HOMEWORK SET 2

Local Class Field Theory - Fall 2011

I put the solutions just of the assigned exercises solved by at least one student in the class. For the other ones ask directly to me.
For questions, remarks or mistakes write me at lapoandrea@alice.it.

Exercise (Fesenko 8.1**).**

(a) *Let $A = \mathbb{F}_p[Z]/(Z^2)$. Show that*

$$F(X,Y) = X + Y + ZXY^p,$$

determines a noncommutative formal group over A.

Proof. It's easy to see that $F(X,0) = F(0,X) = 0$ and also that $F(X,Y)$ is not commutative in X and Y, so the formal group is not commutative.
Also the proof of the associativity is not complicated, indeed we have

$$\begin{aligned} F(F(X,Y),T) &= X + Y + ZXY^p + T + Z(X + Y + ZXY^p)T^p \\ &= X + (Y + T + ZYT^p) + ZX(Y + T + ZYT^p)^p \\ &= F(X, F(Y,T)); \end{aligned}$$

just using the fact that in A we have $Z^2 = 0$ and the property given by the characteristic $(Y + T + ZYT^p)^p = Y^p + T^p + (ZYT^p)^p$. □

(b) *Let A be a commutative ring with unity and let 2 be invertible in A. Show that*

$$F_\alpha(X,Y) = \frac{X\sqrt{(1-Y^2)(1-\alpha^2Y^2)} + Y\sqrt{(1-X^2)(1-\alpha^2X^2)}}{1+\alpha^2X^2Y^2}$$

with $\alpha \in A$, determines a formal group over A.

Proof. The condition on the invertibility of 2 allows us to define the power series of the square roots present in the expression. The denominator is a well defined power series since its leading coefficient is 1 so invertible in A.

This F_α as given in the text, with the " $+$ " at the denominator, is not a formal group, since we meet problems in proving the associativity.
To show that it's sufficient to take $A = \mathbb{C}$ and $\alpha = 1$. If we consider $F_1(X,Y) \in S^{-1}[X,Y] \subset \mathbb{C}[[X,Y]]$, where $S = 1 + (XY)$ we can view now $F_1(X,Y)$ as a rational function and compute its values for $(X,Y) \in \mathbb{C}^2$ (of course just for the values which don't annul the denominator). Thus, thanks to this remark, we see that

$$F_1(F_1(1,1),2) = F_1(0,2) = 2$$

while

$$F_1(1, F_1(1,2)) = F_1\left(1, -\frac{3}{5}\right) = \frac{8}{17};$$

contradicting the associativity (example given by Jacopo Griggio).

F_α does become a formal group if at the denominator we put a " $-$ ". For the computation proving the associativity in this case (without using Elliptic curves' theory), look at (Strickland, page 2). □

(*c*) *Let $F(X,Y) \in \mathbb{Z}[X,Y]$. Show that F determines a formal group over $\mathbb{Z}$ if and only if*

$$F(X,Y) = X + Y + \alpha XY$$

for some $\alpha \in \mathbb{Z}$.

Proof. ($\Leftarrow$) Easy, we have just to verify the three conditions defining a formal group.

($\Rightarrow$) (Solution by Dino Festi). Let $F(X,Y)$ be a formal group in $\mathbb{Z}[X,Y]$ (pay attention that we are working in the ring of polynomials in two variables), from its definition we know that $F(X,Y) = X + Y + XYG(X,Y)$, where $G(X,Y) \in \mathbb{Z}[X,Y]$.
Being in the ring of polynomial, we can define $deg_Y F(X,Y)$ as the highest power of Y in $F(X,Y)$ and in an analogous way $deg_Y G(X,Y)$, the same can be done with the variable X (note that $deg_Y F(X,Y) = 1 + deg_Y G(X,Y)$).
Now consider $F(F(X,X),Y)$ and $F(X,F(X,Y))$, they have to be equal thanks to associativity, but if we look at the degree with respect to Y we have:

$$deg_Y F(F(X,X),Y) = deg_Y F(X,Y),$$

while

$$deg_Y F(X, F(X,Y)) = \left(deg_Y F(X,Y)\right)^2.$$

Thus, in order to respect the associativity, we need for $deg_Y F(X,Y) = \left(deg_Y F(X,Y)\right)^2$ which implies $\deg_Y F(X,Y) = 1$. The same can be done with the variable X. So in conclusion we get $G(X,Y) = \alpha$, as we wanted to show.

□

Exercise (Fesenko 8.3). *Show that the homomorphism $O_K \longrightarrow End_{O_K}(F_f)$ of Proposition* (1.2) *is an isomorphism.*

Proof. In this exercise, unluckily, there is a big mistake at the root. The map of Proposition (1.2) is not well defined, since the $[\alpha]_F$, as defined there, can be not unique.
This is the right way to define that map:
Given $\alpha \in O_K$, we take $[\alpha]_F \in O_K[[X]]$ defined by

♡ $[\alpha]_F(X) \equiv \alpha X +$ terms of degree ≥ 2,

♡ $[\alpha]_F \circ f = f \circ [\alpha]_F$.

Then just now, thanks to the second property and using Lemma 2.11 of Milne, we have that this $[\alpha]_F$ is unique and that it belongs to $End_{O_K}(F_f)$ (look at Milne).
Thus we get a map $O_K \longrightarrow End_{O_K}(F_f)$ which is injective (since α is exactly the leading coefficient of $[\alpha]_F$) and surjective on its image (but not on all $End_{O_K}(F_f)$ as asserted by the exercise). It's not difficult to see that this map is really a ring homomorphism (look at Milne again). □

Exercise (Fesenko 8.5).

(a) *Let $f,\, g \in \mathcal{F}_\pi$. Show that κ_n associated to f is isomorphic to κ_n associated to g. Taking $g = \pi X + X^q$, show that $|\kappa_n| = q^n$.*

(b) *Let $\xi \in \kappa_n \backslash \kappa_{n-1}$. Using the map $O_K \longrightarrow \kappa_n,\ a \longrightarrow [a]_F(\xi)$ show that κ_n is isomorphic to $O_K/\pi^n O_K$.*

(c) *Using the map $O_K \longrightarrow End_{O_K}(\kappa_n),\ a \longrightarrow (\xi \longrightarrow [a]_F(\xi))$ show that $O_K/\pi^n O_K$ is isomorphic to $End_{O_K}(\kappa_n)$ and $U_K/U_{n,K}$ is isomorphic to $Aut_{O_K}(\kappa_n)$.*

Proof. This exercise was very easy because it's really a part of the theory explained by Milne. So give a look at Milne and I suggest you also the undergraduate senior thesis of Emily Riehl. □

Exercise (Fesenko 8.6). *Let $\xi \in \kappa_n \backslash \kappa_{n-1}$. Define the field of π^n-division points $L_n = K(\xi)$. Using exercise* 5 *show that L_n/K is a totally ramified abelian extension of degree $q^{n-1}(q-1)$, $N_{L_n/K}(-\xi) = \pi$ and $Gal(L_n/K)$ is isomorphic to $U_K/U_{n,K}$.*

Proof. Look at the proof of the previous exercise. □

Exercise (Lenstra 2.3). (Solution given by Valentin Zakharevich).

(*a*) *Let $K \subset L$ be a Galois extension of fields, with Galois group G. View G as a subset of the set L^L of all functions $L \longrightarrow L$. Let L be given the discrete topology and L^L the product topology. Prove that the topology of the profinite group G coincides with the relative topology inside L^L.*

Proof. Since under both topologies, G is a topological group, it suffices to show that the basis of the topologies at identity are the same. For the sake of simplifying notation, we will let G denote the Galois group with the profinite topology and G' the Galois group with the topology endowed from L^L.
We have that

$$G = \varprojlim_{i \in I} G_i$$

where $G_i = \text{Gal}(E_i/K)$ for $i \in I$ and E_i a finite Galois extension of K.
Let $f_i : G \to G_i$ be the natural projections. We have that the basis of G at id consists of sets of the form

$$\bigcap_{j \in J} f_j^{-1}(id_j)$$

where $J \subset I$ is a finite set. We can also see that $\bigcap_{j \in J} f_j^{-1}(id_j)$ is the set of elements of G which stabilize the field E_j for each $j \in J$. Thus we have

$$\bigcap_{j \in J} f_j^{-1}(id_j) = f_{J'}^{-1}(id_{J'})$$

where $J' \in I$ such that $E_{J'} = \prod_{j \in J} E_j$. This makes sense since the set J is finite. In other words the basis of G at id consists of sets of the form

$$f_i^{-1}(id_i)$$

for some $i \in I$.
Similarly the basis at id of G' consists of the sets of the form

$$\{g \in G' : \forall x \in L' \quad g(x) = x\}$$

where $L' \subset L$ is a finite set.
Now to show that G and G' have the same topology, we will show that given a basis element U at id of G, U is also a basis element of G' and vice versa.
Let $U = f_i^{-1}(id_i)$ where $i \in I$. We have that E_i is a finite Galois extension of K. In particular $E_i = K(\alpha_1, \ldots, \alpha_n)$. We then have

$$U = \{g \in G' : \forall x \in L' \quad g(x) = x\}$$

where $L' = \{\alpha_1, \ldots, \alpha_n\}$. On the other hand let $U = \{g \in G' : \forall x \in L' \quad g(x) = x\}$ where $L' = \{\alpha_1, \ldots, \alpha_n\}$. Then $U = f_i^{-1}(id_i)$ where $E_i = K(\alpha_1, \ldots, \alpha_n)$. □

(*b*) *Conversely, let L be any field and $G \subset Aut(L)$ a subgroup that is compact when viewed as a subset of L^L (topologized as in (a)). Prove that $L^G \subset L$ is Galois with Galois group G.*

Proof. To show that $L^G \subset L$ is Galois, we will show that every element of L is algebraic and separable over L^G whose minimal polynomial splits over L.
Let $\alpha \in L$. First we show that the orbit of α under G is finite. Let $f_\alpha : G \to L$ be the restriction of the projection from L^L onto its α coordinate. Then $G(\alpha) = f_\alpha(G)$. Since f_α is continuous, $f_\alpha(G)$ is compact and thus finite since L is given the discrete topology. Now consider the polynomial g, given by

$$g = \prod_{\beta \in G(\alpha)} (x - \beta).$$

Clearly $g \in L^G[X]$, is separable and splits over L. The minimal polynomial for α divides g and thus is also separable and splits over L. Thus $L^G \subset L$ is a Galois extension.
To see that $G = \mathrm{Gal}(L/L^G)$ we notice that G is naturally a subgroup of $\mathrm{Gal}(L/L^G)$. Since G is closed (compact in a Hausdorff and then use (a)), by the "main theorem of Galois theory", G corresponds to L^G, thus $G = \mathrm{Gal}(L/L^G)$. □

(*c*) *Prove that any profinite group is isomorphic to the Galois group of a suitably chosen Galois extension of fields.*

Proof. To find the desired field extension, we need to find a field L such that G acts faithfully on L and the map $G \hookrightarrow \mathrm{Aut}(L)$ is continuous. In this case G is isomorphic to a compact subgroup of $\mathrm{Aut}(L)$ and by (b) we can construct the desired field extension. Let

$$G = \varprojlim_{i \in I} G_i.$$

For $i \in I$ fixed, let g_{ij} be the elements of G_i. Fix some field F and let $L = F(\{g_{ij}\})$. We have that G acts faithfully on L (by permuting the "variables" of L). We need to show that $\phi : G \hookrightarrow \mathrm{Aut}(L)$ is continuous. Since both are topological groups, it suffices to show continuity at identity.
Let U be a basis element of $\mathrm{Aut}(L)$ at identity. By the same arguments as in (a), we see that there exist $\psi_1, \dots, \psi_n \in L$ such that

$$U = \{h \in \mathrm{Aut}(L) | \forall l \in \{1, \dots n\} \quad h(\psi_l) = \psi_l\}.$$

In particular both U and $\phi^{-1}(U)$ are subgroups and therefore to show that $\phi^{-1}(U)$ is open, by exercise 1.11 it suffices to prove that $\ker f_k \subset \phi^{-1}(U)$ for some $k \in I$ where $f_k : G \to G_k$ is the projection in the definition of G as a projective limit. Since each element ψ_l has only finitely many g_{ij} in its expressions, there exists $k \in I$ such that $G_k \geq G_i$ for any $i \in I$ such that some $g_{ij} \in G_i$ appears in the expression of some ψ_l. We then have the desired inclusion $\ker f_k \subset \phi^{-1}(U)$. □

Exercise (Lenstra 2.10). *A Steinitz number or supernatural number is a formal expression $a = \prod_p p^{a(p)}$, where $a(p) \in \{0, 1, 2, ..., \infty\}$ for each prime number p. If $a = \prod_p p^{a(p)}$ is a Steinitz number, we denote by $a\widehat{\mathbb{Z}}$ the subgroup of $\widehat{\mathbb{Z}}$ corresponding to $\prod_p p^{a(p)}\mathbb{Z}_p$ (with $p^\infty \mathbb{Z}_p = \{0\}$) under the isomorphism $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ (Exercise 1.14).*

(a) *Prove that the map $a \longrightarrow a\widehat{\mathbb{Z}}$ from the set of Steinitz numbers to the set of closed subgroups of $\widehat{\mathbb{Z}}$ is bijective. Prove also that $a\widehat{\mathbb{Z}}$ is open if and only if a is finite (i.e. $\sum_p a(p) < \infty$).*

Proof. **($a\widehat{\mathbb{Z}}$ is closed).** It suffices to show that $p^n\mathbb{Z}$ is a closed subgroup of $\mathbb{Z}_p$, then product of compact sets is compact and in a Hausdorff space it means to be closed, so using the isomorphism $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ we get that $a\widehat{\mathbb{Z}}$ is closed.

It's easy to see that $p^n\mathbb{Z}_p$ is closed in $\mathbb{Z}_p$, indeed

$$p^n\mathbb{Z}_p = \mathbb{Z}_p \cap \left(\prod_i p^n(\mathbb{Z}/p^i\mathbb{Z}) \right),$$

which is closed by exer. 1.11 of Lenstra.

(Injectivity). $\prod p^{a(p)}\mathbb{Z}_p = \prod p^{b(p)}\mathbb{Z}_p$ implies that for any p we have $p^{a(p)}\mathbb{Z}_p = p^{b(p)}\mathbb{Z}_p$, which means $a(p) = b(p)$ for any p.

(Surjectivity). (Solution by Johan Commelin) Let H be a closed subgroup of $\widehat{\mathbb{Z}}$ and let pr_p denote the projection $\widehat{\mathbb{Z}} \longrightarrow \mathbb{Z}_p$. Then $H_p = pr_p(H)$ is a subgroup of $\mathbb{Z}_p$. Moreover, by exer.1.11 of Lenstra, there exists a system of subgroups $(\rho_i \subset \mathbb{Z}/p^i\mathbb{Z})_{i\in\mathbb{N}}$ such that $H_p = \mathbb{Z}_p \cap \prod_{i\in\mathbb{N}} \rho_i$ inside $\prod_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$. It follows that

$$H_p = p^{\sup\{[\mathbb{Z}/p^i\mathbb{Z}:\rho_i]|i\in\mathbb{N}\}}\mathbb{Z}_p.$$

Thus we put $a(p) = \sup\{[\mathbb{Z}/p^i\mathbb{Z} : \rho_i]|i \in \mathbb{N}\}$ and with $a = \prod_p p^{a(p)}$ we obtain $a\widehat{\mathbb{Z}} = H$.

(Last point). Just use the fact that in a profinite group a subgroup is open iff it's closed of finite index (exer. 1.11).

□

(*b*) *Let $\mathbb{F}_q$ be a finite field, with algebraic closure $\overline{\mathbb{F}_q}$. For a Steinitz number a, let $\mathbb{F}_{q^a}$ be the set of all $x \in \overline{\mathbb{F}_q}$ for which $[\mathbb{F}_q(x) : \mathbb{F}_q]$ divides a (in an obvious sense). Prove that the map $a \longrightarrow \mathbb{F}_{q^a}$ is a bijection from the set of Steinitz numbers to the set of intermediate fields of $\mathbb{F}_q \subset \overline{\mathbb{F}_q}$. [Ernst Steinitz, German mathematician, 1871 − 1928.]*

Proof. **($\mathbb{F}_{q^a}$ is an intermediate field).** Given $x,\, y \in \mathbb{F}_{q^a}$ we know that

$$[\mathbb{F}_q(x,\, y) : \mathbb{F}_q] = \operatorname{lcm}\left([\mathbb{F}_q(x) : \mathbb{F}_q],\, [\mathbb{F}_q(y) : \mathbb{F}_q]\right) \text{ divides } a,$$

which implies that $\mathbb{F}_q(x,\, y) \in \mathbb{F}_{q^a}$.

(Bijection of the map). By infinite Galois Theory we know that there is a bijection between closed subgroups of $\widehat{\mathbb{Z}}$ ($a\widehat{\mathbb{Z}}$ by part (a)) and the intermediate field of $\mathbb{F}_q \subset \overline{\mathbb{F}_q}$. looking at the order and remembering that there is just one extension of finite degree a of $\mathbb{F}_q$ (property of finite fields) we know that, for a finite, $a\widehat{\mathbb{Z}}$ corresponds to $\mathbb{F}_{q^a}$.

If we take an arbitrary Steinitz number, then $\mathbb{F}_{q^a}$ is equal to the compositum of the finite extensions $E \subset \overline{\mathbb{F}_q}$ of $\mathbb{F}_q$, such that $[E : \mathbb{F}_q]$ divides a. We denote by I the set of these subfields, partially ordered by inclusion, then

$$Gal(\overline{\mathbb{F}_q}/\mathbb{F}_{q^a}) = \bigcap_{E\in I} Gal(\overline{\mathbb{F}_q}/E) = \bigcap_{E\in I} [E : \mathbb{F}_q]\widehat{\mathbb{Z}} = \bigcap_{i|a} i\widehat{\mathbb{Z}} = a\widehat{\mathbb{Z}},$$

as we wanted to show. This map is clearly a bijection, using the previous point and the Galois correspondence.

□

Exercise (Lenstra 2.11). *Let G be a profinite group. We call G procyclic if there exists $\sigma \in G$ such that the subgroup generated by σ is dense in G. Prove that the following assertions are equivalent:*

(*a*) *G is procyclic;*

(*b*) *G is the projective limit of a projective system of finite cyclic groups;*

(*c*) *$G = \widehat{\mathbb{Z}}/a\widehat{\mathbb{Z}}$ for some Steinitz number a (Exercise 2.10);*

(*d*) *for any pair of open subgroups $H,\, H' \subset G$ with index $[G : H] =$ index $[G : H']$ we have $H = H'$.*

Prove also that the Steinitz number a in (c) is unique if it exists.

Proof. Two initial remarks can be done:

♡ $\widehat{\mathbb{Z}}$ is a procyclic group generated by $(1)_{i\in\mathbb{N}}$.

♡ Any profinite group G is isomorphic to the inverse limit $\varprojlim G/N$ where N runs through the open normal subgroups of G of finite index (for a proof look for example at "Profinite Groups" by Ribes-Zalesskii, Theorem 2.1.3). So we can consider the morphisms $f_{i,j}$'s and the projections π_i's surjective.

$((a) \Rightarrow (c))$. We consider the group morphism $\phi : \widehat{\mathbb{Z}} \longrightarrow G$ which sends $1 \longrightarrow \sigma$, it's not difficult to see that it's continuous. Since $\widehat{\mathbb{Z}}$ is compact and G is Hausdorff, $\phi(\widehat{\mathbb{Z}})$ is closed and contains $\langle\sigma\rangle$, which implies that ϕ is surjective. Since the kernel is closed, we know by the exercise 2.10 that there exists a unique Steinitz number such that $\widehat{\mathbb{Z}}/a\widehat{\mathbb{Z}} \cong G$.

$((c) \Rightarrow (d))$. We consider the natural quotient map $q : \widehat{\mathbb{Z}} \longrightarrow \widehat{\mathbb{Z}}/a\widehat{\mathbb{Z}}$, then $q^{-1}(H)$ and $q^{-1}(H')$ are open subgroups of $\widehat{\mathbb{Z}}$ (and so they are closed of finite index). Since they have common index, by the unicity given by exercise 2.10 we have $H = H'$.

$((d) \Rightarrow (b))$. We consider as explained in the initial remarks $G = \varprojlim G/N$. Let fix N and consider two open subgroups K, K' of G/N with the same index. Then $K = H/N$ and $K' = H'/N$ for some H, H' opens in G, then looking at the index we obtain $[G : H] = [G : H']$ and so $H = H'$, which implies $K = K'$. Since a group of order n is cyclic if and only if for every divisor d of n the group has at most one subgroup of order d (Wikipedia - Cyclic groups, but you can find it also in any book of Group Theory), we get that for any N, the group G/N is cyclic as we wanted to show.

$((b) \Rightarrow (a))$. If $G = \varprojlim G_i$, with G_i cyclic, we call S_i the set of generators for the group G_i. Then the S_i form a projective system thanks to the surjectivity of the $f_{i,j}$'s (we can assume it as before) and their inverse limit is not empty since they are finite and not empty (Exer. 1.9 of Lenstra). So now we can say that there exists an element σ of G given by $\sigma = (\sigma_1, \sigma_2, \dots)$, where each σ_i is a generator of G_i. Now it's not difficult to see that any open subset of G has not trivial intersection with $\langle\sigma\rangle$, and so $\langle\sigma\rangle$ is really dense in G.

□

Exercise (Lenstra 2.13**).**

(*a*) *Let E be a torsion abelian group. prove that E has exactly one $\widehat{\mathbb{Z}}$-module structure and that the scalar multiplication $\widehat{\mathbb{Z}} \times E \longrightarrow E$ defining this module structure is continous, if E is given the discrete topology.*

Proof. (Solution given by Milan Lopuhaä) Given an element $a = (a_i) \in \widehat{\mathbb{Z}}$ we make it acting on an element x of E of order n as

$$a.x = x^{a_n}.$$

It's not difficult to see that this does give a $\widehat{\mathbb{Z}}$-module structure.

To see that this structure has to be unique, we have just to remark that on an element x of order n we have a trivial action of $n\widehat{\mathbb{Z}}$ and so the action of $\widehat{\mathbb{Z}}$ on it is just defined by the action of the abelian group $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$ which in turn is uniquely determined by the action of $\mathbb{Z}$ (which is clearly unique).

The map $\widehat{\mathbb{Z}} \times E \longrightarrow E$ is continuos since E has the discrete topology and the inverse image of $e = ze'$ is given by $(z + n\widehat{\mathbb{Z}}) \times e'$ (where n is the order of e), which is open in the product topology of $\widehat{\mathbb{Z}} \times E$.

□

(*b*) *Let E be the group of roots of unity in $\bar{\mathbb{Q}}^{\times}$. Prove that the map $\widehat{\mathbb{Z}}^{\times} \longrightarrow Aut(E)$ induced by (a) is an isomorphism of groups.*

Proof. (Solution given by Milan Lopuhaä) If a, $b \in \widehat{\mathbb{Z}}$ differ in their $\mathbb{Z}/n\mathbb{Z}$-coordinate, then their action on ζ_n differs, so the map is injective.
To prove the surjectivity we really construct the inverse map as follows. If we have $\sigma \in \mathrm{Aut}(E)$, then we define an element $h = (h_n) \in \prod_n \mathbb{Z}/n\mathbb{Z}$ by saying that $h_n = k$ if $\sigma(\zeta_n) = \zeta_n^k$. Then if $d|n$, then $\sigma(\zeta_d) = \sigma(\zeta_n^{\frac{n}{d}}) = \zeta_n^{\frac{kn}{d}} = \zeta_d^k$, so $h_n \equiv h_d \bmod d$, so $h \in \widehat{\mathbb{Z}}$.
It's easy to see that this is really the inverse map of the given one. □

(*c*) *Write $\mathbb{Q}(\zeta_\infty) = \mathbb{Q}(E)$, with E as in (b). Prove that $\mathbb{Q} \subset \mathbb{Q}(\zeta_\infty)$ is Galois and that the natural map $Gal(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \longrightarrow Aut(E) \cong \widehat{\mathbb{Z}}^{\times}$ is an isomorphism of topological groups.*

Proof. We know that

$$\mathbb{Q}(\zeta_\infty) = \mathbb{Q}(E) = \bigcup_{n \in \mathbb{N}} \mathbb{Q}(\zeta_n)$$

(where ζ_n is a primitive n-th root of unity), so, by Theorem 2.2 of Lenstra ,we have that this extension is Galois over $\mathbb{Q}$ and also that

$$\mathrm{Gal}\left(\mathbb{Q}(E)/\mathbb{Q}\right) \cong \varprojlim \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right).$$

So it remains to prove that

$$\varprojlim \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong \mathrm{Aut}(E)$$

and this is given by

$$\begin{aligned} \mathrm{Aut}(E) &\cong \varprojlim \mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right), \\ \mathrm{Aut}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) &= \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right). \end{aligned}$$

All the previous isomorphisms are indeed isomorphisms of topological groups. □

(d) *Prove that there are isomorphisms*

$$\widehat{\mathbb{Z}}^\times \cong \prod_{p\ prime} \mathbb{Z}_p^\times \cong \widehat{\mathbb{Z}} \times (\mathbb{Z}/2\mathbb{Z}) \times \prod_{p\ prime} (\mathbb{Z}/(p-1)\mathbb{Z})$$

of topological groups.

Proof. We have just to observe that we have the following topological group isomorphisms:

$$\mathbb{Z}_p^\times \cong \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p, & p > 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2, & p = 2 \end{cases}$$

and remember of the isomorphism

$$\widehat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

□