「ヒルベルトの既約性定理とその応用」資料（修正版）

2008.7.11 玉川安騎男

定義集

定義１

$$\mathbb{Z} = \{\text{ 整数全体 }\} = \{0, \pm 1, \pm 2, \dots\}$$
$$\cap$$
$$\mathbb{Q} = \{\text{ 有理数全体 }\} = \{a/b \mid a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus \{0\}\}$$
$$\cap$$
$$\mathbb{R} = \{\text{ 実数全体 }\}$$
$$\cap$$
$$\mathbb{C} = \{\text{ 複素数全体 }\} = \{a + bi \mid a, b \in \mathbb{R}\}$$

定義２　$(R, 0, 1, +, -, \cdot)$ が［あるいは、R が］（可換）環 $\overset{\text{def}}{\iff}$

R: 集合
$0, 1 \in R$
$+ : R \times R \to R,\ (a, b) \mapsto a + b$
$- : R \to R,\ a \mapsto -a$
$\cdot : R \times R \to R,\ (a, b) \mapsto a \cdot b$

であって、次の (i)–(viii) が成立

(i) $(a + b) + c = a + (b + c)$ $(\forall a, b, c \in R)$
(ii) $a + 0 = 0 + a = a$ $(\forall a \in R)$
(iii) $a + (-a) = (-a) + a = 0$ $(\forall a \in R)$
(iv) $a + b = b + a$ $(\forall a, b \in R)$
(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $(\forall a, b, c \in R)$
(vi) $a \cdot 1 = 1 \cdot a = a$ $(\forall a \in R)$
(vii) $a \cdot b = b \cdot a$ $(\forall a, b \in R)$
(viii) $a \cdot (b + c) = a \cdot b + a \cdot c,\ (a + b) \cdot c = a \cdot c + b \cdot c$ $(\forall a, b, c \in R)$

定義３ $(K, 0, 1, +, -, \cdot, ^{-1})$ が［あるいは、K が］（可換）体 $\overset{\text{def}}{\iff}$

K: 集合
$0, 1 \in K$
$+ : K \times K \to K,\ (a, b) \mapsto a + b$
$- : K \to K,\ a \mapsto -a$
$\cdot : K \times K \to K,\ (a, b) \mapsto a \cdot b$
$^{-1} : K \setminus \{0\} \to K,\ a \mapsto a^{-1}$

であって、次の (i)–(x) が成立

(i) $(a+b)+c=a+(b+c)$ $(\forall a,b,c\in K)$
(ii) $a+0=0+a=a$ $(\forall a\in K)$
(iii) $a+(-a)=(-a)+a=0$ $(\forall a\in K)$
(iv) $a+b=b+a$ $(\forall a,b\in K)$
(v) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ $(\forall a,b,c\in K)$
(vi) $a\cdot 1=1\cdot a=a$ $(\forall a\in K)$
(vii) $a\cdot b=b\cdot a$ $(\forall a,b\in K)$
(viii) $a\cdot(b+c)=a\cdot b+a\cdot c$, $(a+b)\cdot c=a\cdot c+b\cdot c$ $(\forall a,b,c\in K)$
(ix) $a\cdot a^{-1}=a^{-1}\cdot a=1$ $(\forall a\in K\setminus\{0\})$
(x) $1\neq 0$

定義４ 環 R の元 a が単元（可逆元）とは、ある $b\in R$ が存在して $ab=ba=1$ となることをいう。R の単元全体の集合を $R^{\times}$ と記す。

定義５ 環 R の元 a が既約元とは、次の二つの条件をみたすことをいう；
(i) もし $b,c\in R$ が $a=bc$ をみたせば、b または c は R の単元である。
(ii) a は単元ではない。

レポート問題

[Q1] (i) $\mathbb{Z} = \{$ 整数全体 $\} = \{0, \pm 1, \pm 2, \dots\}$ は（通常の $0, 1, +, -, \cdot$ に関して）体にならないことを示せ。
(ii) $n \in \mathbb{Z}, n > 0$ に対し、$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$ の $+, -, \cdot$ を、$\mathbb{Z}$ の $+, -, \cdot$ の結果に対し、それを n で割った余りをとることで定義する。このとき、$\mathbb{Z}/n\mathbb{Z}$ が体になるための必要十分条件は、n が素数であることを示せ。

[Q2] (i) $R[\alpha_1, \dots, \alpha_n] = \{f(\alpha_1, \dots, \alpha_n) \mid f \in R[x_1, \dots, x_n]\}$ を示せ。
(ii) $K(\alpha_1, \dots, \alpha_n) = \{\frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \mid f, g \in K[x_1, \dots, x_n],\ g(\alpha_1, \dots, \alpha_n) \neq 0\}$ を示せ。

[Q3] (i) $R[x_1, \dots, x_n]^\times = R^\times$ を示せ。
(ii) $\mathbb{Z}^\times = \{\pm 1\}$ を示せ。
(iii) $\mathbb{Z}$ の既約元の集合を求めよ。

[Q4] (i) $x^2 - t \in \mathbb{Q}[t, x]$ が既約であることを示せ。
(ii) $x^2 + t^2 + 1 \in \mathbb{Q}[t, x]$ が既約であることを示せ。
(iii) $x^n + t^n - 1 \in \mathbb{Q}[t, x]$ が既約であることを示せ。

[Q5] $f(t, x) = x^2 - t$ を考えて、既約性定理が $\mathbb{C}$ 上では成り立たないことを示せ。

[Q6] $f(t, x) = x^2 - t^2 - 1$ を考えて、既約性定理が $\mathbb{R}$ 上では成り立たないことを示せ。

[Q7] $f(t, x) = x^p - t$ を考えて（あるいは別の方法で）、既約性定理が $\mathbb{F}_p$ 上では成り立たないことを示せ。

[Q8] （必須）講義に対する感想・意見などを書いて下さい。

参考文献

[1] D. Hilbert, Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten, J. Reine Angew. Math. 110 (1892), 104–129.

[2] S. Lang, Diophantine geometry, Interscience Publishers, 1962.

[3] J.-P. Serre, Lectures on the Mordell-Weil theorem, Friedr. Vieweg & Sohn, 1989.

[4] J.-P. Serre, Topics in Galois theory, Jones and Bartlett Publishers, 1992.

[5] M. D. Fried and M. Jarden, Field arithmetic, Springer-Verlag, 1986.