The function $n \longmapsto \left(\frac{d}{n}\right)$

Fix a square-free integer $d \in \mathbb{Z} \setminus \{0\}$. The Jacobi symbol $\left(\frac{d}{n}\right)$ is defined for all $n \in \mathbb{N}_+$ relatively prime to $2d$. However, the reciprocity law $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$ allows us to extend the definition of $n \mapsto \left(\frac{d}{n}\right)$ to a larger set of integers, while preserving the multiplicativity property $\left(\frac{d}{n_1 n_2}\right) = \left(\frac{d}{n_1}\right)\left(\frac{d}{n_2}\right)$. Most astonishingly, the value of this extended function will depend only on the residue class of n modulo a suitable integer depending on d.

Ex 1. $(d=-1)$ $\left(\frac{-1}{n}\right)$ is defined for $n \geq 1$ relatively prime to 2.

For such n we have $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1, & n \equiv 1\,[4] \\ -1, & n \equiv 3\,[4]. \end{cases}$

The expression $(-1)^{\frac{n-1}{2}}$ is defined for $n \in \mathbb{Z}$ relatively prime to 2, depends only on $n \pmod 4$, and satisfies $(-1)^{\frac{mn-1}{2}} = (-1)^{\frac{m-1}{2}}(-1)^{\frac{n-1}{2}}$.

Ex 2. $(d=-3)$ $\left(\frac{-3}{n}\right)$ is defined for $n \geq 1$ relatively prime to 6.

For such n we have $\left(\frac{-3}{n}\right) = \left(\frac{n}{3}\right) = \begin{cases} 1, & n \equiv 1\,[3] \\ -1, & n \equiv 2\,[3]. \end{cases}$

The expression $\left(\frac{n}{3}\right)$ is defined for $n \in \mathbb{Z}$ relatively prime to 3, depends only on $n \pmod 3$, and satisfies $\left(\frac{n_1 n_2}{3}\right) = \left(\frac{n_1}{3}\right)\left(\frac{n_2}{3}\right)$.

Ex 3. $(d=5)$ $\left(\frac{5}{n}\right)$ is defined for $n \geq 1$ relatively prime to 10.

For such n we have $\left(\frac{5}{n}\right) = \left(\frac{n}{5}\right) = \begin{cases} 1, & n \equiv \pm 1\,[5] \\ -1, & n \equiv \pm 2\,[5]. \end{cases}$

The expression $\left(\frac{n}{5}\right)$ is defined for $n \in \mathbb{Z}$ relatively prime to 5, depends only on $n \pmod 5$, and satisfies $\left(\frac{n_1 n_2}{5}\right) = \left(\frac{n_1}{5}\right)\left(\frac{n_2}{5}\right)$.

Ex 4. $(d=-5)$ $\left(\frac{-5}{n}\right)$ is defined for $n \geq 1$ relatively prime to 10.

For such n we have $\left(\frac{-5}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{5}{n}\right) = (-1)^{\frac{n-1}{2}}\left(\frac{n}{5}\right)$. The expression $(-1)^{\frac{n-1}{2}}\left(\frac{n}{5}\right)$ is defined for $n \in \mathbb{Z}$ relatively prime to 10, depends only on $n \pmod{20}$, and satisfies $(-1)^{\frac{mn-1}{2}}\left(\frac{mn}{5}\right) = (-1)^{\frac{m-1}{2}}\left(\frac{m}{5}\right)(-1)^{\frac{n-1}{2}}\left(\frac{n}{5}\right)$.

Explicitly, $\left(\frac{-5}{n}\right) = 1$ is equivalent to

$$\left\{ \begin{array}{l} \left(\frac{-1}{n}\right) = \left(\frac{5}{n}\right) = 1 \iff n \equiv 1\,[4] \text{ and } n \equiv \pm 1\,[5] \iff n \equiv 1, 9\,[20] \\ \text{or} \\ \left(\frac{-1}{n}\right) = \left(\frac{5}{n}\right) = -1 \iff n \equiv 3\,[4] \text{ and } n \equiv \pm 2\,[5] \iff n \equiv 3, 7\,[20] \end{array} \right\},$$

$$\text{hence } \left(\frac{-5}{n}\right) = \left\{ \begin{array}{ll} 1, & n \equiv 1, 3, 7, 9\,[20] \\ -1, & n \equiv 11, 13, 17, 19\,[20] \end{array} \right\}.$$

The general case goes as follows (χ_D below is the Kronecker symbol)

Exercise. Let $d \in \mathbb{Z} \setminus \{0,1\}$ be a square-free integer. Writing $d = \pm 2^s q_1^* \cdots q_r^*$ ($q_i \neq 2$ prime, $q_i^* = (-1)^{\frac{q_i-1}{2}} q_i$) and applying the reciprocity law for the Jacobi symbol, show that there is a unique map $\chi_D : (\mathbb{Z}/|D|\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ (where $D = \begin{cases} d, & d \equiv 1 \,[4] \\ 4d, & d \equiv 2, 3 \,[4] \end{cases}$) such that

(i) $\left(\frac{d}{n}\right) = \chi_D(n \pmod{|D|})$ if $n \in \mathbb{N}_+$ is relatively prime to $2d$.

(ii) $\chi_D(ab) = \chi_D(a)\chi_D(b)$.

[The notation χ_D is justified by the fact that $d \neq d' \Rightarrow D \neq D'$.

Moreover, $|D| \geq 1$ is the smallest positive integer with the above property.

Analytic formulation of unique factorisation (continued)

Recall: ① UFD property of $\mathbb{Z}$ is equivalent to

$$\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}=\prod_{p\in P}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots\right)=\prod_{p\in P}\left(1-\frac{1}{p^s}\right)^{-1}$$

② UFD property of $\mathbb{Z}[i]$ is equivalent to

$$\sum_{\alpha\in(\mathbb{Z}[i]\setminus\{0\})/\mathbb{Z}[i]^\times}\frac{1}{N(\alpha)^s}=\prod_{\pi\in\mathbb{Z}[i]_{irr}/\mathbb{Z}[i]^\times}\left(1-\frac{1}{N(\pi)^s}\right)^{-1}=\left(1-\frac{1}{2^s}\right)^{-1}\prod_{p\equiv 1[4]}\left(1-\frac{1}{p^s}\right)^{-2}\prod_{p\equiv 3[4]}\left(1-\frac{1}{p^{2s}}\right)^{-1}$$

$$=\zeta(s)\prod_{p\in P\setminus\{2\}}\left(1-\left(\frac{-1}{p}\right)\frac{1}{p^s}\right)^{-1}$$

$$L\left(\left(\tfrac{-1}{\cdot}\right),s\right)=\sum_{\substack{n\geq 1\\ 2\nmid n}}\left(\frac{-1}{n}\right)\frac{1}{n^s}=\sum_{\substack{n\geq 1\\ 2\nmid n}}(-1)^{\frac{n-1}{2}}\frac{1}{n^s}$$

$$\frac{1}{4}\sum_{(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\}}\frac{1}{(x^2+y^2)^s}$$

As a result, $r_{x^2+y^2}(n)=\left|\{(x,y)\in\mathbb{Z}^2 \mid x^2+y^2=n\}\right|$ is given by the formula

$$\frac{1}{4}r_{x^2+y^2}(n)=\sum_{2\nmid d\mid n}\left(\frac{-1}{d}\right)=\prod_{\substack{p\mid n\\ p\neq 2}}\sum_{j=0}^{v_p(n)}\left(\frac{-1}{p}\right)^j=\prod_{p\equiv 1[4]}(1+v_p(n))\prod_{p\equiv 3[4]}\begin{cases}1, & 2\mid v_p(n)\\ 0, & 2\nmid v_p(n)\end{cases}$$

Ex. $\mathbb{Z}[\xi_3]$ $\left(\xi_3=e^{2\pi i/3}=\frac{-1+i\sqrt{3}}{2}\right)$ is a UFD, $\alpha=u+v\xi_3$ $u,v\in\mathbb{Z}$

$N(\alpha)=\alpha\bar{\alpha}=u^2-uv+v^2$

$\mathbb{Z}[\xi_3]^\times=\{\pm 1,\pm\xi_3,\pm\xi_3^2\}$

$\mathbb{Z}[\xi_3]_{irr}/\mathbb{Z}[\xi_3]^\times=\{\underbrace{\xi_3-\xi_3^2}_{i\sqrt{3}}\}\cup\{p \mid p\equiv 2[3]\}\cup\{\pi_p,\overline{\pi_p} \mid \pi_p\overline{\pi_p}=p\equiv 1[3]\}$

As in ② above,

$$\sum_{\alpha\in(\mathbb{Z}[\xi_3]\setminus\{0\})/\mathbb{Z}[\xi_3]^\times}\frac{1}{N(\alpha)^s}=\prod_{\pi\in\mathbb{Z}[\xi_3]_{irr}/\mathbb{Z}[\xi_3]^\times}\left(1-\frac{1}{N(\pi)^s}\right)^{-1}=\left(1-\frac{1}{3^s}\right)^{-1}\prod_{p\equiv 1[3]}\left(1-\frac{1}{p^s}\right)^{-2}\prod_{p\equiv 2[3]}\left(1-\frac{1}{p^{2s}}\right)^{-1}=$$

$$=\zeta(s)\prod_{p\in P\setminus\{3\}}\left(1-\underbrace{\left(\frac{p}{3}\right)}_{\left(\frac{-3}{p}\right)}\frac{1}{p^s}\right)^{-1}$$

Therefore

$$L\left(\left(\tfrac{\cdot}{3}\right),s\right)=\sum_{\substack{n\geq 1\\ 3\nmid n}}\left(\frac{n}{3}\right)\frac{1}{n^s}$$

$$\frac{1}{6}r_{x^2-xy+y^2}(n)=\sum_{3\nmid d\mid n}\left(\frac{d}{3}\right)=\prod_{\substack{p\mid n\\ p\equiv 1[3]}}(1+v_p(n))\cdot\prod_{p\equiv 2[3]}\begin{cases}1, & 2\mid v_p(n)\\ 0, & 2\nmid v_p(n)\end{cases}$$

Ex. the ring $\mathbb{Z}[i\sqrt{5}] = \{\alpha = u + iv\sqrt{5} \mid u, v \in \mathbb{Z}\}$ is NOT a UFD:

$2 \cdot 3 = 6 = (1+i\sqrt{5})(1-i\sqrt{5})$, $3 \cdot 7 = 21 = (4+i\sqrt{5})(4-i\sqrt{5})$

All elements $2, 3, 7, 1 \pm i\sqrt{5}, 4 \pm i\sqrt{5}$ are irreducible in $\mathbb{Z}[i\sqrt{5}]$

We have $N(\alpha) = \alpha\bar{\alpha} = u^2 + 5v^2$, hence $\mathbb{Z}[i\sqrt{5}]^\times = \{\pm 1\}$.

Question: is there a relation between

$$\frac{1}{2} \sum_{(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}} \frac{1}{(x^2+5y^2)^s} = \sum_{\alpha \in (\mathbb{Z}[i\sqrt{5}] \setminus \{0\}) / \mathbb{Z}[i\sqrt{5}]^\times} \frac{1}{N(\alpha)^s} = \frac{1}{2} \sum_{n \geq 1} \frac{r_{x^2+5y^2}(n)}{n^s} \quad \text{and}$$

$$\underbrace{\zeta(s) L\left(\left(\frac{-5}{\cdot}\right), s\right)}_{\sum_{n \geq 1} \frac{a(n)}{n^s}}, \quad \text{where } L\left(\left(\frac{-5}{\cdot}\right), s\right) = \sum_{\substack{n \geq 1 \\ (n,10)=1}} \left(\frac{-5}{n}\right) \frac{1}{n^s} = \prod_{p \neq 2,5} \left(1 - \left(\frac{-5}{p}\right) \frac{1}{p^s}\right)^{-1}$$

$\left(\frac{-1}{d}\right)\left(\frac{d}{5}\right)$

As above, $a(n) = \sum_{\substack{d \mid n \\ (d,10)=1}} \left(\frac{-5}{d}\right) = \prod_{p \mid n} (1 + v_p(n)) \prod_{p \mid n} \begin{cases} 1, & 2 \mid v_p(n) \\ 0, & 2 \nmid v_p(n) \end{cases}$.

$\left(\frac{-5}{p}\right) = 1$ $\qquad$ $\left(\frac{-5}{p}\right) = -1$

In particular, for a prime $p \neq 2, 5$,

$$a(p) = \begin{cases} 2, & \left(\frac{-5}{p}\right) = 1 \iff \left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = 1 \text{ or } \left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = -1 \\ 0, & \left(\frac{-5}{p}\right) = -1 \end{cases}$$

On the other hand, if $n \in \mathbb{N}_+$ is relatively prime to 10 and $r_{x^2+5y^2}(n) \neq 0$, then $n = x^2 + 5y^2$ $(x, y \in \mathbb{Z}) \equiv x^2 \equiv \pm 1 \,[5] \Rightarrow \left(\frac{n}{5}\right) = 1$

$\equiv x^2 + y^2 \equiv 1 \,[4] \Rightarrow \left(\frac{-1}{n}\right) = 1$.

Conclusion: for $p \neq 2, 5$

$r_{x^2+5y^2}(p) \neq 0 \Rightarrow \left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = 1$ $\qquad$ $(\iff p \equiv 1, 9 \,[20])$

$a(p) \neq 0 \iff \left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = 1$ or $\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = -1$

$\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = -1 \iff p \equiv 3, 7 \,[20]$

So $\sum \frac{1}{N(\alpha)^s}$ does not contain the terms $\frac{1}{p^s}$ for p satisfying $p \equiv 3, 7 \,[20]$!!

What is going on? We need to convert the condition $\left(\frac{-1}{p}\right) = \left(\frac{p}{5}\right) = -1$ into $\left(\frac{-1}{n}\right) = \left(\frac{n}{5}\right) = 1$. This can be done by choosing $q \in \mathbb{P}$ such that $\left(\frac{-1}{q}\right) = \left(\frac{q}{5}\right) = -1$ and letting $n = pq$. Then there will be a chance of n being of the form $x^2+5y^2 = N(x+iy\sqrt{5})$.

The simplest choice is $q = 3$.

When is $3 \mid (x^2+5y^2)$, $x, y \in \mathbb{Z}$?

$3 \mid (x^2+5y^2) \iff 3 \mid (x^2-y^2) = (x-y)(x+y) \iff x \equiv \pm y \,[3] \iff x = 3u \pm y.$

In this case $\frac{x^2+5y^2}{3} = \frac{(3u \pm y)^2+5y^2}{3} = 3u^2 \pm 2uy + 2y^2.$

So we should also consider a contribution from $3x^2+2xy+2y^2$:

Improved question: is there a relation between

$$(*) \quad \frac{1}{2} \sum_{(x,y) \in \mathbb{Z}^2 - \{(0,0)\}} \frac{1}{(x^2+5y^2)^s} + \frac{1}{2} \sum_{(x,y) \in \mathbb{Z}^2 - \{(0,0)\}} \frac{1}{(3x^2+2xy+2y^2)^s} = \frac{1}{2} \sum_{n \geq 1} \frac{r_{x^2+5y^2}(n) + r_{3x^2+2xy+2y^2}(n)}{n^s}$$

and $\zeta(s) L\left(\left(\frac{-5}{\cdot}\right), s\right)$?

Answer: Yes! the two expressions are equal to each other! In addition,

$$\frac{1}{2} \sum \frac{1}{(x^2+5y^2)^s} - \frac{1}{2} \sum \frac{1}{(3x^2+2xy+2y^2)^s} = \underbrace{L\left(\left(\frac{-1}{\cdot}\right), s\right)}_{\sum_{n \geq 1} \left(\frac{-1}{n}\right) \frac{1}{n^s}} \underbrace{L\left(\left(\frac{5}{\cdot}\right), s\right)}_{\sum_{\substack{n \geq 1 \\ 5 \nmid n}} \left(\frac{5}{n}\right) \frac{1}{n^s}}$$

This is the simplest example of genus theory for binary quadratic forms in action.

A most puzzling question: how can one express the sum $(*)$ in terms of the ring $\mathbb{Z}[i\sqrt{5}]$? The fact that this sum is equal to $\zeta(s) L\left(\left(\frac{-5}{\cdot}\right), s\right)$ seems to be suggesting that there is some kind of unique factorisation lurking behind, even though unique factorisation fails in $\mathbb{Z}[i\sqrt{5}]$.

This phenomenon was first encountered by Kummer during his investigation of rings $\mathbb{Z}[\zeta_p]$ (p prime). He noticed that for small values of p there seemed to be a simple rule for factorisation of primes $l \neq p$ in $\mathbb{Z}[\zeta_p]$ ("small" meaning $p \leq 19$), but the rule broke down for $p = 23$.

Kummer's solution of the puzzle was very imaginative: he postulated existence of certain "ideal numbers" living outside $\mathbb{Z}[\zeta_p]$ for which unique factorisation holds.

For the ring $A = \mathbb{Z}[i\sqrt{5}]$ this would mean that the inequivalent factorisations

$$2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$$

irreducible in $\mathbb{Z}[i\sqrt{5}]$

could be refined into $2 = \mathfrak{P}_1\mathfrak{P}_2$, $3 = \mathfrak{Q}_1\mathfrak{Q}_2$, $1+i\sqrt{5} = \mathfrak{P}_1\mathfrak{Q}_1$, $1-i\sqrt{5} = \mathfrak{P}_2\mathfrak{Q}_2$, for some "ideal numbers" $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{Q}_1, \mathfrak{Q}_2$.

Dedekind realised that all one needed to know about an "ideal number" $\mathfrak{D}$ was the set of elements of A divisible by $\mathfrak{D}$. This turned out to be an ideal of A. Dedekind not only introduced the concept of an ideal, but he showed that rings such as $\mathbb{Z}[i\sqrt{5}]$ are "Dedekind rings" in the sense that their non-zero ideals admit unique factorisation into prime ideals.

For $A = \mathbb{Z}[i\sqrt{5}]$ this says that the sum (*)

$$\sum_{I \subset \mathbb{Z}[i\sqrt{5}]} \frac{1}{N(I)^s} = \sum_{\alpha \in (\mathbb{Z}[i\sqrt{5}] - \{0\})/\mathbb{Z}[i\sqrt{5}]^\times} \frac{1}{N(\alpha)^s} + \left(\begin{array}{c}\text{the contribution}\\ \text{of non-principal}\\ \text{ideals}\end{array}\right)$$

I = non-zero ideal of $\mathbb{Z}[i\sqrt{5}]$

corresponds to principal ideals $I = (\alpha)$

is equal to $\prod_{\mathfrak{P}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1}$.

$\mathfrak{P}$: non-zero prime ideals of $\mathbb{Z}[i\sqrt{5}]$

Structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ and $(\mathbb{Z}/p^r\mathbb{Z})^\times$ (p prime)

Chinese remainder thm: if $(m,n)=1$, then $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (ring isom.)

$\Rightarrow (\mathbb{Z}/mn\mathbb{Z},+) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z},+) \oplus (\mathbb{Z}/n\mathbb{Z},+)$

$(\mathbb{Z}/mn\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times \oplus (\mathbb{Z}/n\mathbb{Z})^\times$ (isom. of abelian groups)

Cor: If $n = \prod_{i=1}^{k} p_i^{r_i}$ ($p_i \in P$ distinct), then $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \bigoplus_{i=1}^{k} (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$.

Structure of $(\mathbb{Z}/p\mathbb{Z})^\times$

Thm (Gauss) For each prime p, $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ is a cyclic group (of order $\varphi(p)=p-1$).

[In other words, $\exists a \in \mathbb{Z}$ $\{a \pmod p, a^2 \pmod p, \dots, a^{p-1} \pmod p\} = (\mathbb{Z}/p\mathbb{Z})^\times$.
We say that a is a primitive root modulo p.]

This is a special case of

Thm'. K field, $A \subset K^\times = (K\setminus\{0\},\cdot)$ finite subgroup $\Rightarrow A$ is cyclic.

Pf (following Gauss' proof of Thm). Let $n := |A|$. We are going to count the number of elements $g \in A$ of a given order ($\forall g \in A$ $\operatorname{order}(g) \mid n$)

Disjoint union $A = \coprod_{d \mid n} U_d$, $U_d := \{g \in A \mid \operatorname{order}(g) = d\}$

$$|A| = \sum_{d \mid n} |U_d|$$
$$\| \qquad\qquad \text{Goal: } U_n \neq \emptyset \ (\Rightarrow \text{each } g \in U_n \text{ will be a generator of } A)$$
$$n = \sum_{d \mid n} \varphi(d)$$

$\Rightarrow \forall d \mid n \ |U_d| = \varphi(d) \Rightarrow |U_n| = \varphi(n) > 0$

$U_n \neq \emptyset \Rightarrow$ Thm'.

Key Lemma: $\forall d \mid n \ |U_d| = 0$ or $\varphi(d)$

Pf of Key Lemma: use

(a) $\forall g \in U_d \ \forall k \geq 1 \ \operatorname{order}(g^k) = d/(d,k)$.

(b) L field, $f \in L[X] \setminus L \Rightarrow |\{\alpha \in L \mid f(\alpha) = 0\}| \leq \deg(f)$.

If $d \mid n$ and $U_d \neq \emptyset$: choose $g \in U_d$; then

$$U_d \hookrightarrow \underbrace{\{\alpha \in K \mid \alpha^d - 1 = 0\}}_{\leq d \text{ elements (by (b))}} \overset{\text{equality}}{=\!=} \underbrace{\{g, g^2, \dots, g^d = 1\}}_{d \text{ distinct elements}}$$

$$U_d = U_d \cap \{g, g^2, \dots, g^d\} \overset{(a)}{=} \underbrace{\{g^k \mid 1 \leq k \leq d, (d,k) = 1\}}_{\varphi(d) \text{ elements}}.$$

~~Solutions de l'exercice 5~~

$(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic

Thm. Let K be a field. Any finite multiplicative subgroup $A \subset K^\times$ is cyclic.

Cor (Gauss) For any prime number p the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Pf of Thm (inspired by the treatment of the Legendre symbol $\left(\frac{a}{p}\right)$ in terms of the factorisation $X^{p-1}-1 = \prod_{a \in \mathbb{F}_p^\times} (X-a) \in \mathbb{F}_p[X]$):

If $n = |A|$ is the order of A, then $\forall a \in A \quad a^n = 1$, which means that the polynomial $\prod_{a \in A} (X-a) \in K[X]$ must divide $X^n - 1 \in K[X]$. For reasons of degree, the two polynomials must be equal: $X^n - 1 = \prod_{a \in A} (X-a) \in K[X]$. We now compare this factorisation to the factorisation $X^n - 1 = \prod_{d \mid n} \Phi_n(X) \in \mathbb{Z}[X]$ into cyclotomic polynomials in $\mathbb{Z}[X]$, which gives rise to an analogous factorisation in $K[X]$ (recall that $\mu_n = \mu_n(\mathbb{C}) = \{ z \in \mathbb{C} \mid z^n = 1 \} = \{ \zeta_n^b \mid b \in \mathbb{Z}/n\mathbb{Z} \}$ decomposes as $\mu_n = \coprod_{d \mid n} \mu_d^\circ$, where $\mu_n^\circ = \mu_n \setminus \bigcup_{m<n} \mu_m = \{ \zeta_n^b \mid b \in (\mathbb{Z}/n\mathbb{Z})^\times \}$; then $\Phi_n(X) = \prod_{b \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^b)$).

There exists $a \in A$ such that $X-a$ divides $\Phi_n(X) \in K[X]$. This implies that $X-a$ does not divide (in $K[X]$) any of the factors $\Phi_d(X)$ of $X^n - 1$ with $d \mid n$, $d < n$.

If $m \nmid n$ and $m < n$, the factorisation $X^m - 1 = \prod_{d \mid m} \Phi_m(X)$ then implies that $a^m \neq 1$. Therefore $a \in A$ is an element of order $n = |A|$, hence a generator of A.

From $1+p\mathbb{Z} \pmod{p^r}$ to $(\mathbb{Z}/p^r\mathbb{Z})^\times$ $(p \neq 2,\ r \geq 1)$

Properties of $G[m] := \{g \in G \mid g^m = 1\}$, $G^m := \{g^m \mid g \in G\}$ subgroups of G (G abelian group, $m \geq 1$)

(1) $\begin{array}{ccc} G & \xrightarrow{\alpha} & G \\ \cup & & \cup \\ g & \longmapsto & g^m \end{array}$, $G[m] = \mathrm{Ker}(\alpha)$, $G^m = \mathrm{Im}(\alpha)$

So $|G| = |G[m]| \cdot |G^m|$, provided $|G| < \infty$.

(2) If $|G| < \infty$ and $G = G[m] \Rightarrow \exists k \in \mathbb{N}$ $|G| \mid m^k$

(if $g_1, \dots, g_k$ generate G, then $\beta : (\mathbb{Z}/m\mathbb{Z})^k \longrightarrow G$, $(a_1, \dots, a_k) \longmapsto g_1^{a_1} \cdots g_k^{a_k}$ is a surjective morphism $\Rightarrow |G| = |(\mathbb{Z}/m\mathbb{Z})^k| / |\mathrm{Ker}(\beta)|$)

(3) If $G \simeq C_n$ cyclic group of order n (generated by $g \in G$) and $m \mid n$, then

G^m = cyclic, generated by g^m, $G^m = \{g^m, (g^m)^2, \dots, (g^m)^{n/m}\} \simeq C_{n/m}$

$G[m] = \{g^k \mid \underbrace{g^{km} = 1}_{\Leftrightarrow\ n \mid km \Leftrightarrow \frac{n}{m} \mid k}\}$ = cyclic, generated by $g^{n/m}$, $\simeq C_m$

$\Rightarrow G^m = G[n/m]$.

(4) $m \mid n \Rightarrow G[m] \subset G[n]$, $G^m \supset G^n$.

(5) $G[m] \cap G[n] = G[\underbrace{\gcd(m,n)}_{d}]$

Pf: $\supseteq \Leftarrow$ (4); $\subseteq$ $d = mu + nv$, $g \in G[m] \cap G[n] \Rightarrow g^d = (g^m)^u (g^n)^v = 1$

(6) $G[m] + G[n] = G[\underbrace{\mathrm{lcm}(m,n)}_{mn/d}]$

Pf: $\subseteq \Leftarrow$ (4); $\supseteq$ $g \in G[mn/d] \Rightarrow g = g^1 = \underbrace{g^{\frac{m}{d}v}}_{g_1} \underbrace{g^{\frac{m}{d}u}}_{g_2}$, $g_1^m = (g^{\frac{mn}{d}})^v = 1$, $g_2^n = (g^{\frac{mn}{d}})^u = 1$

($g^{mn/d} = 1$)

(7) If $(m,n) = 1 \overset{(5),(6)}{\Rightarrow} G[m] \oplus G[n] = G[mn]$

($\Rightarrow$ primary decomposition: $G[\prod_1^k p_i^{n_i}] = \bigoplus_1^k G[p_i^{n_i}]$)

(8) $G = G[n] \Rightarrow G[m] = G[m] \cap G[n] = G[\underbrace{\gcd(m,n)}_{d}]$

(9) $G = G[n] \Rightarrow G^m = G^d$ [Pf: $\subseteq \Leftarrow$ (4); $\supseteq$ $d = mu + nv$, $g^d = g^{mu} g^{nv} = (g^u)^m \in G^m$]

(10) $G \simeq C_n \overset{(3),(8),(9)}{\Longrightarrow} G[m] \simeq C_{(m,n)}$, $G^m \simeq C_{n/(m,n)}$

(11) $G \simeq \bigoplus_j C_{n_j} \overset{(10)}{\Rightarrow} G[m] \simeq \bigoplus_j C_{(m,n_j)}$

$G^m \simeq \bigoplus_j C_{n_j/(m,n_j)}$

From $(\mathbb{Z}/p\mathbb{Z})^\times$ to $(\mathbb{Z}/p^r\mathbb{Z})^\times$ (p prime, $r \geq 1$)

Prop. (Frobenius morphism $x \longmapsto x^p$ improves congruences). Let $x, y \in \mathbb{Z}$.

(a) If $p \in P$, $t \geq 1$, $x \equiv y \ [p^t] \Longrightarrow x^p \equiv y^p \ [p^{t+1}]$.

(b) If $p \in P$, $t \geq 1$, $p^t > 2$, $p \nmid x$, $x \equiv y \ [p^t]$, $x \not\equiv y \ [p^{t+1}] \Longrightarrow x^p \equiv y^p \ [p^{t+1}]$, $x^p \not\equiv y^p \ [p^{t+2}]$

(the improvement in (a) cannot be improved, if $p^t > 2$)

Pf: $x = y + p^t z$, $z \in \mathbb{Z}$ ($p \nmid z$ in (b))

$$x^p = (y + p^t z)^p = y^p + p^{t+1} y^{p-1} z + \underbrace{\binom{p}{2} y^{p-2} (p^t z)^2 + \cdots + \binom{p}{p-1} y (p^t z)^{p-1}}_{\equiv 0 \ [p^{t+2}]} + p^{tp} z^p$$

$tp \geq 2t \geq t+1 \Rightarrow$ (a)

$p^t > 2 \Rightarrow tp \geq t+2 \Rightarrow$ (b)

Natural filtrations: (1) On the **additive group** $\mathbb{Z}/p^k\mathbb{Z}$: (p prime)

$$\mathbb{Z}/p^k\mathbb{Z} \supset p\mathbb{Z}/p^k\mathbb{Z} \supset p^2\mathbb{Z}/p^k\mathbb{Z} \supset \cdots \supset p^{k-1}\mathbb{Z}/p^k\mathbb{Z} \supset p^k\mathbb{Z}/p^k\mathbb{Z} = \{0\}$$

$$|\, p^j\mathbb{Z}/p^k\mathbb{Z} \,| = p^{k-j} \qquad (0 \leq j \leq k)$$

(2) On the **multiplicative group** $G := (\mathbb{Z}/p^r\mathbb{Z})^\times$ (p prime, $r \geq 1$)

$$\underbrace{(\mathbb{Z}/p^r\mathbb{Z})^\times}_{G} \supset \underbrace{1 + p\mathbb{Z} \pmod{p^r}}_{G_1} \supset \underbrace{1 + p^2\mathbb{Z} \pmod{p^r}}_{G_2} \supset \cdots \supset \underbrace{1 + p^{r-1}\mathbb{Z} \pmod{p^r}}_{G_{r-1}} \supset \underbrace{\{1 \pmod{p^r}\}}_{G_r = \{1\}}$$

For $1 \leq t \leq r$, $|G_t| = p^{r-t}$ ($G_t = 1 + p^t j \pmod{p^r}$, $j \in \mathbb{Z}/p^{r-t}\mathbb{Z}$)

$G_t = \mathrm{Ker}\left((\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p^t\mathbb{Z})^\times\right)$, $a \pmod{p^r} \longmapsto a \pmod{p^t}$ surjective morphism

---

Goal: compare (1) and (2) in terms of suitable exponential/logarithm maps

Toy model: for $b \in \mathbb{R}_{>0}$, $\exp_b(x) := \exp(x \ln(b))$ defines group isomorphisms

$$\begin{array}{ccc} \exp_b : \ \mathbb{C}/\frac{2\pi i}{\ln(b)}\mathbb{Z} & \xrightarrow{\sim} & \mathbb{C}^\times \\ \uparrow & & \uparrow \\ \mathbb{R} & \xrightarrow{\sim} & \mathbb{R}^\times_{>0} \end{array}$$

Inverse: $\log_b$

Reformulation of Prop: (a) $x \in G_t \setminus G_{t+1} \Longrightarrow x^p \in G_{t+1} \setminus G_{t+2}$ ($1 \leq t \leq r-1$)

($G_1 = 1$) (b) $p^t > 2$, $x \in G_t \setminus G_{t+1} \Longrightarrow x^p \in G_{t+1} \setminus G_{t+2}$ ($1 \leq t \leq r-2$)

Cor 1. $p^t > 2$, $1 \leq t \leq r-1 \Longrightarrow \{x \in (\mathbb{Z}/p^r\mathbb{Z})^\times \mid x^{(p^{r-t})} \equiv 1 \ [p^r]\} = G_t = 1 + p^t\mathbb{Z} \pmod{p^r}$

[$x^p \equiv 1 \ [p] \Longrightarrow x \equiv 1 \ [p]$]

[redacted]

Note: $p^t > 2 \Longleftrightarrow (p \neq 2$ or $(p = 2, t \geq 2))$

Cor 2. $p^t > 2$, $1 \le t \le r-1 \Rightarrow \forall\, b \equiv 1 \,[p^t] \not\equiv 1 \,[p^{t+1}]$ the "discrete exponential" $z \mapsto b^z$ $(z \in \mathbb{Z})$ induces well-defined group isomorphisms

$$\begin{array}{ccccccccc}
(\mathbb{Z}/p^{r-t}\mathbb{Z},+) & \supset & (p\mathbb{Z}/p^{r-t}\mathbb{Z},+) & \supset & \cdots & \supset & (p^{r-t-1}\mathbb{Z}/p^{r-t}\mathbb{Z},+) & \supset & \{0\} \\
\exp_b \downarrow \wr & & \downarrow \wr & & & & \downarrow \wr & & \downarrow \wr \\
1+p^t\mathbb{Z} \pmod{p^r} & \supset & 1+p^{t+1}\mathbb{Z} \pmod{p^r} & \supset & \cdots & \supset & 1+p^{r-1}\mathbb{Z} \pmod{p^r} & \supset & \{1\}
\end{array}$$

$\left(\exp_b(z \pmod{p^{r-t}}) = b^z \pmod{p^r}\right)$

Cor 3. $p^t > 2$, $1 \le t \le r-1$, $b \equiv 1 \,[p^t] \not\equiv 1 \,[p^{t+1}] \Rightarrow$ b is a generator of $1+p^t\mathbb{Z} \pmod{p^r}$ cyclic, order $= p^{r-t}$.

Moreover, if $0 \le j \le r-t$, b^{p^j} is a generator of $1+p^{t+j}\mathbb{Z} \pmod{p^r}$ cyclic, order $= p^{r-t-j}$

Cor 4. $(p \neq 2, t=1)$ If $p \neq 2$ and $r \ge 1$,

$1+p\mathbb{Z} \pmod{p^r} = \ker\left((\mathbb{Z}/p^r\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times\right)$ is cyclic of order p^{r-1}, generated by any $b \equiv 1\,[p]$, $b \not\equiv 1\,[p^2]$ (e.g., by $b = 1+p$)

$\left(\exp_b : \mathbb{Z}/p^{r-1}\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/p^r\mathbb{Z})^\times,\ z \pmod{p^{r-1}} \mapsto b^z \pmod{p^r}\right)$

Cor 5. $(p=2, t=2)$ If $r \ge 2$,

$1+4\mathbb{Z} \pmod{2^r} = \ker\left((\mathbb{Z}/2^r\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/2^2\mathbb{Z})^\times\right)$ is cyclic of order 2^{r-2}, generated by any $b \equiv 1\,[2^2]$, $b \not\equiv 1\,[2^3]$ (e.g., by $b = 5$).

Cor 6. If $r \ge 2$, $\{\pm 1\} \times \mathbb{Z}/2^{r-2}\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/2^r\mathbb{Z})^\times$ isomorphism

$(\varepsilon, x \pmod{2^{r-2}}) \longmapsto \varepsilon \cdot 5^x \pmod{2^r}$

Cor. 7. If $p \neq 2$, $r \ge 2$ and $p \nmid a$, then

$$\left[\exists x \in \mathbb{Z}\quad x^p \equiv a\,[p^r] \iff \exists x \in \mathbb{Z}\quad x^p \equiv a\,[p^2]\right].$$

If:

$$\begin{array}{ccc}
\underbrace{(\mathbb{Z}/p^r\mathbb{Z})^\times}_{G} & \xrightarrow{\alpha} & \underbrace{(\mathbb{Z}/p^2\mathbb{Z})^\times}_{H} \\
\downarrow & & \downarrow \\
G/G^p & \xrightarrow{\overline{\alpha}} & H/H^p
\end{array}$$

all four morphisms are surjective

$$|G/G^p| = |G[p]| \overset{\text{Cor. 1}}{\underset{t=r-1}{=}} |G_{r-1}| = p = \left(\begin{array}{l}\text{the same} \\ \text{for } r \text{ replaced by } 2\end{array}\right) = |H/H^p|$$

$\Rightarrow \overline{\alpha}$ is an isomorphism $\Rightarrow$ Cor. 7.

Exercise. What about $x^{p^j} \equiv a\,[p^r]$ (including for $p=2$)?

Thm. $p \neq 2$ prime, $r \geq 1 \Rightarrow G = (\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic.

Pf: $r=1$: – proved by Gauss.

$r \geq 2$: (1) Elementary proof: take any $a \in \mathbb{Z}$ such that $p \nmid a$ and $a \pmod p$ generates $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $b := a^{p-1} \equiv 1 \,[p]$.

(1a) If $b \not\equiv 1 \,[p^2] \Rightarrow$ order of $b \pmod{p^r}$ in G is equal to p^{r-1}
$\Big(\text{since } (p-1, p^{r-1}) = 1\Big) \Rightarrow$ order of $\underbrace{a \pmod{p^r}}_{\text{— " —}}$ in G is equal to $(p-1)p^{r-1} = |G|$
is a generator of G.

(1b) If $b \equiv 1 \,[p^2]$, replace a by $a' = (1+p)a$. Then $b' = a'^{p-1}$ satisfies $b' \equiv 1 \,[p]$, but $b' \not\equiv 1 \,[p^2]$ (since $(1+p)^p \equiv 1 \equiv (1+p)(1-p) \,[p^2]$ $\Big(b' \equiv b \cdot (1-p) \,[p^2] \equiv 1 - p \,[p^2]\Big)$. The argument in (1a) applies to $a' \Rightarrow$ result.

(2) Scientific proof: $|G| = (p-1)p^{r-1}$, $((p-1), p^{r-1}) = 1$

$\Rightarrow G = G[p-1] \oplus G[p^{r-1}]$, $|G[p-1]| = p-1$, $|G[p^{r-1}]| = p^{r-1}$.

We know that $G_1 := \operatorname{Ker}\Big(\underbrace{(\mathbb{Z}/p^r\mathbb{Z})^\times}_{G} \xrightarrow{p^r} (\mathbb{Z}/p\mathbb{Z})^\times\Big) = G[p^{r-1}]$, but this is not necessary for the argument.

Consider the morphism $\alpha: G[p-1] \hookrightarrow G \xrightarrow{p^r} (\mathbb{Z}/p\mathbb{Z})^\times$.

$|\operatorname{Ker}(\alpha)| = |G[p-1] \cap \underbrace{\operatorname{Ker}(p^r)}_{G_1}|$ divides $\Big(\underbrace{|G[p-1]|}_{p-1}, \underbrace{|G_1|}_{p^{r-1}}\Big) = 1$

$\Rightarrow \alpha$ is injective. But $|G[p-1]| = p-1 = |(\mathbb{Z}/p\mathbb{Z})^\times| \Rightarrow$
α is an isomorphism $\Rightarrow G[p-1]$ is cyclic, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is.

Moreover, $G[p-1] \oplus G_1 \hookrightarrow G$ is injective by the previous discussion, and $|G[p-1] \oplus G_1| = |G| \Rightarrow G = \underbrace{G[p-1]}_{C_{p-1}} \oplus \underbrace{G_1}_{C_{p^{r-1}}} \simeq$
$\simeq C_{(p-1)p^{r-1}}$ (since $(p-1, p^{r-1}) = 1$).
is cyclic.

Thm: $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic $\Leftrightarrow n = 1, 2, 4, p^r, 2p^r$ $(p \neq 2$ prime, $r \geq 1)$.

Pf: ($\Rightarrow$) We have proved this already ($\Leftarrow$ improved version of Euler's thm)

($\Leftarrow$) • $n = 1, 2, 4$ – easy.

$(\mathbb{Z}/2p^r\mathbb{Z})^\times = \underbrace{(\mathbb{Z}/2\mathbb{Z})^\times}_{0} \oplus \underbrace{(\mathbb{Z}/p^r\mathbb{Z})^\times}_{\text{cyclic}}$.

Decomposition of $(\mathbb{Z}/n\mathbb{Z})^\times$ into cyclic groups:

Thm: (1) p prime, $r \geq 1 \Rightarrow (\mathbb{Z}/p^r\mathbb{Z})^\times \simeq \begin{cases} C_{\varphi(p^r)} = C_{p-1} \oplus C_{p^{r-1}}, & p \neq 2 \text{ or } p=2, r \leq 2 \\ C_2 \oplus C_{2^{r-2}}, & p=2, r \geq 2. \end{cases}$

(2) $n = \prod_p p^{v_p(n)} \Rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \simeq \bigoplus_{\substack{p \mid n \text{ prime} \\ p \neq 2}} \left(C_{p-1} \oplus C_{p^{v_p(n)-1}} \right) \oplus \begin{cases} 0, & 4 \nmid n \\ C_2 \oplus C_{2^{v_2(n)-2}}, & 4 \mid n \end{cases}$

Exercise: Determine the number of solutions of $x^{30} \equiv 1 \ [240]$.

Exercise: If $k, r \geq 1$, $a \in \mathbb{Z}$, $2 \nmid a$, show that:

$\exists x \in \mathbb{Z} \quad x^{(2^k)} \equiv a \ [2^r] \iff \begin{cases} a \equiv 1 \ [2^r], & r \leq k+2 \\ \exists x \in \mathbb{Z} \ x^{(2^k)} \equiv a \ [2^{k+2}], & r \geq k+2. \end{cases} \iff$

$\iff a \equiv 1 \ [2^{\min(r, k+2)}]$.

($a \equiv 1 \ [2^{k+2}]$)

Exercise: If $p \neq 2$ prime, $k, r \geq 1$, $a \in \mathbb{Z}$, $p \nmid a$, show that:

$\exists x \in \mathbb{Z} \quad x^{(p^k)} \equiv a \ [p^r] \iff \begin{cases} a^{p-1} \equiv 1 \ [p^r] & r \leq k+1 \\ \exists x \in \mathbb{Z} \ x^{(p^k)} \equiv a \ [p^{k+1}] & r \geq k+1 \end{cases} \iff$

$\iff a^{p-1} \equiv 1 \ [p^{\min(r, k+1)}]$

($\Rightarrow a^{p-1} \equiv 1 \ [p^{k+1}]$)

Uniform formulation: If p = prime, $a \in \mathbb{Z}$, $p \nmid a$, $k, r \geq 1$, then:

$\exists x \in \mathbb{Z} \quad x^{(p^k)} \equiv a \ [p^r] \iff a^{p-1} \equiv 1 \ [p^{\min(r, k+1+\delta_{p2})}]$

(δ: Kronecker's delta)

Exercise. Let $p \equiv 1 \ [3]$ be a prime, let $n \geq 2$. Show that:

(1) $\exists \overline{a} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ of order 3 in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

(2) $\overline{a} + 1 = -\overline{a}^2 \in \mathbb{Z}/p^n\mathbb{Z}$.

(3) If $\overline{a} = a \pmod p$ $(a \in \mathbb{Z})$ $(a \neq 0, \pm 1 \ [p])$, then $(a+1)^p \equiv a^p + 1^p \ [p^n]$.

Question: Does $(a+1)^p \equiv a^p + 1 \ [p^2]$ have a solution $a \neq 0, \pm 1 \ [p]$ for some $p \equiv -1 \ [3]$? [YES, for $p = 59$, for example]

Solvability of $x^2 \equiv a\ [n]$

If $n = \prod_{i=1}^{k} p_i^{r_i}$, then: $\left[\exists x \in \mathbb{Z}\ \ x^2 \equiv a[n] \iff \forall i = 1, \dots, k\ \ \exists y_i \in \mathbb{Z}\ \ y_i^2 \equiv a\ [p_i^{r_i}] \right]$

Thm. Let p = prime, $r \geq 1$, $a \in \mathbb{Z}$, $p \nmid a$.

(1) If $p \neq 2$: $\left[\exists x \in \mathbb{Z}\ \ x^2 \equiv a\ [p^r] \iff \exists y \in \mathbb{Z}\ \ y^2 \equiv a\ [p] \ (\iff \left(\frac{a}{p}\right) = 1) \right]$.

(2) If $p = 2$, $r \leq 3$: $\exists x \in \mathbb{Z}\ \ x^2 \equiv a\ [2^r] \iff a \equiv 1\ [2^r]$ (~~exercise~~ easy)

(3) If $p = 2$, $r \geq 3$: $\exists x \in \mathbb{Z}\ \ x^2 \equiv a\ [2^r] \iff \exists y \in \mathbb{Z}\ \ y^2 \equiv a\ [2^3]$ $\left(\overset{(2)}{\iff} a \equiv 1\ [2^3]\right)$.

Reformulation: (1)' ($p \neq 2$) $\Rightarrow$

$$\begin{array}{ccc} G := (\mathbb{Z}/p^r\mathbb{Z})^\times & \xrightarrow{pr} & H := (\mathbb{Z}/p\mathbb{Z})^\times \\ \downarrow & & \downarrow \\ G/G^2 & \xrightarrow{\overline{pr}} & H/H^2 \end{array} \qquad \left(\frac{\cdot}{p}\right) : \{\pm 1\}$$

$\overline{pr}$ is an isomorphism.

(3)' ($r \geq 3$)

$$\begin{array}{ccc} G := (\mathbb{Z}/2^r\mathbb{Z})^\times & \xrightarrow{pr} & H := (\mathbb{Z}/2^3\mathbb{Z})^\times \\ \downarrow & & \downarrow \\ G/G^2 & \xrightarrow{\overline{pr}} & H/H^2 = H = (\mathbb{Z}/2^3\mathbb{Z})^\times \end{array}$$

$\overline{pr}$ is an isomorphism.

Pf: (1)', (3)' All four morphisms in either diagram are surjective.

So it is enough to check that $\underbrace{|G/G^2|}_{|G[2]|} \overset{?}{=} \underbrace{|H/H^2|}_{|H[2]|}$

But in (1)': $G[2] = \{\text{solutions of } x^2 \equiv 1\ [p^r]\} = \{\pm 1 \pmod{p^r}\}$ (exercise)

$H[2] = \{$ " $\}$ $= \{\pm 1 \pmod{p}\}$,

so $|G[2]| = 2 = |H[2]|$.

In (3'): $H[2] = \{\text{solutions of } x^2 \equiv 1\ [2^3]\} = H = \{\pm 1, \pm 5 \pmod{2^3}\}$

$G[2] = \{\text{solutions of } x^2 \equiv 1\ [2^r]\} = \{\pm 1, \pm(1 + 2^{r-1}) \pmod{2^r}\}$

($r \geq 3$) so $|G[2]| = 4 = |H[2]|$.

Elementary proof of (1): If $y^2 \equiv a\ [p]$, then $b y^2 \equiv a\ [p^r]$, $b \equiv 1\ [p]$. But $b^{p^{r-1}} \equiv 1\ [p^r] \Rightarrow b \equiv z^2\ [p^r]$, $z = b^{(p^r+1)/2}$

$\Rightarrow a \equiv (yz)^2\ [p^r]$.

Exercise: Prove (1)' (resp. (3)') using snake Lemma for

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Ker}(pr) & \longrightarrow & G & \xrightarrow{pr} & H & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \beta \\ 1 & \longrightarrow & \mathrm{Ker}(\overline{pr}) & \longrightarrow & G/G^2 & \longrightarrow & H/H^2 & \longrightarrow & 1 \end{array} \qquad \begin{array}{c} g \\ \downarrow \\ g^2 \end{array}$$

Remarks on $\mathbb{F}_p^{\times m}$ (p prime)

Fix a prime p. For each $m \geq 1$, $\mathbb{F}_p^{\times m} = \mathbb{F}_p^{\times d}$, $d = (m, p-1) \mid (p-1)$ (since $\mathbb{F}_p^{\times} = \mathbb{F}_p^{\times [p-1]}$). So it is enough to investigate $\mathbb{F}_p^{\times m}$ for $m \mid (p-1)$

Prop. If p = prime, $m \mid (p-1)$, $a \in \mathbb{Z}$, $p \nmid a$, then:

$a \pmod p \in \mathbb{F}_p^{\times m} \iff a^{\frac{p-1}{m}} \equiv 1 \ [p]$ ("Euler's criterion")

If: $\mathbb{F}_p^{\times} = C_{p-1} \Rightarrow C_{p-1}^{m} = C_{p-1}[(p-1)/m]$

Example: For which $p \neq 2, 3$ does one have $2 \in \mathbb{F}_p^{\times 3}$?

(always, if $p \equiv -1 \ [3]$, since $\mathbb{F}_p^{\times 3} = \mathbb{F}_p^{\times}$ then)

If $p \equiv 1 [3]$: $2 \in \mathbb{F}_p^{\times 3} \iff 2^{\frac{p-1}{3}} \equiv 1 \ [p]$.

$p \equiv 1 [3]$	7	13	19	(31)	37	(43)	61	67	73	79	97	103	(109)
$\frac{p-1}{3}$	2	4	6	10	12	14	20	22	24	26	32	34	36
$2^{\frac{p-1}{3}} \pmod p$	4	3	7	1	-11	1							1
$2 \in \mathbb{F}_p^{\times 3}$?	NO	NO	NO	(YES)	NO	(YES)	NO	NO	NO	NO	NO	NO	(YES)

So: for $p \equiv 1 [3]$, $2 \in \mathbb{F}_p^{\times 3} \iff p = 31, 43, 109, \ldots$

What is the rule?

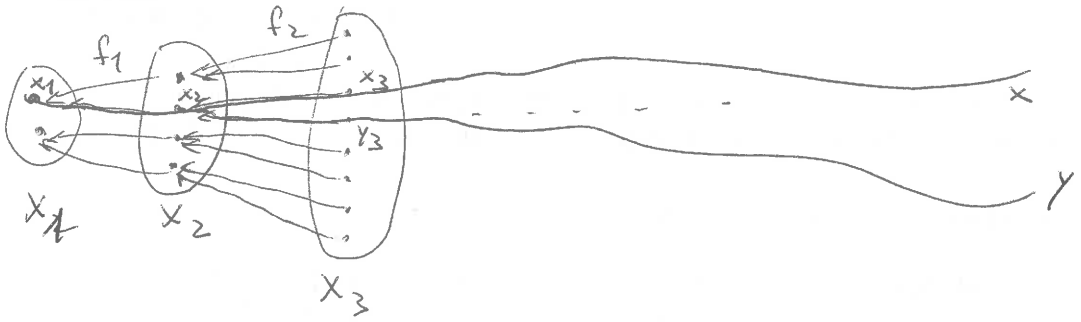
Solution de l'exercice

Projective limits (abstract theory)

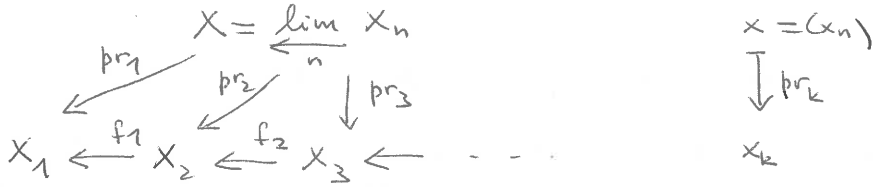
Recall: if $X_1 \xleftarrow{f_1} X_2 \xleftarrow{f_2} \cdots \xleftarrow{f_n} X_{n+1} \leftarrow \cdots$ is a sequence of sets (X_n) together with "transition maps" $(f_n : X_{n+1} \longrightarrow X_n)$ (a "projective system of sets indexed by $\mathbb{N}_+ = \{1,2,\dots\}$"), its projective limit consists of compatible systems of elements of the X_n's

$$X = \varprojlim_n X_n := \{ x = (x_n)_{n\geq 1} \mid \forall n \quad x_n \in X_n \ , \ f_n(x_{n+1}) = x_n \} \subset \prod_{n\geq 1} X_n .$$

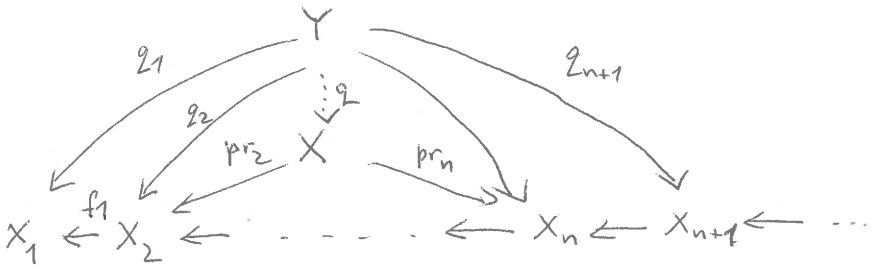
Picture:



There are canonical maps



such that $\forall n \geq 1 \quad f_n \circ pr_{n+1} = pr_n$, and X is a universal object among the sets having this property:



if Y is a set equipped with maps $q_n : Y \longrightarrow X_n$ such that $\forall n \quad f_n \circ q_{n+1} = q_n$, then there is a unique map $q : Y \longrightarrow X$ such that $\forall n \geq 1 \quad q_n = pr_n \circ q$

(indeed, we can define $q(y) = (q_n(y))_{n\geq 1} \quad (y \in Y)$, and this is the only map that works).

If each X_n is a $\left\{\begin{matrix}\text{group}\\ \text{ring}\end{matrix}\right\}$ and each f_n is a $\left\{\begin{matrix}\text{group}\\ \text{ring}\end{matrix}\right\}$ homomorphism, $X = \varprojlim_n X_n$ is again a $\left\{\begin{matrix}\text{group}\\ \text{ring}\end{matrix}\right\}$ (a $\left\{\begin{matrix}\text{subgroup}\\ \text{subring}\end{matrix}\right\}$ of $\prod_{n\geq 1} X_n$), and the universal property holds for $\left\{\begin{matrix}\text{group}\\ \text{ring}\end{matrix}\right\}$ homomorphisms.

Projective limits of topological spaces

Assume that each X_n is a topological space and each map $f_n : X_{n+1} \longrightarrow X_n$ is continuous.

Claim: there is a canonical topology on $X = \varprojlim_n X_n$ for which each $pr_n : X \longrightarrow X_n$ is continuous and which makes X into a universal object among topological spaces Y equipped with continuous maps $g_n : Y \to X_n$ satisfying $f_n \circ g_{n+1} = g_n$

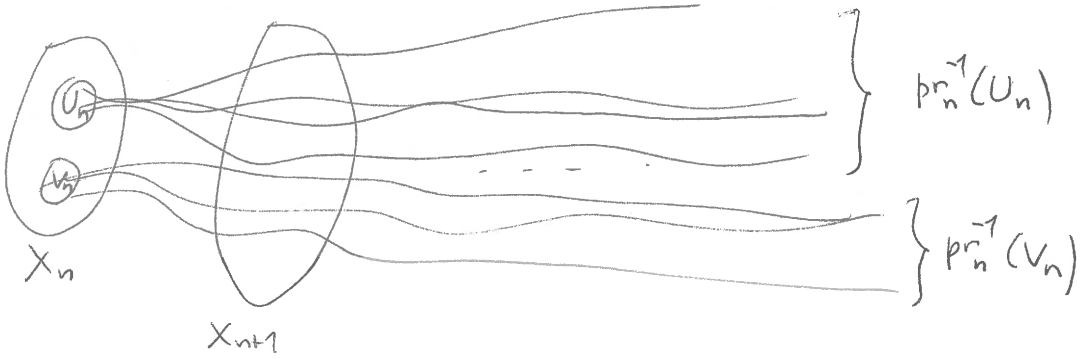
$$\cdots \leftarrow X_n \xleftarrow{f_n} X_{n+1} \leftarrow \cdots, \qquad g_n : Y \to X_n, \quad g_{n+1} : Y \to X_{n+1}$$

Equivalent descriptions of this projective limit topology:

(1) equip $\prod_{n\geq 1} X_n$ with the product topology and take the induced topology on $\varprojlim_n X_n \subset \prod_{n\geq 1} X_n$.

(2) A basis of this topology is given by the sets $pr_n^{-1}(U_n)$, where $n \in \mathbb{N}_+$ and $U_n \subset X_n$ is open (note that a finite intersection $\bigcap_{i=1}^{k} pr_{n_i}^{-1}(U_{n_i})$ can be written as $pr_n^{-1}(U_n)$, where $n \geq \max\{n_i \mid i=1,\dots,k\}$ and $U_n = \bigcap_{i=1}^{k} f_{n/n_i}^{-1}(U_{n_i})$; here $f_{m/n} : X_n \xrightarrow{f_{n-1}} X_{n-1} \longrightarrow \cdots \longrightarrow X_{m+1} \xrightarrow{f_m} X_m$).

Picture:



Note: If each X_n is Hausdorff, so is $X = \varprojlim_n X_n$.

Indeed, if $x, y \in X$ and $x \neq y$, then $x_n \neq y_n$ for some $n \geq 1$.

If $U_n \ni x_n$, $V_n \ni y_n$ are open sets in X_n such that $U_n \cap V_n = \emptyset$, then $U := pr_n^{-1}(U_n) \ni x$, $V := pr_n^{-1}(V_n) \ni y$ are open in X and $U \cap V = \emptyset$.

---

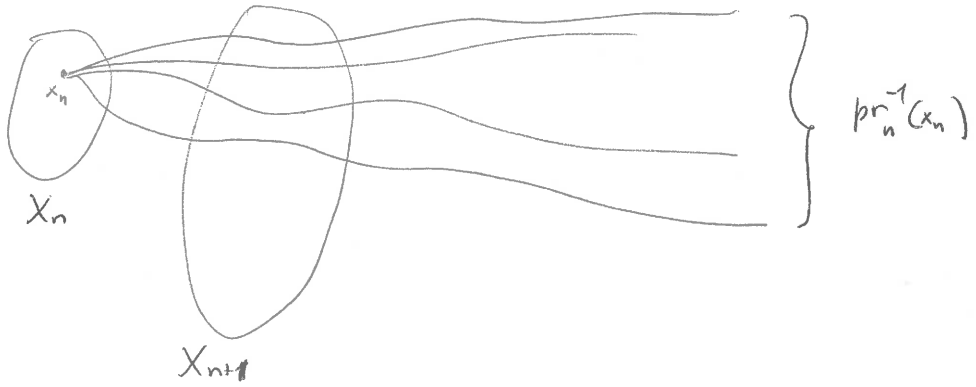
(3) In fact, it is enough to take in (2) only $pr_n^{-1}(U_n)$ for U_n belonging to a basis of the topology of X_n ($n \geq 1$).

The prodiscrete case

Assume each X_n is equipped with <u>discrete topology</u> (every subset of X_n is open). The projective limit topology on $X = \varprojlim_n X_n$ has as a basis the sets $pr_n^{-1}(x_n)$ $(n \in \mathbb{N}_+,\ x_n \in X_n)$.

<u>Note</u>: the set $pr_n^{-1}(x_n)$ is both <u>open and closed</u> in X, since $X - pr_n^{-1}(x_n) = \bigcup_{y_n \in X - \{x_n\}} pr_n^{-1}(y_n)$.

We also know that X is Hausdorff, since each X_n is.



<u>Claim</u>: there is a natural class of metrics defining the above topology on $X = \varprojlim_n X_n$.

Indeed, we first define

$$w : X \times X \longrightarrow \mathbb{N} \cup \{+\infty\}$$

by

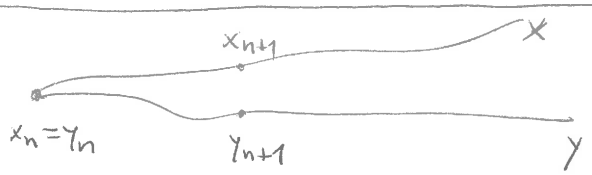
$$w(x,y) = \begin{cases} +\infty & \text{if } x = y \\ n & \text{if } x_n = y_n,\ x_{n+1} \neq y_{n+1} \end{cases}$$

Then we fix a strictly decreasing map

$$\lambda : \mathbb{N} \longrightarrow \mathbb{R}_{>0} \quad \text{such that} \quad \lim_{n \to \infty} \lambda(n) = 0$$

and define

$$d(x,y) := \lambda(w(x,y)) \qquad (\lambda(+\infty) := 0).$$



$w(x,y) = n$

<u>Note</u>: (a) $w(x,y) = w(y,x) \Rightarrow d(x,y) = d(y,x)$

(b) $x \neq y \iff w(x,y) < +\infty \iff d(x,y) \neq 0$

(c) $[x_n = y_n \text{ and } y_n = z_n \Rightarrow x_n = z_n] \Rightarrow w(x,z) \geq \min(w(x,y), w(y,z))$

$\iff \boxed{d(x,z) \leq \max(d(x,y), d(y,z))}$

ultrametric property of d

The profinite case

Thm. Let $(X_n)_{n\geq 1}$ be a projective system of nonempty finite sets.

(1) $X = \varprojlim_n$ is nonempty.

(2) Equip each X_n with discrete topology and X with the corresponding projective limit topology. Then every sequence in X contains a convergent subsequence.

(3) X is compact (it is Hausdorff and every open covering $X = \bigcup_\alpha U_\alpha$ has a finite subcovering $X = U_{\alpha_1} \cup \dots \cup U_{\alpha_k}$).

Pf. (1) Define $X_n^k := \mathrm{Im}(X_{n+k} \to X_{n+k-1} \to \cdots \to X_{n+1} \to X_n)$ $(k \geq 0)$

We have $X_n = X_n^0 \supset X_n^1 \supset X_n^2 \supset \dots$ with each X_n^k nonempty finite

$\Rightarrow X_n^\infty := \bigcap_{k\geq 0} X_n^k \subset X_n$ is nonempty (and finite).

By definition, $f_n(X_{n+1}^\infty) \subset X_n^\infty$, so $\varprojlim_n (X_n^\infty) \subset \varprojlim_n (X_n) = X$ is defined. On the other hand, for each $x = (x_n) \in X$ $\forall n$ $x_n \in X_n^\infty$, hence $\varprojlim_n (X_n^\infty) = X$.

Claim: $\forall n$ $X_{n+1}^\infty \xrightarrow{f_n} X_n^\infty$ is surjective

(this implies (1), since we can take $x_1 \in X_1^\infty$, $x_2 \in (f_1)^{-1}(x_1) \cap X_2^\infty$, $x_3 \in f_2^{-1}(x_2) \cap X_3^\infty$ etc. to obtain $(x_n) \in X$.)

Pf of Claim: if $\exists\ a \in X_n^\infty \setminus f_n(X_{n+1}^\infty)$, then $\forall\ b \in f_n^{-1}(a) \subset X_{n+1}$

$b \notin X_{n+1}^\infty \Rightarrow \exists\ k_b \in \mathbb{N}_+$ $b \notin \mathrm{Im}(X_{n+k_b} \to X_{n+1})$. But $|f_n^{-1}(a)| < \infty$,

and so $k = \sup\{k_b \mid f_n(b) = a\} < \infty \Rightarrow a \notin \mathrm{Im}(X_{n+k} \to X_n)$

contradiction with $a \in X_n^\infty$.

Pf of (2). Given a sequence $x^{(k)}$ $(k \geq 1)$ of elements $x^{(k)} = (x_n^{(k)})_{n\geq 1} \in X$ $(x_n^{(k)} \in X_n)$, the finiteness of each X_n implies that $\forall n$ $Y_n := \{y_n \in X_n \mid \exists_\infty k\ \ \mathrm{pr}_n(x^{(k)}) = y_n\} \subset X_n$ is nonempty. Moreover, $f_n(Y_{n+1}) \subset Y_n$, so $\exists\ y = (y_n) \in \varprojlim_n Y_n \subset X$, by (1). For each $n \in \mathbb{N}_+$ choose $k_n \in \mathbb{N}_+$ such that $k_n > k_{n-1}$ and $y_n = \mathrm{pr}_n(x^{(k_n)})$. The subsequence $x^{(k_n)}$ then converges to y in X.

(of $(x^{(k)})_{k\geq 1}$)

Pf of (3). It is enough to show:

if $X = \bigcup_{n\geq 1} pr_n^{-1}(Y_n)$ for some $Y_n \subset X_n$, then $\exists n_0 \quad X = \bigcup_{n\leq n_0} pr_n^{-1}(Y_n)$.

Let $Y_n' := \bigcup_{m\leq n} f_{n/m}^{-1}(Y_m) \supset Y_n$; then $f_n^{-1}(Y_n') \subset Y_{n+1}'$, hence

$f_n(X_{n+1} \smallsetminus Y_{n+1}') \subset X_n \smallsetminus Y_n'$. We have

$$\emptyset = X \smallsetminus \bigcup_{n\geq 1} pr_n^{-1}(Y_n') = \bigcap_{n\geq 1} (X \smallsetminus pr_n^{-1}(Y_n')) = \bigcap_{n\geq 1} pr_n^{-1}(X_n \smallsetminus Y_n')$$

$$\Rightarrow \varprojlim_n (X_n \smallsetminus Y_n') = \emptyset \overset{(1)}{\Longrightarrow} \exists n_0 \quad Y_{n_0}' = X_{n_0} \Rightarrow X = \bigcup_{n\leq n_0} pr_n^{-1}(Y_n') = \bigcup_{n\leq n_0} pr_n^{-1}(Y_n)$$

Example: If $X = \mathbb{Z}/2^n\mathbb{Z}$, then the open subsets $U_n = pr_n^{-1}(2^{n-1} \pmod{2^n})$ $(n\geq 1)$ of $X = \varprojlim_n X_n = \mathbb{Z}_2$ are disjoint and nonempty, but their union misses the point $0 = (0)_{n\geq 1}$: $\coprod_{n\geq 1} U_n = \coprod_{n\geq 1} (2^{n-1} + 2^n\mathbb{Z}_2) = \mathbb{Z}_2 \smallsetminus \{0\}$.

Cor. Assume that $X = \varprojlim_n X_n$ ($0 < |X_n| < \infty$ $\forall n$) is as in Thm, that $\alpha: X \longrightarrow Y$ is a continuous map to a Hausdorff topological space Y and that $x^{(k)} \in X$ $(k\geq 1)$ is a sequence for which $\alpha(x^{(k)})$ converges to $y \in Y$. Then $\exists x \in X \quad \alpha(x) = y$.

Pf. Take $x \in X$ to be the limit of any convergent subsequence of $x^{(k)}$.

Special case:

$$\begin{array}{ccccccccccc} X = \varprojlim_n & (X_1 & \leftarrow & X_2 & \leftarrow & \cdots & \leftarrow & X_n & \xleftarrow{f_n} & X_{n+1} & \leftarrow \cdots) \\ \alpha\downarrow & \downarrow\alpha_1 & & \downarrow\alpha_2 & & & & \downarrow\alpha_n & & \downarrow\alpha_{n+1} & \\ Y = \varprojlim_n & (Y_1 & \leftarrow & Y_2 & \leftarrow & \cdots & \leftarrow & Y_n & \xleftarrow{g_n} & Y_{n+1} & \leftarrow \cdots) \end{array}$$

$\forall n \quad \alpha_n \circ f_n = g_n \circ \alpha_{n+1}$ ("$(\alpha_n)_{n\geq 1}$ is a morphism of projective systems")

$\Rightarrow \quad \alpha : (x_n)_{n\geq 1} \longmapsto (\alpha_n(x_n))_{n\geq 1}$ is a morphism $\alpha: X \longrightarrow Y$.

If all X_n, Y_n are topological spaces and all maps f_n, g_n, α_n are continuous (the continuity is automatic if all X_n, Y_n are discrete), then α is continuous.

In particular, if all X_n, Y_n are finite and non-empty (with discrete topology), Cor. above says the following:

if each α_n is surjective, then α is surjective.

More precisely, if we only assume that $\forall n \quad 0 < |X_n| < \infty$ and that $\forall n \quad Y_n$ is discrete, then

$$\alpha(X) = \{ y \in Y \mid \forall n\geq 1 \quad pr_n(y) \in \alpha_n(X_n) \}.$$

Density

Recall: a subset Y of a topological space X is *dense* in X if its closure coincides with X. Equivalently, $Y \cap U \neq \emptyset$ for every nonempty open set $U \subset X$.

Prop. Let (X_n) be a projective system of topological spaces (with continuous transition maps $X_n \leftarrow X_{n+1}$). A subset $Y \subset X = \varprojlim_n X_n$ is dense in $X \iff \forall n \geq 1$ $\mathrm{pr}_n(Y)$ is dense in X_n.

[If X_n is discrete, then the above condition $\iff \mathrm{pr}_n(Y) = X_n$.]

Pf. Y is dense in $X \iff \forall n \ \forall\, 0 \neq U_n \subset X_n$ open $\underbrace{Y \cap \mathrm{pr}_n^{-1}(U_n) \neq \emptyset}_{\mathrm{pr}_n(Y) \cap U_n \neq \emptyset}$.

$\uparrow$ $\{\mathrm{pr}_n^{-1}(U_n)\}$ is a basis of topology of X

Completeness

Recall: (a) A sequence of points $x^{(k)}$ $(k \geq 1)$ of a metric space (X,d) is a *Cauchy sequence* if $\forall \varepsilon > 0$ $\exists k_0(\varepsilon)$ $\forall k, l \geq k_0(\varepsilon)$ $d(x^{(k)}, x^{(l)}) < \varepsilon$.

(b) (X,d) is a *complete metric space* if every Cauchy sequence in X converges.

(c) A *completion* of a metric space (X,d) is a distance-preserving inclusion $(X,d) \hookrightarrow (X',d')$ to a complete metric space in which X is dense.

(d) A completion of (X,d) exists; any two completions are canonically isometric. For example, one can take

$X' = \{\text{Cauchy sequences in } X\} / (\text{equivalence } \sim)$, with two Cauchy sequences being equivalent if their union is again a Cauchy sequence. The metric is given by

$$d'\left((x^{(k)})_{k\geq 1}, (y^{(k)})_{k\geq 1}\right) = \lim_{k\to+\infty} d(x^{(k)}, y^{(k)}).$$

If X'' is another completion of X, then

$$X' \longrightarrow X''$$

$$(x^{(k)})(\mathrm{mod}\sim) \longmapsto \lim_{k\to\infty} x^{(k)} \text{ in } X''$$

is the unique isometry extending the identity map $X \xrightarrow{id} X$

(the inclusion $X \hookrightarrow X'$ sends $x \in X$ to the constant sequence $x^{(k)} = x$ $\forall k$).

Basic example: $X = \mathbb{Q}$, $d(x,y) = |x-y|$

the completion $= \mathbb{R}$.

Prop. The projective limit $X = \varprojlim_n X_n$ of an arbitrary projective system $(X_n)_{n\geq 1}$ of discrete topological spaces is a complete metric space (with respect to the metric $d(x,y) = \lambda(w(x,y))$, for any choice of $\lambda(1) > \lambda(2) > \dots > \lambda(n) > \dots > 0$ tending to 0 as $n \to +\infty$).

Pf. If $x^{(k)}$ $(k \geq 1)$ is a Cauchy sequence in X, then, for each fixed $n \geq 1$ there exists $k_0(n) \in \mathbb{N}_+$ such that

$$\forall k, l \geq k_0(n) \qquad \underbrace{d(x^{(k)}, x^{(l)}) \leq \lambda(n)}_{w(x^{(k)}, x^{(l)}) \geq n} \iff (x^{(k)})_n = (x^{(l)})_n \in X_n.$$

Denote by $x_n \in X_n$ this common value of $(x^{(k)})_n$ for large enough k. As $x_n = (x^{(k)})_n = f_n((x^{(k)})_{n+1}) = f_n(x_{n+1})$ for $k \geq \max(k_0(n), k_0(n+1))$, we have $x = (x_n) \in X$. By construction, $d(x, x^{(k)}) \leq \lambda(n)$ if $k \geq k_0(n)$, hence $x = \lim_{k\to\infty} x^{(k)}$ in X.

Cor. If $Y \subset X = \varprojlim_n X_n$ (with all X_n discrete topological spaces) satisfies $\forall n \quad pr_n(Y) = X_n$, then X is a completion of Y (with respect to the (restriction to Y of the) metric $d(x,y) = \lambda(w(x,y))$).

Basic example: p prime number, $X_n = \mathbb{Z}/p^n\mathbb{Z}$,

$X = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ the p-adic integers,

$Y = \mathbb{Z}$, $\lambda(n) = \frac{1}{p^n}$ $\left(\Rightarrow d_p(x,y) = \frac{1}{p^{v_p(x-y)}} = |x-y|_p \right.$

$w(x,y) = v_p(x-y)$ $\left. x, y \in \mathbb{Z}_p \right)$
