Poniżej zakładamy że F to ciało i że F oraz elementy które rozważamy są zawarte w pewnym wiekszym ciele U. Wtedy dla $a_1, \ldots, a_n$ z większego ciała U istnieje najmniejsze podciało zawarte w U i zawierające F oraz $a_1, \ldots, a_n$. Aby to pokazać zauważmy że istnieje co najmiej jedno podciało U zawierające F i $a_1, \ldots, a_n$, mianowicie U. Przekrój wszystkich podciał U zawierających F i $a_1, \ldots, a_n$ jest ciałem, zawiera F i $a_1, \ldots, a_n$ a więc jest najmniejszym podciałem U zawierające F i $a_1, \ldots, a_n$. Takie podciało oznaczamy przez $F(a_1, \ldots, a_n)$. Niżej to ciało będziemy oznaczać przez L, tzn. $L = F(a_1, \ldots, a_n)$. W rozumowaniach niżej natura ciała U jest nieistotna, istotne jest że takie ciało istnieje (oznacza to np. że nie ma dzielników zera).

Lemat 0.1 *Każdy element $x \in L$ jest postaci*

$$x = R(a_1, \ldots, a_n) = \frac{P(a_1, \ldots, a_n)}{Q(a_1, \ldots, a_n)}$$

gdzie R jest funkcją wymierną n zmiennych o współczynnikach z F zaś P i Q są wielomianami n zmiennych o współczynnikach z F przy tym $Q(a_1, \ldots, a_n) \neq 0$.

Dowód: Zbiór elementów S które daje się zapisać w postaci wyżej jest zamknięty ze względu na dodawanie, odejmowanie i mnożenie. S jest też zamknięty ze względu na branie odwrotności niezerowych elementów, czyli jest ciałem. Wartości funkcji stałych dają elementy F, czyli S zawiera F. Wartości zmiennych to $a_1, \ldots, a_n$, czyli S zawiera $a_1, \ldots, a_n$. Jako że L jest najmniejszym podciałem U o tej własności to $S = L$. □

Definicja 0.2 *$a_1, \ldots, a_n$ są algebraicznie zależne nad F $\iff$ istnieje niezerowy wielomian Q o współczynnikach w F taki że $Q(a_1, \ldots, a_n) = 0$.*

Definicja 0.3 *$a_1, \ldots, a_n$ są algebraicznie niezależne $\iff$ $a_1, \ldots, a_n$ nie są algebraicznie zależne $\iff$ dla każdego niezerowego wielomianu Q o współczynnikach w F mamy $Q(a_1, \ldots, a_n) \neq 0$.*

Lemat 0.4 *Jeśli $a_1, \ldots, a_n$ są algebraicznie niezależne to L jest izomorficzne z ciałem funkcji wymiernych n zmiennych o współczynnikach z F.*

Dowód: Niech $K = F(X_1, \ldots, X_n)$ będzie ciałem funkcji wymiernych n zmiennych o współczynnikach z F. Dla

$$f(X_1, \ldots, X_n) = \frac{P(X_1, \ldots, X_n)}{Q(X_1, \ldots, X_n)}$$

definiujemy odwzorowanie ϕ wzorem

$$\phi(f(X_1, \ldots, X_n)) = \frac{P(a_1, \ldots, a_n)}{Q(a_1, \ldots, a_n)}.$$

Zauważmy że ϕ jest dobrze zdefiniowane. Mianowicie, skoro $a_1, \ldots, a_n$ są algebraicznie niezależne to $Q(a_1, \ldots, a_n) \neq 0$ i dzielenie jest wykonalne. Wynik nie zmieni się jeśli pomnożymy licznik i mianownik przez ten sam czynnik. Łatwo sprawdzić że ϕ przeprowadza sumę na sumę, różnicę na różnicę, iloczyn na iloczyn, iloraz na iloraz a więc jest homomorfizmem. Jądro ϕ składa się z takich f że $P(a_1, \ldots, a_n) = 0$. Lecz jako że $a_1, \ldots, a_n$ są algebraicznie to wtedy $P = 0$, czyli jądro jest trywialne (składa się tylko z funkcji zerowej). Oznacza to że ϕ jest różnowartościowe. Na mocy Lematu 0.1 ϕ jest na czyli jest izomorfizmem. □

Uwaga: W szczególności dostaniemy izomorficzne L niezależnie od natury $a_1, \ldots, a_n$. Nieważne czy to są zmienne, czy liczby czy też funkcje.

Definicja 0.5 *a jest przestępny nad F $\iff$ ciąg jednoelementowy składający się z a jest algebraicznie niezależny nad F $\iff$ a nie jest pierwiastkiem żadnengo niezerowego wielomianu jednej zmiennej nad F.*

Lemat 0.6 $\exp(x)$ *jest przestępny nad* $F = \mathbb{Q}(x)$.

Dowód: Nie wprost, rozważmy niezerowy wielomian M minimalnego stopnia n taki że $M(\exp(x)) = 0$. Rozpisując mamy

$$c_n(x)\exp(x)^n + c_{n-1}(x)\exp(x)^{n-1} + \cdots + c_0(x) = 0$$

($c_i \in F$ czyli są funkcjami wymiernymi od x). Przy tym $c_n(x) \neq 0$ i $c_0(x) \neq 0$. Mianowicie, gdyby $c_n(x) = 0$ to stopień M byłby mniejszy od n, wbrew wyborowi n. Podobnie, gdyby $c_0(x) = 0$, to dzieląc równanie wyżej przez $\exp(x)$ otrzymalibyśmy równanie niższego stopnia. Dzieląc powyższe równanie przez $c_0(x)$ otrzymujemy równanie postaci

$$d_n(x)\exp(x)^n + d_{n-1}(x)\exp(x)^{n-1} + \cdots + 1 = 0.$$

Różniczkując dostajemy równanie

$$(d_n(x)' + nd_n(x))\exp(x)^n + (d_{n-1}(x)' + (n-1)d_{n-1}(x))\exp(x)^{n-1} +$$

$$\cdots + (d_1(x)' + d_1(x))\exp(x) = 0.$$

Po podzieleniu przez $\exp(x)$ daje to równanie niższego stopnia niż n, a więc wszystkie współczynniki są zerami. W szczególności mamy $d_n(x) \neq 0$ i

$$d_n(x)' + nd_n(x) = 0.$$

Pokażemy że taka równość jest niemożliwa. Mianowicie, zapiszmy

$$d_n(x) = \frac{P(x)}{Q(x)}$$

gdzie P i Q są wielomianami i są względnie pierwsze. Jeśli Q nie jest stałe to dzieli się przez wielomian nierozkładalny S_1. Można zapisać $Q(x) = S_1(x)^k S_2(x)$ gdzie $k \geq 1$ zaś S_2 nie dzieli się przez S_1 (dzielimy Q przez S_1 tyle razy ile się da (czyli k-razy), S_2 to wynik dzielenia). Teraz liczymy pochodną

$$d_n(x)' = \frac{P(x)'Q(x) - Q(x)'P(x)}{Q(x)^2}$$

$$= \frac{P(x)'S_1(x)^k S_2(x) - (kS_1(x)'S_1(x)^{k-1}S_2(x) + S_1(x)^k S_2(x)')P(x)}{S_1(x)^{2k}S_2(x)^2}$$

$$= \frac{P(x)'S_1(x)S_2(x) - kS_1(x)'S_2(x)P(x) - S_1(x)S_2(x)'P(x)}{S_1(x)^{k+1}S_2(x)^2}$$

$$= \frac{-kS_1(x)'S_2(x)P(x) + S_1(x)R(x)}{S_1(x)^{k+1}S_2(x)^2}$$

gdzie $R(x) = P(x)'S_2(x) - S_2(x)'P(x)$. Zauważmy że stopień $S_1(x)'$ jest mniejszy niż stopień S_1, a więc S_1 nie dzieli S_1'. Z wyboru wyżej S_1 nie dzieli S_2. Jako że wybraliśmy nieskracalny zapis ułamka dającego d_n to S_1 nie dzieli P. Lecz wielomian nierozkładalny jest elementem pierwszym w pierścieniu $\mathbb{Q}[x]$, skoro nie dzieli czynników to nie dzieli produktu $S_1(x)'S_2(x)P(x)$. Drugi składnik licznika jest podzielny przez S_1 więc nie wpływa na podzielność całego licznika przez S_1, czyli licznik nie dzieli się przez S_1. A więc S_1^{k+1} z mianownika nie skróci się z licznikiem, czyli w zapisie nieskracalnym $d_n(x)'$ mianownik dzieli się przez S_1^{k+1}. Lecz to oznacza że równość

$$d_n(x)' = -nd_n(x)$$

z niestałym S jest niemożliwa: mianownik lewej strony dzieli się przez S_1^{k+1} zaś mianownik prawej strony nie (najwyższa potęga k przez którą dzieli się mianownik d_n to k). Pozostaje rozważyć przypadek gdy S jest stałą. Wtedy można wziąść $S = 1$ i zapisać $d_n(x) = P(x)$. Lecz stopień $P(x)'$ jest mniejszy niż stopień x więc również w tym przypadku równość

$$d_n(x)' = -nd_n(x)$$

jest niemożliwa. Otrzymana sprzeczność pokazuje że $\exp(x)$ nie może być pierwiastkiem M, czyli jest przestępne nad F. □

Definicja 0.7 *M jest wielomianem minimalnym elementu a $\iff$ $M(a) = 0$, $M \neq 0$ i stopień M jest minimalny.*

Uwaga: Wielomian minimalny jest jednoznaczny z dokładnością do mnożenia przez element z F.

Uwaga: Wielomian minimalny jest nierozkładalny, bo zero M jest zerem jednego z czynników a nietrywialny czynnik ma niższy stopień.

Lemat 0.8 *Jeśli a jest algebraiczy nad F z wielomianym minimalnym M stopnia d to każdy element $x \in F(a)$ można zapisać jednoznacznie w postaci $R(a)$ gdzie R jest wielomianem stopnia mniejszego niż d.*

Dowód: Na mocy Lematu 0.1 element x można zapisać jako

$$x = \frac{P(a)}{Q(a)}$$

gdzie $P, Q \in F(X)$ i $Q(a) \neq 0$. Skoro $Q(a) \neq 0$ to Q nie dzieli się przez M, a więc Q i M są względnie pierwsze. Przy pomocy rozszerzonego algorytmu Euklidesa można znaleźć wielomian A i B takie że

$$1 = A(X)Q(X) + B(X)M(X).$$

Podstawiając a za X otrzymujemy stąd

$$1 = A(a)Q(a) + B(a)M(a) = A(a)Q(a)$$

czyli

$$x = \frac{P(a)}{Q(a)} = P(a)A(a).$$

Dla wielominów nad ciałem jest określone dzielenie z resztą, w szczególności można podzielić $P(X)A(X)$ przez $M(X)$, czyli można zapisać

$$P(X)A(X) = S(X)M(X) + R(X)$$

gdzie stopień R jest mniejszy niż stopień M czyli d. Teraz

$$x = P(a)A(a) = S(a)M(a) + R(a) = R(a)$$

czyli faktycznie x można zapisać w podanej postaci. Zapis jest jednoznaczny, bo gdy $x = R_1(a) = R_2(a)$ to $(R_1 - R_2)(a) = 0$. $R_1 - R_2$ jest wielomianem stopnia mniejszego niż stopień M, więc z definicji wielomianu minimalnego równość $(R_1 - R_2)(a) = 0$ implikuje że $R_1 - R_2$ jest wielomianem zerowym. □