Section 3

2.3

3.1

3.2

3.3

4.1

06.12.17

P15

$$m = q_1 n + r_1$$

$$n = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\dots$$

$$r_{j-1} = q_{j+1} r_j + r_{j+1}$$

$$\dots\dots$$

$$r_j = q_{j+2} r_{j+1} + r_{j+2}$$

Lemma 2.15

$$\left\{\begin{array}{l} m = r_{j-1} \\ n = r_j \\ r = r_{j+1} \end{array}\right.$$

$$\Downarrow$$

$$hcf(r_{j-1}, r_j) = hcf(r_j, r_{j+1})$$

$$
\begin{aligned}
hcf(r_j, r_{j+1}) &= hcf(r_{j-1}, r_j) \\
&= \dots \\
&= hcf(r_1, r_2) \\
&= hcf(n, r_1) \\
&= hcf(m, n)
\end{aligned}
$$

$$\left\{\begin{array}{l|l} m & n \\ n & r_1 \\ r & r_2 \end{array}\right.$$

lecture note | this page

# P16

lemma

$$\boxed{a \in S \Rightarrow \forall k \in \mathbb{Z},\ ak \in S}$$

$$a\mathbb{Z} = \{an : n \in \mathbb{Z}\}$$

WTP $a\mathbb{Z} \subseteq S$

$\forall x \in a\mathbb{Z}$

WTP $x \in S$

$\exists n \in \mathbb{Z}$ s.t.

$an = x$.

$a \in S$.

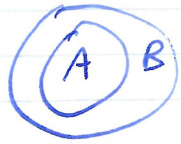
$an \in S$

$x \in S$.

$\square$

$A \subseteq B$ SUBSET

$\boxed{\forall x \in A,\ x \in B.}$




$A = \{f(x) \mid x \in B\}$ CONDITION

$\forall a \in A$

$\exists b \in B$ s.t.

$f(b) = a$.

Page 16/7

Prop 1.2

$S \subseteq \mathbb{Z}$ a subgroup.

WTS $\exists g \in \mathbb{N}$ s.t. $S = g\mathbb{Z}$

$S \neq \emptyset$ $S \neq \{0\}$

$\left\{ \begin{array}{l} ① \; S \subseteq g\mathbb{Z} \\ ② \; S \supseteq g\mathbb{Z} \; \boxed{\checkmark} \end{array} \right.$

$\forall n \in S$

$n = qg + r$

where $0 \le r < g$

"bounded"

$n \in S_+ \Rightarrow n \in g\mathbb{Z}$

$S = S_+ \cup \{0\} \cup S_-$

$\checkmark \quad \checkmark \quad ?$

$\forall m \in S_-$

$m < 0$

$-m > 0$

$-m \in S_+$

$\checkmark$

$\square$

$A = B$

$A \subseteq B$

$A \supseteq B$

WTP

$A = B$

$\left.\begin{array}{l}\forall x \in A \\ x \in B.\end{array}\right\} A \subseteq B$

$\left.\begin{array}{l}\forall x \in B \\ x \in A\end{array}\right\} B \subseteq A$

$$\begin{array}{r} 11 \\ 9\overline{)100} \\ 99 \\ \hline 1 \end{array}$$

$0 \le 1 < 9$

# Page 18

Prop. 3.4 (i) $G_1 + G_2 = \{m+n : m \in G_1, n \in G_2\}$.

(i) (a) $G_1 \cap G_2$ is a sg.

(i) (b) $G_1 + G_2$ is a sg.

---

(i)(a) $\left[\begin{matrix} m, n \in G_1 \\ m, n \in G_2 \end{matrix}\right] \Longrightarrow m+n,\ m-n \in G_1$ □

(i)(b) □

---

Prop. 3.4 (ii)

$\emptyset$

e.g. $x$ satisfies $x = ky$
$\updownarrow$
enjoys

~~(a) $A \in G_1$~~
~~(b)~~
~~(ii) (a)~~

Thm 3.5 Ⓟ $a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$

Ⓒ $A + B = \{ \cancel{x \in A}\ a+b : a \in A, b \in B\}$

(1) $m\mathbb{Z} + n\mathbb{Z} \overset{©}{=} \{\cancel{a+b}\ x+y : \cancel{a}\ x \in m\mathbb{Z}, \cancel{b}\ y \in n\mathbb{Z}\}$

$\overset{Ⓟ}{=} \{mk_1 + nk_2 : k_1, k_2 \in \mathbb{Z}\}$

$h\mathbb{Z} = \{hk_3 : k_3 \in \mathbb{Z}\}.$

$m\mathbb{Z} + n\mathbb{Z} = h\mathbb{Z}.$ □

---

$A \cap B = \{r : r \in A, r \in B\}$

(2) □

---

219

$am + bn = hcf(m, n)$

$a$ ? $b$ ?

$h = 5$

$= 365 - 18 \times 20$

$= 365 - 18 \times (750 - 2 \times 365)$

Step 2

$365 = 18 \times 20 + 5$

Step 1

$750 = 2 \times 365 + 20$

□

P23

Ex. 3.12

$$1 + 1 \equiv 0 \pmod 2$$
$$5 + 2 \equiv 0 \pmod 7$$
$$5 \equiv -2$$

Ex. 3.5

$$5^4 \pmod 7 \equiv (-2)^4 \pmod 7$$
$$= 16$$
$$\equiv 2 \pmod 7$$

$16 = 2 \times 7 + 2$

---

P30

$$\begin{array}{r}
0.4285714 \\
7\overline{)3.0} \\
28 \\
\hline
20 \\
14 \\
\hline
60 \\
56 \\
\hline
40 \\
35 \\
\hline
50 \\
49 \\
\hline
10 \\
7 \\
\hline
30 \\
28 \\
\hline
2
\end{array}$$

Repeat

$$\frac{3}{7} = 0.\dot{4}2857\dot{1}$$

$$\begin{array}{r} 30 \\ 28 \\ \hline 20 \\ 14 \\ \hline 6 \end{array}$$

$30 \equiv 2 \pmod 7$

$20 \equiv 6 \pmod 7$

$\square$

---

Pf $342 = 3 \times 10^2 + 4 \times 10^1 + 2 \times 10^0$.

Thm 4.5 $(m_k \times 10^k) + \cdots + m_0 + \frac{n_1}{10} + \cdots$
is rational

$\Updownarrow$

$\lambda := (m_k, m_{k-1}, \cdots, m_0, n_1, n_2, \cdots, n_t, \cdots)$
eventually periodic.

| | |
|---|---|
| $(\lambda_j)_{j=0}^{\infty}$ is periodic if $\exists N \in \mathbb{N}$ s.t. $\forall p \in \mathbb{N}$ $\lambda_{p+N} = \lambda_p$ | $\exists T \in \mathbb{N}$ s.t. $(\lambda_{i+T})_{i=0}^{\infty}$ is periodic |

$\Uparrow$ : $\boxed{d}$ $\forall p \in \mathbb{N}$, $\lambda_{p+d} = \lambda_p$

$10^d x = y$ $\square$

$$(\lambda_j)_{j=0}^{\infty} \qquad (\lambda_{j+1})_{j=0}^{\infty} \quad \text{~~where $k = j+1$~~}$$

$$\frac{\lambda_0, \lambda_1, \cdots}{\lambda_0\lambda_1 \cdots} = x \qquad \frac{\lambda_1, \lambda_2, \cdots}{\lambda_1\lambda_2 \cdots} = y$$

$$10x = y$$

---

$\Downarrow$:

$$x = 3.\underset{1}{1}\underset{2}{4}\underset{3}{1}\underset{4}{5}\underset{\substack{5\\ \| \\ e}}{4}\underbrace{74}_{d=2}74747\cdots$$

$$10^e x = 10^5 x = 31415.\boxed{474747\cdots}$$

$$10^{d+e} x = 10^7 x = 3141547.\boxed{474747\cdots}$$

$10^{d+e}x$