4. Симметрические мн-ны

__Опр 1__ Пусть $n>1$, R – комм. ассоц. кольцо с 1 и уже определено кольцо (комм. ассоц. с 1) $R[x_1, x_2, \ldots x_{n-1}]$ от $n-1$ переменной. Кольцо от n переменных $R[x_1, \ldots, x_{n-1}, x_n] = R[x_1, \ldots x_{n-1}][x_n]$, т.е определяется как кольцо от переменной x_n с коэф-ми из $R[x_1 \ldots x_{n-1}]$.

Из опр. 1 и т-мы 1.1. вытекает, что $R[x_1, \ldots x_n]$ – комм. ассоц кольцо с 1.

Далее см. [Вин] гл.5 §4.

5. Идеал кольца и существование корня в расширении поля

В среду в этом параграфе R – асс. комм. кольцо с единицей

Опр 1 Непустое подмн-во I кольца R наз-ся **идеалом** этого кольца, если

1) $\forall a, b \in I \quad a+b \in I$
2) $\forall a \in I \quad -a \in I$
3) $\forall x \in R \ \forall a \in I \quad xa \in I$

Обозн: $I \trianglelefteq R$

Пример 0. $O = \{0\} \trianglelefteq R$ и $R \trianglelefteq R$ в любом кольце R.

1. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$

2. $R = F[x]$ $f(x) \in F[x]$ $I = (f) = \{g \in F[x] : f \mid g\}$

$I \trianglelefteq R$ — идеал, порожд. мн-ком f.

3. Если R — поле и $I \trianglelefteq R$, то $I = R$ или $I = 0$.

Предл 1 Пусть $0 \neq I \trianglelefteq R$. Тогда $\forall x, y \in R$

$$(x+I)+(y+I) = (x+y)+I \text{ и } (x+I)(y+I) = xy+I.$$

Отн-но этих операций мн-во R/I образует ассоц ком. кольцо с 1.

Д-во: Вытекает из опр 1

Опр 2 Кольцо R/I из предл 1 наз-ся фактор кольцом кольца R по идеалу I.

Примеры 0. Если $I = R$, то $R/R \cong 0$ — тривиальное кольцо

1. Если $R = \mathbb{Z}$, $I = n\mathbb{Z}$, то $R/I = \mathbb{Z}_n$ — кольцо вычетов по модулю n.

Предл 2 Пусть $0 \neq I \trianglelefteq R$. Если $I \subseteq J \subseteq R$, то

$$J \trianglelefteq R \iff J = \bigcup_{x \in J} (x + I) \text{ и } J/I = \{x + I \mid x \in J\} \trianglelefteq R/I.$$

Д-во: Упр 1.

Опр 3 Идеал I кольца R наз-ся **максимальным**, если для любого идеала J: $I \subseteq J \subseteq R$ вып-ся либо $J = I$, либо $J = R$

Пример $I \trianglelefteq \mathbb{Z}$ максимален $\iff I = (p)$, где p — простое число

Т-1 Идеал I кольца R максимален $\Leftrightarrow$ R/I — поле

Д-во: $\Leftarrow$) вытекает из предл. 2

$\Rightarrow$) Пусть $I \trianglelefteq R$ максимален. и $u \in R \setminus I$.

Р-м $J = \{xu + a \mid x \in R, a \in I\}$. Несложно показать, что $J \trianglelefteq R$. Т.к. $x \cdot 1 + 0 = x \in J$, то $J \neq I \Rightarrow J = R \Rightarrow 1 = xu + a$ для некоторых $x \in R$ и $a \in I$. Но тогда $(x + I)(u + I) = 1 + I \Rightarrow$ элемент $u + I$ кольца R/I обратим. Поскольку это верно $\forall$ ненулевого эл-та из R/I, R/I — поле $\blacksquare$

Предл 3 Пусть R – евкл. кольцо и $0 \neq I \trianglelefteq R$. Тогда $\exists u \in R$: $I = (u) = \{v \in R : u \mid v\}$.

Д-во: Пусть $0 \neq u \in I$ с наим. возм. нормой и $v \in I$. Тогда $N(u) \leq N(v)$. Разделим v на u с остатком: $v = ua + r$. Эл-т $r = v - ua \in I$ и либо $r = 0$ либо $N(r) < N(u)$. Последнее невозможно, т.к. мы выбирали u как эл-т с наим. нормой в I $\Rightarrow r = 0 \Rightarrow u \mid v$ $\blacksquare$

Следствие Пусть $0 \neq I \trianglelefteq F[x]$. Тогда $\exists f(x) \in F[x]$: $I = (f)$.

Т.2 Пусть R - евклидово кольцо и π - ненулевой необратимый эл-т из R. Фактор-кольцо $R/(\pi)$ - поле $\Leftrightarrow$ π - простой эл-т

Д-во: $\Rightarrow$) Если π разложим, то $\exists$ необр. эл-ты $v, w \in R$: $\pi = vw \Rightarrow (v+I)(w+I) =$
$= I$, где $I = (\pi)$, но тогда в R/I есть делители нуля; противоречие

$\Leftarrow$) Если π - прост, то $\forall x \notin I$ $(\pi, x) = 1 \Rightarrow$
$\exists a, b \in R$: $ax + b\pi = 1 \Rightarrow (a+I)(x+I) =$
$= 1 + I \Rightarrow x$ обратим $\Rightarrow R/I$ - поле. ∎

Т.3 Пусть F — поле и $f(x) \in F[x]$, $\deg f > 0$. Тогда $\exists$ расширение K поля F (т.е. поле K такое, что F — подполе поля K), в котором f имеет корень.

Д-во: Можно считать, что $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$, $\deg f \geq 1$ и f неразложим (см. д-во т.5.5.1 из [ВМ])

Р-м фактор-кольцо $K = F[t] / (f(t))$.

По т. 2 K — поле. Отождествляя мн-ны нулевой степени (вместе с нулевым мн-ном) из K с эл-ми поля F, получаем, что K — расширение поля F. Р-м эл-т $\alpha = t + I$, где $I = (f)$ из K.

Имеем

$$(*)\ f(\alpha) = a_0 + a_1(t+I) + \ldots + a_{n-1}(t+I)^{n-1} + (t+I)^n =$$

$$= a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} + t^n + I = f(t) + I = 0 + I$$

$\Rightarrow \alpha \in K$ – корень мн-на $f(x)$ в поле K $\blacksquare$

Далее см. § 5.5 из [ВМ] $\blacksquare$