Exercise 1

(a) For the modulus $m = (m)\infty$ we get a surjective map

$$\varphi : I^{S(m)} \longrightarrow (\mathbb{Z}/m)^*$$

sending $\mathfrak{a} = (a)$ to the class of the positive generator of $\mathfrak{a}$. The kernel is

$$\ker \varphi = \{ \mathfrak{a} = (a) : a > 0 \text{ and } \operatorname{ord}_p(a-1) \geq \operatorname{ord}_p(m) \ \forall p \mid m \}$$
$$= P_m,$$

hence $I^{S(m)}/\ker\varphi = C_m \cong (\mathbb{Z}/m)^*$.

If we skip the requirement that $a > 0$ in the definition of φ we get a surjection onto $(\mathbb{Z}/m)^*/\{\pm 1\}$ and an isomorphism

$$C_m \cong (\mathbb{Z}/m)^*/\{\pm 1\} \quad \text{for } m = (m).$$

2)

(b) $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is ramified at m and ∞,

and has Galois group $(\mathbb{Z}/m)^*$.

So the ray class field of $(m)\infty$ is $\mathbb{Q}(\zeta_m)$.

For the modulus $\mathfrak{m} = (m)$ we need

an extension $\mathbb{Q}(m)/\mathbb{Q}$ ramified only at m,

hence a real extension, so that $\mathrm{Gal}(\mathbb{Q}(m)/\mathbb{Q}) \simeq (\mathbb{Z}/m)^*/\{\pm 1\}$.

Now the maximal real subextension of

$\mathbb{Q}(\zeta_m)$ is $\mathbb{Q}(\zeta_m + \bar{\zeta}_m) = \mathbb{Q}\left(2\cos\left(\frac{2\pi}{m}\right)\right)$.

The minimal polynomial of ζ_m over $\mathbb{Q}(\zeta_m + \bar{\zeta}_m)$

is $X^2 - (\zeta_m + \bar{\zeta}_m)X + 1$, hence

$[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m + \bar{\zeta}_m)] = 2$. Hence, by Galois

theory, $\mathrm{Gal}(\mathbb{Q}(\zeta_m + \bar{\zeta}_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m)^*/\{\pm 1\}$

Moreover, $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \bar{\zeta}_m)$ is ramified

only at ∞, so $\mathbb{Q}(\zeta_m + \bar{\zeta}_m)/\mathbb{Q}$ is

ramified at m.

(c) If $K(m)$ denotes the ray class field for a modulus m, note that $m \mid m' \Rightarrow K(m) \subseteq K(m')$.

Let $K/\mathbb{Q}$ be a finite abelian extension.

By Artin reciprocity, K is the ray field for some modulus m.

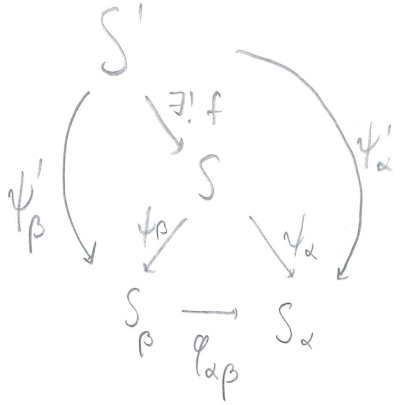
Since m is a product of rational primes and possibly ∞, m divides $(m)\infty$ for some $m \in \mathbb{Z}$.

Hence $K \subseteq \mathbb{Q}(\zeta_m)$.

Exercise 2

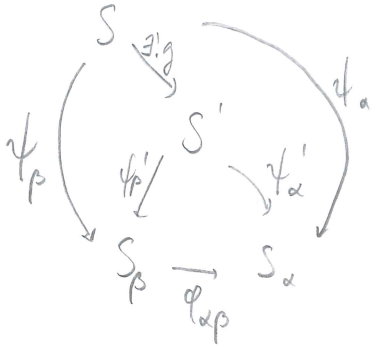
Let $(S_\alpha)_{\alpha \in I}$ be an inverse system, and suppose there are two objects S, S' satisfying the universal property for $\varprojlim_\alpha S_\alpha$.

Consider first S and use S' as test object:

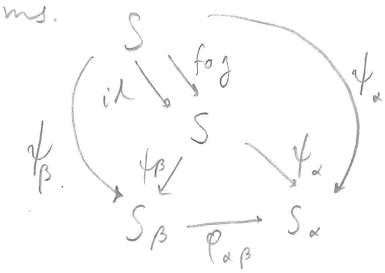


$\Rightarrow$ Get unique $f: S' \to S$ making everything commutative.

Now consider S' and use S as test object to get $g: S \to S'$:



Now use S as test object against itself. Then both id and $f \circ g$ makes everything commute, so by uniqueness, $id = f \circ g$. Similarly for $g \circ f$, so they are inverse isomorphisms.



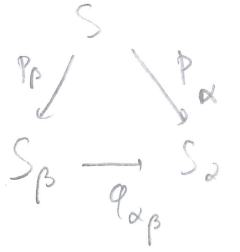
5)

Exercise 3

Let $S = \{(x_\alpha)_\alpha : \varphi_{\alpha\beta}(x_\beta) = x_\alpha\} \subseteq \prod_\alpha S_\alpha$

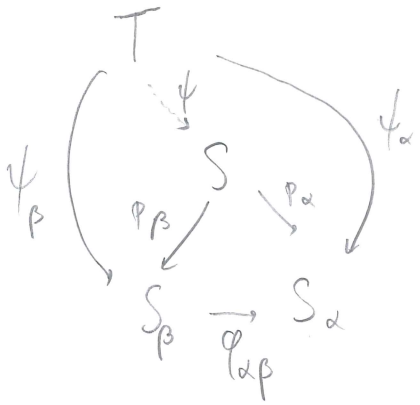
We show that S satisfies the universal property.

Since $S \subseteq \prod_\alpha S_\alpha$, there are projection maps



for all α, β, which makes the diagram commutative by definition of S.

Let T be a set with:



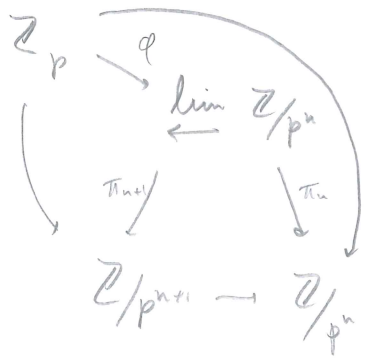
We define $\psi: T \to S$ by

$$\psi(y) = (\psi_\alpha(y))_\alpha$$

If $\varphi: T \to S$ is another map, then, by commutativity, the α^{th} component of $\varphi(y)$ is $\psi_\alpha(y)$. So $\varphi = \psi$, and thus ψ is unique.

Exercise 4

Reduction mod p^n gives maps $\mathbb{Z}_p \to \mathbb{Z}/p^n$ for all n. Hence we get a unique map of topological groups



sending $\sum_{i \geq 0} a_i p^i$ to $(a_i)_i \in \varprojlim \mathbb{Z}/p^n$.

This map is injective. Let $(a_n) \in \varprojlim \mathbb{Z}/p^n$. Since $a_{n+1} \equiv a_n \bmod p^n$, $\lim_{n \to \infty} |a_{n+1} - a_n|_p = 0$.

So (a_n) is a Cauchy sequence p-adically, hence has a limit $a \in \mathbb{Z}_p$. So φ is surjective as well.

Finally, since $\varphi(p^n \mathbb{Z}_p) = \pi_n^{-1}(0)$, φ is an open map. So φ is an isomorphism of topological groups.

7)

Exercise 5

(a) This follows from the description of inverse limits in Exercise 3.

(b) We have $\mathbb{Z}/n \cong \prod_p \mathbb{Z}/p^{\mathrm{ord}_p(n)}$, so

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n \cong \varprojlim_n \prod_p \mathbb{Z}/p^{\mathrm{ord}_p(n)}$$

$$\cong \varprojlim_m \prod_p \mathbb{Z}/p^m$$

$$\cong \prod_p \varprojlim_m \mathbb{Z}/p^m = \prod_p \mathbb{Z}_p .$$

(c) Given $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, with componentwise multiplication, we can take

$$x = (1, 0, 0, \dots), \quad 1 \in \mathbb{Z}_2$$

$$y = (0, 1, 0, 0, \dots) \quad 1 \in \mathbb{Z}_3$$

to get $x, y \neq 0$ but $xy = 0$.

Exercise 6

We have

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \varprojlim_r \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p) \cong \varprojlim (\mathbb{Z}/p^r)^*$$

$$\cong \mathbb{Z}_p^* .$$

8)

Exercise 7 See pp. 130-131 of Milnes notes "Algebraic number theory".