Answersheet 12 - Yiwei Yang 2018533218

1.

Since $[E_1E_2 : k] = [E_1E_2 : L_1]\,[L_2 : k]$, it suffices to show $[E_1E_2 : E_1] \leq [E_2 : k]$. Let $\{e_i\}$ be a k -basis of E_2. Since the E_j 's are finite algebraic over k, E_1E_2 consists of polynomials in elements of E_2 with coefficients in E_1, so E_1E_2 is spanned by the $\{e_i\}$ over E_1 (but possibly with linear dependence relations).

2.

a.

First prove that the intersection is finite if it's non-empty.

By contradiction, suppose $\cap_{n\in N} A_n = \phi$. For each $x \in A_1$ let $f(x)$ be the least $n \in N$ such that $x \notin A_n$. Then $B = \{f(x) : x \in A_1\}$ is a finite subset of N, so there exists $m \in N$ such that $\forall n \in B(m \geq n)$ For such an m, we have $\forall x \in A_1\ (x \notin A_m)$ because $\forall x \in A_1 \left(x \notin A_{f(x)} \supset \cap_{j=f(x)}^{m} A_j \supset A_m\right)$. But then $A_m \cap A_1 = \phi$, contradicting $\phi \neq A_m \subset \cap_{j=1}^{m} A_j \subset A_1$.

Then prove that there's a bijection between profinite group of A and extending sequence A_n of finite primary groups belong to C_I is that A_n be regular

Proof. Again, it is immediate that the condition is necessary. In fact, one needs only to make the obvious replacements in the proof of Theorem 1. Recall that $\sum \oplus$, the direct sum, should be replaced by $\sum' \oplus$, the complete direct sum, and the group of type p^{∞} by the p -adic group.

Denote by A^* the (discrete) character group of A. With an inverse sequence

$$A_1 \leftarrow A_2 \leftarrow \cdots \leftarrow A_n \leftarrow \cdots \tag{1}$$

there is associated in a natural way a (unique) direct sequence

$$A_1^* \rightarrow A_2^* \rightarrow \cdots \rightarrow A_n^* \rightarrow \cdots \tag{2}$$

which in turn gives rise to an inverse sequence

$$A1^{**} \leftarrow A_2^{**} \leftarrow \cdots \leftarrow A_n^{**} \leftarrow \cdots \tag{3}$$

Together with the usual isomorphism between A_n and A_n^{**}, (1) and (3) form a commutative diagram and therefore have isomorphic limits. However, the limit of (3) is the character group of the limit of (2). Thus if A_n is regular, the limit of (1) is determined by the groups alone and $A_n \in C_I$.

Now let A_n be an extending sequence of finitely generated groups. Analogous to the p -rank of a sequence, the torsion free rank of the sequence A_n is defined as the limit of the torsion free ranks of the groups $A_n, r_0 = \lim_{n\to\infty} r_0\left(A_n\right)$. The question of whether or not A_n is contained in C_I depends to a large degree on whether r_0 is finite or not; consequently, the two cases are distinguished.

Reference: Hill, Paul. "Limits of sequences of finitely generated abelian groups." *Proceedings of the American Mathematical Society*12.6 (1961): 946-950.

b.

The elements of $\hat{\mathbb{Z}}$ have very explicit descriptions in terms of compatible sequences $(x_i)_{i\in\mathbb{N}}$ where each $x_i \in \mathbb{Z}/i\mathbb{Z}$. Note that $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

Show that the equation $x^2 = 2$ has a solution in $\mathbb{Z}_7$ where: $\mathbb{Z}_7 = \overset{\lim}{\longleftarrow} A_n, (A_n = \mathbb{Z}/7^n\mathbb{Z})$

Consider the polynomial $f(x)$=x2−2f(x)=x2−2, check that there is some a∈$\mathbb{Z}$/7$\mathbb{Z}$a∈Z/7Z such that $f(a)$=0f(a)=0 but $f'(a)$≠0f'(a)≠0, and apply Hensel's Lemma.

Proof of Hensel's Lemma: If $f(X) \in \mathbf{Z}_p[X]$ and $a \in \mathbf{Z}_p$ satisfies: $f(a) \equiv 0\ mod\ p$, $f'(a) \not\equiv 0\ mod\ p$. then there is a unique $\alpha \in \mathbf{Z}_p$ such that $f(\alpha) = 0$ in $\mathbf{Z}_p$ and $\alpha \equiv a \bmod p$.

We will prove by induction that for each $n \geq 1$ there is an $a_n \in \mathbf{Z}_p$ such that

- $f(a_n) \equiv 0 \bmod p^n$
- $a_n \equiv a \bmod p$.

Since $f(a_{n+1}) \equiv 0 \bmod p^{n+1} \Rightarrow f(a_{n+1}) \equiv 0 \bmod p^n$, each root of $f(X) \bmod p^{n+1}$ reduces to a root of $f(X) \bmod p^n$. By the inductive hypothesis there is a root $a_n \bmod p^n$, so we seek a p-adic integer a_{n+1} such that $a_{n+1} \equiv a_n \bmod p^n$ and $f(a_{n+1}) \equiv 0 \bmod p^{n+1}$. Writing $a_{n+1} = a_n + p^n t_n$ for some $t_n \in \mathbf{Z}_p$ to be determined, can we make $f(a_n + p^n t_n) \equiv 0 \bmod p^{n+1}$?
To compute $f(a_n + p^n t_n) \bmod p^{n+1}$, we use a polynomial identity:
(2.1)

$$f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2 \tag{4}$$

for some polynomial $g(X,Y) \in \mathbf{Z}_p[X,Y]$. This formula comes from isolating the first two terms in the binomial theorem: writing $f(X) = \sum_{i=0}^d c_i X^i$ we have

$$f(X+Y) = \sum_{i=0}^d c_i (X+Y)^i = c_0 + \sum_{i=1}^d c_i \left(X^i + iX^{i-1}Y + g_i(X,Y)Y^2\right) \tag{5}$$

where $g_i(X,Y) \in \mathbf{Z}[X,Y]$. Thus

$$f(X+Y) = \sum_{i=0}^d c_i X^i + \sum_{i=1}^d i c_i X^{i-1} Y + \sum_{i=1}^d g_i(X,Y)Y^2 = f(X) + f'(X)Y + g(X,Y)Y^2 \tag{6}$$

where $g(X,Y) = \sum_{i=1}^d c_i g_i(X,Y) \in \mathbf{Z}_p[X,Y]$. This gives us the desired identity. [1] To make (2.1) numerical, for all x and y in $\mathbf{Z}_p$ the number $z := g(x,y)$ is in $\mathbf{Z}_p$, so
(2.2)
$x, y \in \mathbf{Z}_p \Longrightarrow F(x+y) = f(x) + f'(x)y + zy^2$, where $z \in \mathbf{Z}_p$
In this formula set $x = a_n$ and $y = p^n t_n$:
(2.3)
$f(a_n + p^n t_n) = f(a_n) + f'(a_n) p^n t_n + z p^{2n} t_n^2 \equiv f(a_n) + f'(a_n) p^n t_n \bmod p^{n+1}$
since $2n \geq n+1$. In $f'(a_n) p^n t_n \bmod p^{n+1}$, the factors $f'(a_n)$ and t_n only matter mod p since there is already a factor of p^n and the modulus is p^{n+1}. Recalling that $a_n \equiv a \bmod p$ we get $f'(a_n) p^n t_n \equiv f'(a) p^n t_n \bmod p^{n+1}$. Therefore from (2.3),

$$\begin{aligned} f(a_n + p^n t_n) \equiv 0 \bmod p^{n+1} &\Longleftrightarrow f(a_n) + f'(a) p^n t_n \equiv 0 \bmod p^{n+1} \\ &\Longleftrightarrow f'(a) t_n \equiv -f(a_n)/p^n \bmod p \end{aligned}$$

where the ratio $f\left(a_n\right) / p^n$ is in $\mathbf{Z}_p$ since we assumed that $f\left(a_n\right) \equiv 0 \bmod p^n$. There is a solution for t_n in the congruence $\bmod p$ since we assumed that $f^{\prime}(a) \not\equiv 0 \bmod p$.

Armed with this choice of t_n and setting $a_{n+1}=a_n+p^n t_n$, we have $f\left(a_{n+1}\right) \equiv 0 \bmod p^{n+1}$ and $a_{n+1} \equiv a_n \bmod p^n$, so in particular $a_{n+1} \equiv a \bmod p$. This completes the induction. Starting with $a_1=a$, our inductive argument has constructed a sequence $a_1, a_2, a_3, \ldots$ in $\mathbf{Z}_p$ such that $f\left(a_n\right) \equiv 0 \bmod p^n$ and $a_{n+1} \equiv a_n \bmod p^n$ for all n. The second condition, $a_{n+1} \equiv a_n \bmod p^n$, implies that $\left\{a_n\right\}$ is a Cauchy sequence in $\mathbf{Z}_p$. Let α be its limit in $\mathbf{Z}_p$. We want to show $f(\alpha)=0$ and $\alpha \equiv a \bmod p$ From $a_{n+1} \equiv a_n \bmod p^n$ for all n we get $a_m \equiv a_n \bmod p^n$ for all $m>n$, so $\alpha \equiv a_n \bmod p^n$ by letting $m \rightarrow \infty$. At $n=1$ we get $\alpha \equiv a \bmod p$. For general n,

$$\alpha \equiv a_n \bmod p^n \Longrightarrow f(\alpha) \equiv f\left(a_n\right) \equiv 0 \bmod p^n \Longrightarrow|f(\alpha)|_p \leq \frac{1}{p^n} \tag{7}$$

Since this estimate holds for all n, $f(\alpha)=0$.

It remains to show α is the unique root of $f(X)$ in $\mathbf{Z}_p$ that is congruent to $a \bmod p$. Suppose $f(\beta)=0$ and $\beta \equiv a \bmod p$. To show $\beta=\alpha$ we will show $\beta \equiv \alpha \bmod p^n$ for all n. The case $n=1$ is clear since α and β are both congruent to $a \bmod p$. Suppose $n \geq 1$ and we know that $\beta \equiv \alpha \bmod p^n$. Then $\beta=\alpha+p^n \gamma_n$ with $\gamma_n \in \mathbf{Z}_p$, so a calculation similar to implies

$$f(\beta)=f\left(\alpha+p^n \gamma_n\right) \equiv f(\alpha)+f^{\prime}(\alpha) p^n \gamma_n \bmod p^{n+1} \tag{8}$$

Both α and β are roots of $f(X)$, so $0 \equiv f^{\prime}(\alpha) p^n \gamma_n \bmod p^{n+1}$. Thus $f^{\prime}(\alpha) \gamma_n \equiv 0 \bmod p$. Since $f^{\prime}(\alpha) \equiv f^{\prime}(a) \not\equiv 0 \bmod p$, we have $\gamma_n \equiv 0 \bmod p$, which implies $\beta \equiv \alpha \bmod p^{n+1}$.

3.

Let $f \in F[X]$ be the irreducible polynomial of α. The degree of f is odd. Let $f=X^d+f_{d-1} x^{d-1}+\cdots+f_0, f_i \in F$. Then. we have $\alpha^d+f_{d-1} \alpha^{d-1}+\cdots+f_0=0$. Seperate the even and odd powers. We can see that there exists $h, g \in F[X]$ with h monic, such that, $\alpha h\left(\alpha^2\right)=g\left(\alpha^2\right)$. This shows that, $\alpha \in F\left(\alpha^2\right)$ and hence $F(\alpha)=F\left(\alpha^2\right)$.

4.

Proof. There is an obvious embedding of Y into $\underline{\lim}_i\left(\varphi_i(Y)\right)$. Since Y is compact and Hausdorff, the previous corollary implies that the induced mapping of Y to $\lim \left(\varphi_i(Y)\right)$ is onto, and by uniqueness this mapping is the afore mentioned embedding in (i). Thus we find that $Y=\lim_{\underline{L}}\left(\varphi_i(Y)\right)$