Доказательство. Запишем U в виде произведения подгрупп $U(p)$ для всех простых p, где $U(p)$ есть p-группа. В силу упражнения 22 из гл. I достаточно доказать, что $U(p)$ циклическая для каждого p. Пусть a — элемент из $U(p)$ максимального периода p^r, где r — некоторое целое число. Тогда $x^{p^r}=1$ для всех элементов $x \in U(p)$ и, следовательно, все элементы из $U(p)$ являются корнями многочлена

$$X^{p^r}-1.$$

Циклическая группа, порожденная a, содержит p^r элементов. Если эта циклическая группа не совпадает с $U(p)$, то наш многочлен имеет более чем p^r корней, что невозможно. Следовательно, a порождает $U(p)$, и наша теорема доказана.

Следствие. *Если k — конечное поле, то группа k^* — циклическая.*

Элемент ζ поля k, для которого существует такое целое число $n \geqslant 1$, что $\zeta^n=1$, называется *корнем из единицы* или, более точно, корнем n-й степени из единицы. Таким образом, множество корней n-й степени из единицы — это множество корней многочлена X^n-1. Существует самое большее n таких корней, и они, очевидно, образуют группу, которая, согласно теореме 6, является циклической. Позднее мы изучим корни из единицы более подробно. Образующая группы корней n-й степени из единицы (в том случае, если эта группа имеет порядок n) называется *примитивным* (или *первообразным*) корнем n-й степени из единицы. Например, в поле комплексных чисел $e^{2\pi i/n}$ — примитивный корень n-й степени из единицы, а все корни n-й степени из единицы имеют вид $e^{2\pi i\nu/n}$, где $1 \leqslant \nu \leqslant n$.

§ 5. Простейшие дроби

В этом параграфе мы займемся анализом поля частных кольца главных идеалов, используя факториальность такого кольца.

Теорема 7. *Пусть A — целостное кольцо главных идеалов и P — множество представителей для его неприводимых элементов. Пусть K — поле частных кольца A и α — некоторый элемент из K. Тогда для каждого $p \in P$ найдутся элемент $\alpha_p \in A$ и целое число $j(p) \geqslant 0$, такие, что $j(p)=0$ для почти всех $p \in P$, α_p и $p^{j(p)}$ взаимно просты и*

$$\alpha=\sum_{p \in P} \frac{\alpha_p}{p^{j(p)}}.$$

Если имеется другое такое представление

$$\alpha=\sum_{p\in P}\frac{\beta_p}{p^{i(p)}},$$

то $j(p)=i(p)$ *и* $\alpha_p\equiv\beta_p \bmod p^{j(p)}$ *для всех* p.

Доказательство. Докажем сначала существование такого представления. Пусть a, b — взаимно простые ненулевые элементы из A. Тогда существуют x, $y\in A$, для которых $xa+yb=1$. Следовательно,

$$\frac{1}{ab}=\frac{x}{b}+\frac{y}{a},$$

так что любая дробь c/ab с $c\in A$ может быть разложена в сумму двух дробей (а именно, cx/b и cy/a), знаменатели которых делят b и a соответственно. По индукции отсюда вытекает, что любой элемент $\alpha\in K$ имеет требуемое представление, за тем возможным исключением, что p может делить α_p. Сокращение на наибольший общий делитель приводит к представлению, удовлетворяющему всем нужным условиям.

Что касается единственности, то предположим, что α имеет два представления, указанных в теореме. Пусть q — фиксированный простой элемент из P. Тогда

$$\frac{\alpha_q}{q^{j(q)}}-\frac{\beta_q}{q^{i(q)}}=\sum_{p\neq q}\frac{\beta_p}{p^{i(p)}}-\frac{\alpha_p}{p^{j(p)}}.$$

Если $j(q)=i(q)=0$, то для q наши условия удовлетворяются. Предположим, что одно из чисел $j(q)$, $i(q)$ отлично от нуля, скажем $j(q)>0$ и $j(q)\geqslant i(q)$. Пусть d — наименьшее общее кратное для всех степеней $p^{j(p)}$ и $p^{i(p)}$, таких, что $p\neq q$. Умножим предыдущее равенство на $dq^{j(q)}$. Получим

$$d\,(\alpha_q-q^{j(q)-i(q)}\beta_q)=q^{j(q)}\beta$$

для некоторого $\beta\in A$. Кроме того, d не делится на q. Если $i(q)<$ $<j(q)$, то q делит α_q, что невозможно. Следовательно, $i(q)=j(q)$. Но тогда $\alpha_q-\beta_q$ делится на $q^{j(q)}$, что и доказывает теорему.

Применим теорему 7 к кольцу многочленов $k[X]$ над полем k. Пусть P — множество неприводимых многочленов, нормированных так, чтобы старший коэффициент у них был равен 1. Тогда P будет множеством представителей для всех неприводимых элементов из $k[X]$. В представлении для α, указанном в теореме 7, мы можем теперь разделить α_p на $p^{j(p)}$, т. е. применить алгоритм Евклида, если $\deg\alpha_p\geqslant\deg p^{j(p)}$. Мы обозначаем поле частных кольца $k[X]$ через $k(X)$ и называем его элементы рациональными функциями.

Теорема 8. *Пусть $A = k[X]$ — кольцо многочленов от одной переменной над полем k. Пусть P — множество неприводимых многочленов в $k[X]$ со старшим коэффициентом* 1. *Тогда любой элемент f из $k(X)$ имеет единственное представление в виде*

$$f(X) = \sum_{p \in P} \frac{f_p(X)}{p(X)^{j(p)}} + g(X),$$

где f_p, g — многочлены, $f_p = 0$ при $j(p) = 0$, f_p взаимно прост с p при $j(p) > 0$ и $\deg f_p < \deg p^{j(p)}$ при $j(p) > 0$.

Доказательство. Существование немедленно вытекает из предшествующих замечаний. Единственность следует из того факта, что если имеются два представления с элементами f_p и φ_p соответственно и с многочленами g, h, то $p^{j(p)}$ делит $f_p - \varphi_p$, откуда $f_p - \varphi_p = 0$, а потому $f_p = \varphi_p$, $g = h$.

Можно и дальше разложить член $f_p/p^{j(p)}$, выразив f_p через суммы степеней p. При этом мы добьемся того, что в выражении многочлена f, указанном в теореме 8, будут содержаться лишь так называемые *простейшие дроби* $f_p/p^{j(p)}$, в которых $\deg f_p < \deg p$. В действительности это можно сделать в несколько более общей форме.

Теорема 9. *Пусть k — поле, $k[X]$ — кольцо многочленов от одной переменной, $f, g \in k[X]$. Предположим, что $\deg g \geqslant 1$. Тогда существуют однозначно определенные многочлены*

$$f_0, f_1, \ldots, f_d \in k[X],$$

такие, что $\deg f_i < \deg g$ и

$$f = f_0 + f_1 g + \ldots + f_d g^d.$$

Доказательство. Сначала докажем существование. Если $\deg g > \deg f$, то возьмем $f_0 = f$ и $f_i = 0$ для $i > 0$. Предположим, что $\deg g \leqslant \deg f$. Можно найти многочлены q, r, такие, что

$$f = qg + r, \quad \deg r < \deg g,$$

и так как $\deg g \geqslant 1$, то $\deg q < \deg f$. По индукции существуют многочлены $h_0, h_1, \ldots, h_s$, для которых

$$q = h_0 + h_1 g + \ldots + h_s g^s$$

и, следовательно,

$$f = r + h_0 g + \ldots + h_s g^{s+1},$$

что и доказывает существование.

Что касается единственности, то пусть

$$f = f_0 + f_1 g + \ldots + f_d g^d = \varphi_0 + \varphi_1 g + \ldots + \varphi_m g^m$$

— два разложения, удовлетворяющие условиям теоремы. Добавляя члены, равные 0, к одной из сторон, мы можем считать, что $m = d$. Вычитая, получим

$$0 = (f_0 - \varphi_0) + \ldots + (f_d - \varphi_d) g^d.$$

Следовательно, g делит $f_0 - \varphi_0$, а поскольку $\deg(f_0 - \varphi_0) < \deg g$, то $f_0 = \varphi_0$. Возьмем наименьшее i, для которого $f_i \neq \varphi_i$ (если такое i существует). Разделив наше равенство на g^i, мы найдем, что g делит $f_i - \varphi_i$ и что, следовательно, такого i не может существовать. Это доказывает единственность.

Полученное в теореме 9 разложение f по степеням g мы будем называть *g-адическим разложением* многочлена f. Если $g(X) = X$, то g-адическое разложение совпадает с обычной записью f как многочлена.

§ 6. Однозначность разложения на простые множители многочленов от нескольких переменных

Пусть A — факториальное кольцо и K — его поле частных. Пусть $a \in K$, $a \neq 0$. Мы можем представить a в виде отношения элементов из A, не имеющих общих простых множителей. Если p — простой элемент из A, то

$$a = p^r b,$$

где $b \in K$, r — целое число и p не делит ни числитель, ни знаменатель элемента b. Используя однозначность разложения на простые множители в A, мы тотчас убеждаемся, что число r однозначно определено элементом a. Будем называть r *порядком a в p* (и записывать $r = \operatorname{ord}_p a$). Порядок элемента $a = 0$ в p полагаем равным $+\infty$.

Если $a, a' \in K$ и $aa' \neq 0$, то

$$\operatorname{ord}_p(aa') = \operatorname{ord}_p a + \operatorname{ord}_p a'.$$

Это очевидно.

Пусть $f(X) \in K[X]$ — многочлен от одной переменной

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n.$$

Для $f = 0$ полагаем $\operatorname{ord}_p f = +\infty$. Если $f \neq 0$, то считаем по определению

$$\operatorname{ord}_p f = \min \operatorname{ord}_p a_i,$$

где минимум берется по тем i, для которых $a_i \neq 0$.

Будем называть всякий элемент вида up^r, где $r = \operatorname{ord}_p f$ и u — любая единица в A, *p-содержанием* многочлена f. *Содержанием* f будем называть выражение

$$\prod p^{\operatorname{ord}_p f},$$