, and by Cl^* the *strict* (or *narrow*) class group of K; i.e., the ray class group modulo the cycle $\mathfrak{f} = \prod_{\mathfrak{p}\ \mathrm{real}} \mathfrak{p}$. The 2-rank $\mathrm{rk}_2 A$ of a multiplicatively written abelian group A is defined to be the dimension of the $\mathbf{F}_2$-vector space A/A^2.
(a) Prove that $\mathrm{rk}_2\mathrm{Cl} \le \mathrm{rk}_2\mathrm{Cl}^* \le \mathrm{rk}_2\mathrm{Cl} + r - 1$ if $r > 0$.
(b) Let $H = \{x \in K^* : K(\sqrt{x})$ is unramified over K at all finite primes$\}$, and let H^+ be the set of elements of H that are positive at all real primes of K. Prove that $\mathrm{rk}_2\mathrm{Cl}^*$ equals the dimension of the $\mathbf{F}_2$-vector space H/K^{*2}, and that $\mathrm{rk}_2\mathrm{Cl}$ equals the dimension of the $\mathbf{F}_2$-vector space H^+/K^{*2}.

Exercise 29. Let the notation be as in the previous exercise.
(a) Let a, $b \in H$. Prove that the norm residue symbol $(a,b)_{2,\mathfrak{q}}$ equals 1 for every finite prime $\mathfrak{q}$ of K, and that $\prod_{\mathfrak{p}\text{ real}}(a,b)_{2,\mathfrak{p}} = 1$.
(b) Prove that $\mathrm{rk}_2\mathrm{Cl}^* \leq \mathrm{rk}_2\mathrm{Cl} + [r/2]$.

Exercise 30. Let p be a prime number, E a finite extension of $\mathbf{Q}_p$, and F a finite abelian tamely ramified extension of E. Denote by $\mathfrak{p}_E$ and $\mathfrak{p}_F$ the maximal ideals of the rings of integers of E and F, and by k_E, k_F the residue class fields. We let I be the inertia group of F over E, and $m = \#I$; so m is the ramification index of F over E.
(a) Prove that the local reciprocity map $E^* \to \mathrm{Gal}(F/E)$ induces a surjective group homomorphism $k_E^* \to I$.
(b) Prove that E contains a primitive m-th root of unity.
(c) From 254A we know that there is an injective group homomorphism $I \to k_F^*$, which is induced by the k_F-linear action of I on the one-dimensional k_F-vector space $\mathfrak{p}_F/\mathfrak{p}_F^2$; so $\sigma \in I$ is sent to the image of $\sigma(\pi_F)/\pi_F$ in k_F^*, where π_F is any prime element of F.

Prove that the composed map $k_E^* \to I \to k_F^*$ sends every $x \in k_E^*$ to $x^{-\#k_E^*/m}$.
[*Hint.* Prove first that the composed map sends a unit $(u \bmod \mathfrak{p}_E)$ to the image of the norm residue symbol $(\pi_E, u)_m$ in k_F^*, where π_E is an arbitrary prime element of E.]