2022/06/03

Note $a \equiv b \pmod{n}$

$:\Longleftrightarrow \exists k \in \mathbb{Z} : \quad a-b = kn$

$\Longleftrightarrow a-b \in n\mathbb{Z}$

$n\mathbb{Z} := \{ kn \mid k \in \mathbb{Z} \}$

Ex. 1.6.3

$\because$ 反射律： [示すこと: $\forall a \in \mathbb{Z} \ , \ a \sim a$]

$\forall a \in \mathbb{Z}$ をとる

[示すこと: $a \sim a$ i.e. $\exists k \in \mathbb{Z} : a-a = kn$]

$k := 0$ とおくと, $k \in \mathbb{Z}$

[示すこと: $a-a = kn$]

$a-a = 0 = 0 \times n = kn$ //

対称律：[示すこと：$\forall a,b\in\mathbb{Z}\ (a\sim b),\quad b\sim a$]

$\forall a,b\in\mathbb{Z}\ (a\sim b)$ をとる

[示すこと：$b\sim a$ i.e. $\exists k\in\mathbb{Z} : b-a=kn$]

$a\sim b$ より $\exists k'\in\mathbb{Z} : a-b=k'n$

$k := -k'$ とおくと、$k\in\mathbb{Z}$

[示すこと：$b-a=kn$]

$b-a=-(a-b)=-k'n=kn$ //

推移律: [示すこと: $\forall a,b,c \in \mathbb{Z}\ (a \sim b,\ b \sim c),\ a \sim c$]

$\forall a,b,c \in \mathbb{Z}\ (a \sim b,\ b \sim c)$ をとる

[示すこと: $a \sim c$ i.e., $\exists k \in \mathbb{Z} : a - c = kn$]

$a \sim b$ より $\exists k_1 \in \mathbb{Z} : a - b = k_1 n$

$b \sim c$ より $\exists k_2 \in \mathbb{Z} : b - c = k_2 n$

$k := k_1 + k_2$ とおくと, $k \in \mathbb{Z}$

[示すこと: $a - c = kn$]

$$
\begin{aligned}
a - c &= (a-b) + (b-c) \\
&= k_1 n + k_2 n = (k_1 + k_2) n = kn
\end{aligned}
$$

//

Ex. 1.6.5

∵ 反射 [示すこと: $\forall a \in A$, $a \sim a$]

$\forall a \in A$ をとる.

[示すこと: $a \sim a$ i.e. $\exists C \in \mathcal{U}: a \in C$]

$a \in A = \bigcup \mathcal{U}$ より

$\exists C \in \mathcal{U}: a \in C$ //

対称 [示すこと: $\forall a, b \in A\ (a \sim b)$, $b \sim a$]

$\forall a, b \in A\ (a \sim b)$ をとる.

[示すこと: $b \sim a$, i.e. $\exists C \in \mathcal{U}: b, a \in C$]

$a \sim b$ より

$\exists C \in \mathcal{U}: a, b \in C$

$\therefore b, a \in C$

//

<u>推移</u> [示すこと: $\forall a,b,c \in A \ (a \sim b,\ b \sim c),\ a \sim c$]

$\forall a,b,c \in A \ (a \sim b,\ b \sim c)$ をとる

[示すこと: $a \sim c$, i.e., $\exists C \in \mathcal{U} : a, c \in C$]

$a \sim b$ より $\exists C_1 \in \mathcal{U} : a, b \in C_1$

$b \sim c$ より $\exists C_2 \in \mathcal{U} : b, c \in C_2$

$C := C_1$ とおいて, $C \in \mathcal{U}$

[示すこと: $a, c \in C$]

$b \in C_1 \cap C_2$ より $C_1 \cap C_2 \neq \emptyset$

直和分解の条件(ii) より $C_1 = C_2$

$\therefore$ $a \in C_1 = C$

$c \in C_2 = C$

//

Prop 1.6.7

(1) [示すこと: $a \in C(a)$ i.e. $a \sim a$]

明らか

(2) claim $a \sim b \Rightarrow C(a) = C(b)$

∵) $a \sim b$ とする.

[示すこと: $C(a) = C(b)$ i.e. $C(a) \subset C(b)$ & $C(a) \supset C(b)$]

$C(a) \subset C(b)$ のみ示す

[示すこと: $\forall x \in C(a)$, $x \in C(b)$]

$\forall x \in C(a)$ をとる

[示すこと: $x \in C(b)$ i.e. $x \sim b$]

$x \in C(a)$ より $x \sim a$

仮定 より $a \sim b$

推移律 より $x \sim b$ //

<u>claim</u> $C(a)=C(b) \Longrightarrow C(a)\cap C(b)\neq\phi$

$\because$) $C(a)=C(b)$ とする.

[示すこと: $C(a)\cap C(b)\neq\phi$]

$a\in C(a)=C(b)$ より

$a\in C(a)\cap C(b)$

$\therefore$ $C(a)\cap C(b)\neq\phi$ //

<u>claim</u> $C(a)\cap C(b)\neq\phi \Longrightarrow a\sim b$

$\because$) $C(a)\cap C(b)\neq\phi$ とする.

[示すこと: $a\sim b$]

仮定より $\exists x\in C(a)\cap C(b)$

$x\in C(a)$ より $x\sim a$ $\therefore$ $a\sim x$

$x\in C(b)$ より $x\sim b$

推移律 より $a\sim b$ //

Thm 1.6.8 (みておく)

(1) $\mathcal{U} := \{C(a) \mid a \in A\}$ とおく.

[示すこと: $\mathcal{U}$ は A の直和分割

i.e, (i) $A = \bigcup \mathcal{U}$

(ii) $\forall C, C' \in \mathcal{U} \, (C \neq C'),\ C \cap C' = \phi$]

(i): $(\supset)$ 明らか.

$(\subset)$ [示すこと: $\forall a \in A,\ a \in \bigcup \mathcal{U}$]

$\forall a \in A$ をとる

[示すこと: $a \in \bigcup \mathcal{U}$]

$a \in C(a) \subset \bigcup \mathcal{U}$ //

(ii) Prop 1.6.7 (2) より //

(2) $\mathcal{U}$ から決まる同値関係を $\sim_{\mathcal{U}}$ とする.

$$\left(a \sim_{\mathcal{U}} b \ :\Longleftrightarrow \ \exists C \in \mathcal{U} : a, b \in C \right)$$

[示すこと: $\forall a, b \in A$, "$a \sim_{\mathcal{U}} b \Longleftrightarrow a \sim b$"]

$\forall a, b \in A$ をとる.

[示すこと: $a \sim_{\mathcal{U}} b \Longleftrightarrow a \sim b$]

($\Rightarrow$) $a \sim_{\mathcal{U}} b$ とする.

[示すこと: $a \sim b$]

def より $\exists C \in \mathcal{U} : a, b \in C$

$C \in \mathcal{U}$ より $\exists x \in A : C = C(x)$

$\therefore a \sim x \sim b \quad \therefore a \sim b$

($\Leftarrow$) $a \sim b$ とする.

[示すこと: $a \sim_{\mathcal{U}} b$

i.e. $\exists C \in \mathcal{U} : a, b \in C$]

$C := C(a)$ とすればよい. //