体とは可換環 $R=(R,+,\cdot,0,1)$ であって，以下をみたすものであった：

$0\neq 1$ かつ $\forall a\in R\setminus\{0\},\ \exists b\in R$ s.t. $ab=1=ba$

記法 体の準同型とは（可換）環の準同型写像のことである。

prop K_1, K_2：体，$\varphi: K_1\to K_2$：準同型 は単射である。

☺ $\ker\varphi=:I$ は K_1 の ideal なので $I=\{0\}$ or $I=K_1$。$0\neq 1$ から $I\neq K_1$ が分かる //

注 以上より体では商を考えない

記法 体の間の単射準同型 $K_1\xrightarrow{\varphi}K_2$ を K_1 の拡大という。
しばしば $K_1\subseteq K_2$（部分体 := 部分環で体になっている）を考え，φ は省略する。

記法 K：部分体，S：部分集合 のとき K と S を含む最小の K' の部分体を $K(S)$ と書く。

$\cap$
K'：拡大体

$S=\{s_1,s_2,\dots\}$ のとき $K(S)=K(s_1,s_2,\dots)$ のように書くこともある。

Ex $\mathbb{Q}$ $\sqrt{2}$ で $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ であることは簡単に分かる。
$\cap$
$\mathbb{C}$ //
（$\mathbb{R}$でもよい）

同様に $\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbb{Q}\}$ も分かる。

記法 拡大 $K\xrightarrow{\tau}K'$ について K' は $f\cdot f':=\tau(f)f'$ $(f\in K,\ f'\in K')$ によって K 線型空間の構造をもつ。K' が有限生成（$\Leftrightarrow$ 有限次元）K 線型空間のとき，この拡大を有限次拡大といい，$\dim_K K'=[K':K]_\tau$ を次数という。以下，拡大は主に包含写像の場合を扱う。

Ex $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$, $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$

prop $F_1 \subseteq F_2 \subseteq F_3$：体の拡大において

① $F_3 \supseteq F_1$ が有限次拡大 $\Leftrightarrow$ $F_2 \supseteq F_1$ と $F_3 \supseteq F_2$ が有限次拡大

② ①のとき $[F_3:F_1]=[F_3:F_2]\cdot[F_2:F_1]$

(:) ① $\Rightarrow$：明らか

① $\Leftarrow$：F_2 の F_1 基底を $v_1,\dots,v_m$
(と)
② F_3 の F_2 基底を $w_1,\dots,w_n$
とすると，$\{v_i w_j \mid 1\le i\le m,\ 1\le j\le n\}$ が F_3 の F_1 基底であることが分かる。

応用 コンパスと定規による作図について、以下を示す：

① 一般に角の3等分は不可能

② 立方体の体積2倍の立方体は作図不可能

(:) まず、コンパスと定規による作図の意味をはっきりさせておく。

- 最初に $(0,0)$ と $(1,0)$ が与えられている。
- 円を描くときの中心と半径，直線を書くときの2点はすでにあるものを使う
- 新たな点は，直線又は円の交点とする
- 有限回のステップで終わる。

作図の n ステップ目にえられている座標の数たちを S_n (例えば $S_0=\{0,1\}$)
$K_n=\mathbb{Q}(S_n)\ (\subseteq \mathbb{R})$ とする。

claim $[K_n:K_{n-1}]=1$ or 2 (各自考えよ)

②を示す：$\sqrt[3]{2} \in K_n$ となったとすると，$\mathbb{Q}(\sqrt[3]{2}) \subseteq K_n$

一方で $\mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q}\}$ なので $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$。

連鎖律より $\dim_{\mathbb{Q}} K_n$ は2のべきかつ3の倍数で，これは矛盾。//

①を示すのも同様に $\cos 30^\circ$ は作図可能だが，$\cos 10^\circ$ は作図不可能であることが分かる//

Def 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ において，$\theta \in \mathbb{F}'$ が $\mathbb{F}$ 上代数的 $\overset{\text{def}}{\iff} \exists f \in \mathbb{F}[x]$ s.t. $f(\theta) = 0$ (in $\mathbb{F}'$)

② 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ が代数拡大 $\overset{\text{def}}{\iff} \forall \theta \in \mathbb{F}'$ は $\mathbb{F}$ 上代数的

Ex $\left.\begin{matrix}\mathbb{Q} \subseteq \mathbb{R} \\ \overline{\mathbb{Q}} \subseteq \mathbb{C}\end{matrix}\right\}$ は代数拡大ではないが，$\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ は有限次拡大でない代数拡大

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ は有限次拡大で代数拡大

Prop $\mathbb{F} \subseteq \mathbb{F}'$ が有限次拡大 $\Rightarrow$ 代数拡大

(:) $\forall \theta \in \mathbb{F}'$ について，$\theta^0, \cdots, \theta^n$ は $\mathbb{F}$ 線形関係をもつ（ここで $n := [\mathbb{F}' : \mathbb{F}]$）//

記法 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ と $\theta \in \mathbb{F}'$ について，$I := \{f(x) \in \mathbb{F}[x] \mid f(\theta) = 0 \text{ in } \mathbb{F}'\}$

は $\mathbb{F}[x]$ の ideal である。$I \neq \{0\} \iff \theta : \mathbb{F}$ 上代数的だが，このとき

I の生成元で最高次の係数が1のものを θ の $\mathbb{F}$ 上の最小多項式といって

$\mathrm{Irr}(\mathbb{F}; \theta)$ とこの講義では書くかもしれない。

Prop $\mathbb{F} \subseteq \mathbb{F}'$：拡大，$\theta \in \mathbb{F}'$：$\mathbb{F}$ 代数的で $f(x) := \mathrm{Irr}(\mathbb{F}; \theta)$

このとき $f(x)$ は既約で，$\mathbb{F}(\theta) \overset{\sim}{\leftarrow} \mathbb{F}[x]/(f(x))$

(1) $F[X] \to F(\theta)$ は環準同型なので、 $F[X]/(f(X)) \hookrightarrow F(\theta)$
$f(X) \longmapsto f(\theta)$

よって $F[X]/(f(X))$ は整域なので $f(X)$ は素元 $\Leftrightarrow$ 既約元で(注：Kerを別の方法で)

今、さらに $(f(X))$ は極大idealなので $F[X]/(f(X))$ は体でもある。

つまり $F[X] \twoheadrightarrow F[\theta] \subseteq F(\theta)$ が $F[X]/(f(X)) \xrightarrow{\sim} F[\theta] \subseteq F(\theta)$ を
$f(X) \longmapsto f(\theta)$

誘導し、$F[\theta]$ が体なので $F[\theta] = F(\theta)$ //

系 propの設定で $F(\theta)$ は F の有限次拡大で、$[F(\theta) : F] = \deg f(X) \left(= \deg \mathrm{Irr}(F;\theta)\right)$

系 $F_1 \subseteq F_2 \subseteq F_3$: 拡大において $F_1 \subseteq F_3$: 代数拡大 $\Leftrightarrow$ $F_1 \subseteq F_2$, $F_2 \subseteq F_3$ が共に代数拡大

(1) $\Rightarrow$: 明らか
$\Leftarrow$: $\theta \in F_3$ は F_2 上代数的なので $\mathrm{Irr}(F_2;\theta) = X^m + a_1 X^{m-1} + \cdots + a_m \in F_2[X]$
をとると、$F' = F_1(a_1, \cdots, a_m) = F_1(a_1, \cdots, a_{m-1})(a_m)$ … は
F_1 の有限次拡大。又、$[F'(\theta) : F'] = m$ でもあるので、
$F'(\theta)$ は F_1 の有限次拡大。よって θ は F_1 上代数的 //

注 代数拡大 $F \subseteq F'$ が分離的とは、任意の $\theta \in F'$ について $\mathrm{Irr}(F;\theta)$ が"重根をもたない"ことである。しかし" "をきちんと論じるのは、一般の設定では意外とめんどうなため、この講義では分離拡大という言葉を使わず、主に(1)の部分体で考えることにする(有限体を除いては)が、本当は重要な概念である。

記法 $\mathbb{F}$：体 は可換環なので、ただ1つの環準同型 $\mathbb{Z} \xrightarrow{\exists!} \mathbb{F}$ が存在する。
よって $\mathbb{Z}/\ker \hookrightarrow \mathbb{F}$ で左辺は整域でなければならないので
$\ker = (0)$ or (p) （pは素数）。それぞれに応じて $\mathbb{F}$ は標数0 又は標数p
といって、$\mathrm{char}\,\mathbb{F}=0$ 又は $\mathrm{char}\,\mathbb{F}=p$ のように書く。

Ex $\mathrm{char}\,\mathbb{R}=0$, $\mathrm{char}\,\mathbb{Z}/p\mathbb{Z}=p$ （p：素数）

記法 $\mathbb{Z}/p\mathbb{Z}$ を（体であることを強調する際は）$\mathbb{F}_p$ と書く

prop $\mathbb{F}$：有限体 $\Rightarrow$ $\mathrm{char}\,\mathbb{F}$ は素数pで、$|\mathbb{F}|$ はpのべ

☺ $\mathbb{F}$ は標数に応じて $\mathbb{Q}$ 又は $\mathbb{F}_p$ をふくむ。$\mathbb{F}$ はこれら素体上の線形空間である。

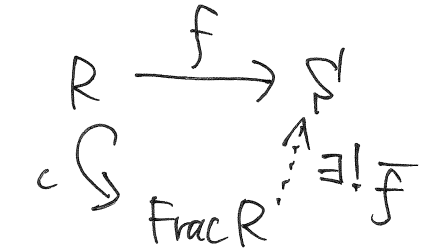
注： 商体について（これは可換環のidealによる商環とは異なる概念である）
Rが整域ならば、$R\times(R\setminus\{0\})$ に $(a,b)\sim(c,d) \overset{\text{def}}{\Longleftrightarrow} ad=bc$
は同値関係になる。(a,b) の同値類を $\frac{a}{b}$ と書くことにすると、
$\mathrm{Frac}(R) := (R\times(R\setminus\{0\}))/\sim$ には $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$, $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$
で2項演算が定義でき、$(\mathrm{Frac}(R), +, \cdot, \frac{0_R}{1_R}, \frac{1_R}{1_R})$ は体になる
ことがcheckできる。

Ex $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}$, $\mathrm{Frac}(\mathbb{Z}[x])=\mathrm{Frac}(\mathbb{Q}[x])=\mathbb{Q}(x)$（1変数有理関数体）

注 構成法 Frac より、整域は体の部分環と同じ概念であることが分かる。
実際 $R \hookrightarrow \mathrm{Frac}(R)$ は単射環準同型である。
$r \longmapsto \frac{r}{1}$

注 $\mathrm{Frac}(R)$ は以下の普遍性をもつことが check できる:

任意の可換環 S' と任意の環準同型 $f: R \to S'$ について, $\forall r \in R \setminus \{0\},\ f(r) \in S'^{\times}$ ならば, $\tilde{f} \circ \iota = f$ なる環準同型 $\tilde{f}: \mathrm{Frac}R \to S'$ がただ1つ存在する。ここで $\iota: R \hookrightarrow \mathrm{Frac}R$ は先の単射環準同型である。



注 以上より $\mathbb{Z} \overset{\iota}{\hookrightarrow} \mathbb{Q}\left(\underset{g}{\overset{f}{\rightrightarrows}} R\right)$ は任意の可換環 R と, 環準同型 $\mathbb{Q} \underset{g}{\overset{f}{\rightrightarrows}} R$ について $f \circ \iota = g \circ \iota \Rightarrow f = g$ を導く。これは $\mathbb{Z} \overset{\iota}{\hookrightarrow} \mathbb{Q}$ が環の圏で "全射のようなもの"(エピ射という) だと言っている。

注 $\mathrm{Frac}R$ は $R:\mathrm{UFD} \Rightarrow R[X]:\mathrm{UFD}$ の証明にも使われる。

($K := \mathrm{Frac}R$ について $K[X]$ は PID なので UFD であることを用いる)

prop 任意の素数 $p \geq 2$ と任意の $n \geq 1$ について, 位数 p^n の体が存在する。

☺ $\left|\{\mathbb{F}_p[X] \text{の} n \text{次既約モニック多項式}\}\right| =: a_n$ について $a_n \neq 0$ を言えばよいが,

(*) $a_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$ が以下の通りである。

ここで $\mu(d) := \begin{cases} 0 & d \text{が平方因子をもつ} \\ (-1)^r & d = p_1 \cdots p_r \ (\text{各 } p_i \text{は相異なる素数}) \end{cases}$ //

Lemma $(x_d)_{d \geq 1}$ について $\sum_{d \mid n} x_d = y_n \Rightarrow x_n = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) y_d$

☺! メビウス反転公式として知られている

ここに $\mathbb{F}_p[X]$ が UFD を使った

(*)の証明 $\prod_{d\geq 1}\left(\frac{1}{1-u^d}\right)^{a_d} \overset{\text{(*)}}{=} \sum_{k\geq 0} p^k u^k = \frac{1}{1-pu}$ in $\mathbb{C}[[u]]$

よって $-\sum_{d\geq 1} a_d \log(1-u^d) = -\log(1-pu)$

$-\log 1-u = u + \frac{u^2}{2} + \frac{u^3}{3} + \cdots$ より u^n の係数を比較すると, $\sum_{d\mid n} d\,a_d = p^n$ //

注 普通, 任意の体 $\mathbb{F}$ について, それを含む代数閉包 $\overline{\mathbb{F}}$ の存在を示し,

$\mathbb{F}_{p^n} = \{u\in\overline{\mathbb{F}_p} \mid u^{p^n}=u\}$ を示す。しかしこの講義では $\overline{\mathbb{F}}$ の存在や"一意性"を示さないため, 初等的な有限体の存在証明を行った。$\overline{\mathbb{F}}$ にふれないことは, 重根の議論をさけたこととも関係している。(c.f. 分離拡大)

prop p: 素数, $n\geq 1$, $\mathbb{F}, \mathbb{F}'$: 体 s.t. $|\mathbb{F}| = |\mathbb{F}'| = p^n \Rightarrow \mathbb{F}\simeq\mathbb{F}'$

(;) $\mathbb{F}^\times \simeq C_{p^n-1}$ だったことを思い出す(有限アーベル群の構造定理を用いて示した)。

よって $\forall x\in\mathbb{F}^\times$, $x^{p^n-1}=1$。よって $\forall x\in\mathbb{F}$, $x^{p^n}=x$

$\mathbb{F}^\times$ の原始根 x_0 を選び, $f(X) = \mathrm{Irr}(\mathbb{F}_p, x_0)$ とする。$f(x)\mid x^{p^n}-x$ である。

$\mathbb{F} = \mathbb{F}_p[x_0] \simeq \mathbb{F}_p[X]/(f(X))$。今, $\forall y\in\mathbb{F}'$, $y^{p^n}-y=0$ でもあるので,

$\exists y_0\in\mathbb{F}'^\times$, $f(y_0)=0$。 $\mathbb{F}'\supseteq \mathbb{F}_p[y_0] \simeq \mathbb{F}_p[X]/(f(X))$

なので $\mathbb{F}' = \mathbb{F}_p[y_0] \simeq \mathbb{F}_p[X]/(f(X)) \simeq \mathbb{F}$ //

記法 位数 p^n の有限体を $\mathbb{F}_{p^n}$ とか $GF(p,n)$ のように書く。

これは同型を除いて一意的だが, 上の prop で自然な同型を選ぶ…ことはできない(と思う)。

応用 フィボナッチ数の周期

$a_0=0,\ a_1=1,\ a_{n+2}=a_n+a_{n+1}\ (n\geq 2)$ で定まる数列 $(a_n)_{n\geq 0}$ を(この講義では)フィボナッチ数列といい、一般項の公式 $a_n=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ は

$p\neq 2,5$ (素数) について $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ で意味をもつ。

Fact $p\neq 2,5$ (素数) について $X^2-5=0$ は既約 in $\mathbb{F}_p[X]$ $\Leftrightarrow$ $p\equiv\pm 1 \pmod 5$

☹ 平方剰余の相互法則 $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ から従う。

ここで p,q : 奇素数で、$\left(\frac{p}{q}\right)=\begin{cases}1 & (\exists x\in\mathbb{F}_q \text{ s.t. } x^2=p \text{ in } \mathbb{F}_q)\\ -1 & (\text{o.w.})\end{cases}$

系 ① $p\equiv\pm 1 \pmod 5$: 素数について、$\forall n\geq 0,\ a_{n+p}=a_n$ in $\mathbb{F}_p$

② $p\equiv\pm 2 \pmod 5$: 素数について、$\forall n\geq 0,\ a_{n+p^2-1}=a_n$ in $\mathbb{F}_p$

Lemma $\mathbb{F}$: 体 s.t. $\mathrm{char}\,\mathbb{F}=p$: 素数 のとき、$\sigma_{\mathbb{F}}:\mathbb{F}\to\mathbb{F}$, $x\mapsto x^p$ は準同型 (フロベニウス射)

☹ $\sigma_{\mathbb{F}}(a+b)=\sigma_{\mathbb{F}}(a)+\sigma_{\mathbb{F}}(b)$ のみ非自明で、これは $0<\forall i<p,\ \binom{p}{i}$ $p\mathbb{Z}$ から従う//

Def $\mathbb{F}\subseteq\mathbb{F}'$: 拡大について、$\mathrm{Gal}_{\mathbb{F}}(\mathbb{F}'):=\{f:\mathbb{F}'\xrightarrow{\sim}\mathbb{F}' : \text{同型 s.t. } f|_{\mathbb{F}}=\mathrm{id}_{\mathbb{F}}\}$ は群

Thm $p\geq 2$: 素数, $n\geq 1$ について $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_{p^n})\simeq C_n\ (=\mathbb{Z}/n\mathbb{Z})$

$\sigma_{\mathbb{F}_{p^n}}^{x} \longleftrightarrow [x]$

☺ $\sigma_{\mathbb{F}_{p^n}}$ は単射なので、全単射。$\therefore \sigma_{\mathbb{F}_{p^n}}\in\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$

又、$\mathbb{F}_{p^n}^{\times}\simeq C_{\varphi(p^n)}$ だったから $\sigma_{\mathbb{F}_{p^n}}$ の位数は n である。よって $|\mathrm{Gal}|\geq n$

さらに $\mathbb{F}_p[X]/(f(X))\simeq\mathbb{F}_{p^n}=\mathbb{F}_p(\theta)$ とすると $\forall\tau\in\mathrm{Gal}$ について

$f(\tau(\theta))=0$ かつ $\tau\neq\tau'\Rightarrow\tau(\theta)\neq\tau'(\theta)$ なので、$|\mathrm{Gal}|\leq n$。//

($\mathrm{Gal}(\mathbb{F}'/\mathbb{F})$ とも書く)

記法 拡大 $\mathbb{F} \subseteq \mathbb{F}'$ と部分群 $G \subseteq \mathrm{Gal}_{\mathbb{F}}(\mathbb{F}')$ について

$\mathbb{F}'^{G} := \{ x \in \mathbb{F}' \mid {}^\forall \tau \in G,\ \tau(x) = x \}$ は $\mathbb{F}$ の拡大体 (で $\mathbb{F}'$ の部分体)

Def 有限次拡大 $\mathbb{F} \subseteq \mathbb{F}'$ がガロア拡大 $\Longleftrightarrow$ $\mathbb{F}'^{\mathrm{Gal}_{\mathbb{F}}(\mathbb{F}')} = \mathbb{F}$

系 $p \geq 2$: 素数, $n \geq 1$ について 拡大 $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ はガロア拡大

ガロアの基本定理とは, ガロア拡大 $\mathbb{F} \subseteq \mathbb{F}'$ について, 中間体 $\mathbb{F} \subseteq M \subseteq \mathbb{F}'$ を $\mathrm{Gal}_{\mathbb{F}}(\mathbb{F}')$ の部分群と 1:1 対応をつけるものである。

系②の精密化 $p \equiv \pm 2 \pmod 5$: 素数について, ${}^\forall n \geq 0$, $a_{n+2(p+1)} = a_n$ in $\mathbb{F}_p$

(∵) このとき $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[x]/(x^2 - x - 1)$ で $\sigma_{\mathbb{F}_{p^2}}$ は $x^2 - x - 1$ の解を入れ替える。

つまり解を $\alpha, \beta \in \mathbb{F}_{p^2}$ とすると, $\alpha^p = \beta$, $\beta^p = \alpha$ なので $\alpha^{p+1} = \beta^{p+1} = -1$。 //

注 フィボナッチ数列の mod n での周期は pisano period と呼ばれ, 様々な研究があるようである。