ISSN 1680-9165

НАУЧНЫЙ ЖУРНАЛ
ПАВЛОДАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. С. ТОРАЙГЫРОВА

4'2002

НАУКА И ТЕХНИКА КАЗАХСТАНА

ҚАЗАҚСТАН ҒЫЛЫМЫ МЕН ТЕХНИКАСЫ

10-летию

НЕЗАВИСИМОСТИ РЕСПУБЛИКИ КАЗАХСТАН

посвящается

№4 `2002

ҚАЗАҚСТАН ҒЫЛЫМЫ МЕН ТЕХНИКАСЫ

С. ТОРАЙҒЫРОВ АТЫНДАҒЫ ПАВЛОДАР МЕМЛЕКЕТТІК УНИВЕРСИТЕТІНІҢ ҒЫЛЫМИ ЖУРНАЛЫ

МАЗМҰНЫ

Жаратылыстану ғылымдары

Адрес редакции:
637034, г. Павлодар,
ул. Ломова, 64.
Тел.: (3182) 45-11-43
(3182) 45-38-60
Факс: (3182) 45-11-23
E-mail: publish@psu.kz
nauka@psu.kz

УДК 378.146.51

О ПРЕДСТАВЛЕНИИ КОЛЬЦА ЦЕЛЫХ ЧИСЕЛ И КОЛЬЦА МНОГОЧЛЕНОВ

Б.Н. Дроботун

Павлодарский государственный университет им.С.Торайгырова

Жұмыста абстрактілі берілген алгебралық жүйелерді құрылысы таныс жүйелерге келтіріп, оқытуға негізделген құрылымдарды қолдануға қатысты, методологиялық сипаттағы нұсқаулар беріледі.

В работе даются рекомендации методологического характера к применению конструкций, сводящих изучение абстрактно заданных алгебраических систем к системам, строение которых известно.

In activity the guidelines of methodological nature to application of designs reducing analysis abstract of given algebraic systems to systems are given the constitution which one is known.

§1. В рамках вузовской дисциплины "Алгебра и теория чисел" изучаются классические алгебраические системы: группы, кольца, поля и простейшие конструкции, посредством которых из этих систем получаются новые алгебраические системы.

Многолетняя практика преподавания данной дисциплины показывает, что редкие студенты в полном объеме усваивают методологию применения этих конструкций, в частности конструкций, связанных с построением фактор-систем. Это вызвано в первую очередь тем, что главенствующее положение в школьной математике занимают традиционные разделы, связанные с изучением конкретных числовых структур. Хотя в рамках школьных программ и изучается "буквенная алгебра", уровень ее изучения таков, что в качестве областей значений букв предполагаются изначально те или иные числовые множества (и только!), что ни в коей мере не способствует формированию современных представлений об алгебраических операциях, алгебрах, моделях и их свойствах.

Автором при изложении материала разделов, связанных с построением фактор-систем, применялись различные подходы, но наиболее плодотворным оказался подход, основанный на выявлении глубоких, не предполагаемых ранее, аналогий; акцентировании внимания студентов на общности идей и однотипности конструкций, определяющих общую методологию их применения.

В данной работе даются некоторые рекомендации методологического характера, связанные с теорией полей, в основе которых лежат далеко идущие аналогии между кольцом целых чисел и кольцом полиномов над полем. Наличие этих аналогий обусловлено тем, что данные кольца являются факториальными, т.е. каждое из них является целостным; в каждом из них однотипными способами строится теория делимости; в частности, действует алгоритм деления с остатком, определяются простые элементы; имеет место однозначность разложения на простые множители; оба этих кольца являются кольцами главных идеалов.

Выбор рассматриваемых ниже фрагментов теории чисел и теории полей обусловлен местом, которое занимают числа и многочлены в современной математике, а также тем, что глубокие аналогии между числами и многочленами определяют не менее глубокие аналогии между их представлениями. Кроме того, конструкции, применяемые в теории полей для описания типов простых подполей и построения простого алгебраического расширения поля и вызывающие наибольшие затруднения у студентов, используют кольца целых чисел и многочленов над полями в качестве естественных прообразов.

Общая схема S, позволяющая, в определенных случаях, представлять новые, абстрактно заданные, системы (B) посредством систем (A), строение которых известно, выглядит следующим образом.

A. Находим гомоморфное отображение φ системы A на B (если, конечно, это возможно). В случае конкретных систем (A) с известным строением и абстрактно (т.е. аксиоматически) заданных систем (B) из самых общих соображений, основывающихся на аксиомах, задающих абстрактные системы, нередко удается предугадать характер такого отображения.

B. Находим ядро $(\ker\varphi)$ этого гомоморфизма, т.е. даем характеризацию его элементов на языке (в терминах) операций известной системы (A).

C. Рассматриваем два исчерпывающих возможные исходы, случая.

C.1. Ядро гомоморфизма φ является нулевым $(\ker\varphi = \{0\})$. При этом исходе система B, с точностью до изоморфизма, совпадает с A $(B \cong A)$.

C.2. Ядро гомоморфизма φ содержит элементы, отличные от нуля $(\ker\varphi \neq \{0\})$. При таком исходе, согласно теореме о гомоморфизмах, система B, с точностью до изоморфизма, совпадает с некоторой фактор-структурой системы $A\,(B \cong A/\ker\varphi)$.

Именно этим методом были получены многие глубокие результаты математики, представляющие абстрактные системы через конкретные (так называемые теоремы о представлениях). Отметим, что на этом пути находит реализацию один из важнейших принципов познания: переход от конкретного к абстрактному.

Некоторые методические рекомендации к изучению разделов алгебры в вузе, связанных с этой проблематикой, даны автором в [1].

§2. Проследим реализацию схемы **S** на примерах описания типов простых подполей и строения простого алгебраического расширения подполя абстрактно заданного поля. В этих примерах, в качестве конкретных систем с известными свойствами, как раз и будут выступать кольца целых чисел и многочленов над полем соответственно. В процессе реализации этой схемы будет выявлена полная идентичность применяемых конструкций.

В работе автор придерживается терминологии и системы символических обозначений из [2],[3]. В [2]- одном из основных действующих учебников по алгебре и теории чисел даются следующие определения.

Определение 1. Поле называется простым, если оно не имеет собственных подполей.

Определение 2. Пусть P - подполе поля F и $\alpha \in \mathrm{F}$. Простым расширением поля P с помощью элемента α называется наименьшее подполе поля F, содержащее множество P и элемент α.

Отметим, что эти определения описывают два однотипных понятия как бы на разных языках, что уже на уровне определений затушевывает общность подходов к их дальнейшему изучению. В соответствии с этим желательно и простое подполе и простое алгебраическое расширение данного поля с помощью данного элемента определить по одной и той же схеме, реализуя их как наименьшие элементы некоторого частично упорядоченного множества подполей данного поля. На указанном пути получается как бы "внешнее" описание изучаемых объектов. Для этого, обобщая ситуацию, нужно дать такие определения.

Определение 1г. Простым подполем данного поля F называется наименьшее подполе P этого поля.

Определение 2г. Простым подполем данного поля F с условием s называется наименьшее подполе P_s этого поля с условием s.

Заметим, что при таком подходе определение 1г становится частным случаем определения 2г (в качестве условия s здесь нужно взять любое условие, которое выполняется для всех подполей поля F).

Давая "внешнюю" характеризацию полей P и P_s, полезно предварительно отметить, что:

1) понятие подполя является "наследственным" относительно расширений полей;

2) пересечение любой совокупности подполей поля F является подполем этого поля;

3) совокупность $B(F)$ - всех подполей поля F и $B_s(F)$ - всех подполей поля F; удовлетворяющих условию s, образует (по отношению включения "$\subseteq$") частично упорядоченные множества (ч. у. м.) $< B(F);\subseteq >$ (1) и $< B_s(F);\subseteq >$ (2) соответственно.

В связи с этим ч. у. м. (1) и (2) имеют наименьшие элементы:

$$P = \bigcap_{P'\in B(F)} P' \; ; \; P_S = \bigcap_{P'\in B_S(F)} P' \; ,$$

которые и будут искомыми простым подполем и простым подполем с условием s поля F.

Далее нужно конкретизировать условие s для получения простого алгебраического расширения, как поля P_s. Для этого рассматриваются следующие исходные данные: P подполе поля F и элемент $\alpha \in F$. Тогда условие s выглядит так: "содержать поле P и элемент α ", т.е. $P' \in B_S(F)$ тогда и только тогда, когда $\mathrm{P} \subseteq \mathrm{P}$ и $\alpha \in \mathrm{P}'$. При этом конкретном условии s поле P_S обозначается $P(\alpha)$. "Внешнее" описание подполей P и $P(\alpha)$ поля F желательно проиллюстрировать на диаграммах (см. рис. 1. а),б)).

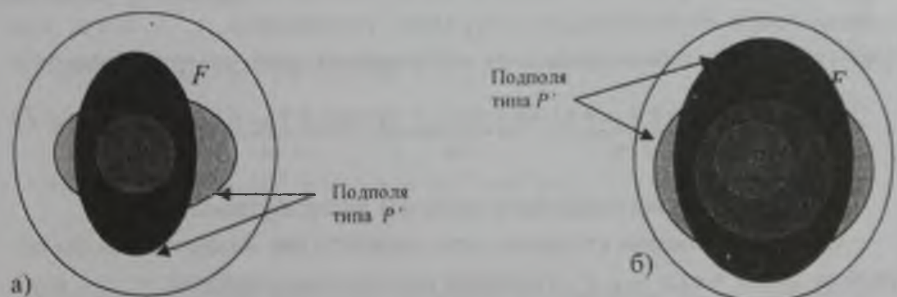

Рис 1

В заключение разбора "внешнего" описания полей P и $P(\alpha)$ следует обратить внимание студентов, что этим описанием поля P и $P(\alpha)$ определяются однозначно.

Далее делается естественный переход к “внутреннему” описанию полей P и $P(\alpha)$, т. е. описанию их в терминах основных операций поля

$$F = \langle \mathrm{F}; +; \cdot; -; \mathbf{o}; \mathbf{e} \rangle.$$

Дальнейшее изложение работы будет осуществлятся параллельным образом: материал, относящийся к полю P, будет даваться под номером I, а относящийся к полю $P(\alpha)$ - под номером II.

I. Так как подполе P должно быть замкнуто относительно основных операций поля F, то

$$\mathbf{o};\ \mathbf{e};\ \underbrace{\mathbf{e}+\mathbf{e}+\ldots+\mathbf{e}}_{n\ \text{раз}}\ (3);\ -(\underbrace{\mathbf{e}+\mathbf{e}+\ldots+\mathbf{e}}_{n\ \text{раз}}) \in \mathrm{P}\ (n \in \mathrm{N})$$

Обозначая, как обычно запись вида (3) через $n\mathbf{e}$ $((-n)\mathbf{e})$ $(n \in \mathrm{N})$, мы получаем, что

$$\mathrm{P}^{\bullet} = \{m\mathbf{e}/m \in Z\} \subseteq \mathrm{P}$$

Здесь необходимо предостеречь студентов, что выражение $m\mathbf{e}$ ни в коем случае не должно восприниматься как произведение целого числа m на еденицу $\mathbf{e}$ поля F. Далее нужно отметить, что множество $\mathrm{P}^{\bullet}$ замкнуто относительно операций $+; \cdot; -; \mathbf{o}; \mathbf{e}$, т. е. система $P^{\bullet} = \langle \mathrm{P}^{\bullet}; +; \cdot; -; \mathbf{o}; \mathbf{e} \rangle$ является подкольцом поля P. При этом, доказывая замкнутость множества $\mathrm{P}^{\bullet}$ относительно операций кольца, желательно продемонстрировать “работу” аксиом, определяющих поле F. В частности, при доказательстве замкнутости относительно операции умножения, т. е. того, что $(r\mathbf{e}) \cdot (s\mathbf{e}) = (rs)\mathbf{e}$ нужно применить обобщенный закон дистрибутивности:

$$(r\mathbf{e}) \cdot (s\mathbf{e}) = (\underbrace{\mathbf{e}+\mathbf{e}+\ldots+\mathbf{e}}_{r\ \text{раз}}) \cdot (\underbrace{\mathbf{e}+\mathbf{e}+\ldots+\mathbf{e}}_{s\ \text{раз}}) = \underbrace{\mathbf{e}+\mathbf{e}+\ldots+\mathbf{e}}_{rs\ \text{раз}} = (rs)\mathbf{e} \quad (r, s \in Z)$$

который является следствием аксиомы дистрибутивности.

Обратив внимание студентов, что элементы $m\mathbf{e}$ являются как бы образами целых чисел $m \in Z$, а правила выполнения операций $+; \cdot; -$ в $P^{\bullet}$ над ними аналогичны правилам выполнения операций $+; \cdot; -$ в Z:

$(r\mathbf{e}) + (s\mathbf{e}) = (r+s)\mathbf{e}$ (4);
$(r\mathbf{e}) \cdot (s\mathbf{e}) = (rs)\mathbf{e}$ (5);
$-(r\mathbf{e}) = (-r)\mathbf{e}$ (6).

обосновать естественность дальнейшего шага сравнения колец Z и P^*.

II. Аналогично, подполе $P(\alpha)$ должно быть замкнуто относительно операций поля F. Так как $\alpha \in P(\alpha)$, то все произведения вида $\underbrace{\alpha \cdot \alpha \cdot \ldots \cdot \alpha}_{k\ \text{раз}} = \alpha^k$ $(k \in N)$ должны принадлежать $P(\alpha)$. Таким образом, получаем, что $\{\alpha^k / k \in N\} \subseteq P(\alpha)$. Так как $P \subseteq P(\alpha)$, то все произведения вида $a \cdot \alpha^k$ также должны лежать в $P(\alpha)$, для любого $a \in P$. А так как $P(\alpha)$ замкнуто относительно сложения, то и всевозможные суммы вида

$$(a_0 \cdot \alpha^{k_0}) + (a_1 \cdot \alpha^{k_1}) + \ldots + (a_t \cdot \alpha^{k_t})(a_i \in P; k_i \in N; i = 0, 1, \ldots, t) \quad (7)$$

также должны лежать в $P(\alpha)$.

Далее, как и выше, необходимо отметить, что множество

$$P[\alpha] = \left\{ (a_0 \cdot \alpha^{k_0}) + (a_1 \cdot \alpha^{k_1}) + \ldots + (a_t \cdot \alpha^{k_t}) \Big/ (a_i \in P; k_i \in N; i = 0, 1, \ldots, t) \right\}$$

замкнуто относительно операций $+; \cdot; -;$ **o** ; **e** поля F, т. е. является подкольцом поля $P(\alpha)$. При этом, при доказательстве замкнутости, опять же полезно продемонстрировать использование аксиом поля, а не полагаться на школьные представления о действиях над многочленами. В частности, при доказательстве замкнутости $P[\alpha]$ относительно умножения, нужно применить обобщенный закон дистрибутивности и затем законы ассоциативности и коммутативности. В соответствии с этим, при умножении одночленов $a_i \cdot \alpha^{k_i}$; $a_j \cdot \alpha^{k_j}$ $(a_i; a_j \in P; k_i, k_j \in N; i, j = 0, 1, \ldots, t)$ последовательно получаем:

$$(a_i \cdot \alpha^{k_i}) \cdot (a_j \cdot \alpha^{k_j}) = ((a_i \cdot \alpha^{k_i}) \cdot a_j) \cdot \alpha^{k_j} =$$
$$= (a_i \cdot (\alpha^{k_i} \cdot a_j)) \cdot \alpha^{k_j} = (a_i (a_j \cdot \alpha^{k_i})) \cdot \alpha^{k_j} =$$
$$= ((a_i \cdot a_j) \cdot \alpha^{k_i}) \cdot \alpha^{k_j} = (a_i \cdot a_j) \cdot (\alpha^{k_i} \cdot \alpha^{k_j}) =$$
$$= (a_i \cdot a_j) \cdot \alpha^{k_i + k_j}.$$

Далее естественно обратить внимание студентов на то, что элементы из $P(\alpha)$ вида (7) напоминают многочлены от α над полем P (вернее являются значениями многочленов от одной переменной x над полем P в точке α) и правила выполнения операций $+; \cdot; -;$ **o** ; **e** над ними аналогичны правилам выполнения операций $+; \cdot; -;$ **o** ; **e** в кольце $P[x]$ многочленов от одной переменной над полем P:

$f(\alpha)+g(\alpha)=(f(x)+g(x))(\alpha)$ (8);
$f(\alpha)\cdot g(\alpha)=(f(x)\cdot g(x))(\alpha)$ (9);
$-f(x)=(-f(x))(\alpha)$ (10)

и затем, основываясь на этом, сравнить кольца $P[x]$ и $P[\alpha]$.

В качестве "инструмента сравнения " в обоих случаях используется гомоморфизм ранее детально изученной системы в определяемую, т. е., начиная с этого момента, реализуется схема **S**.

I. Отображение φ кольца Z в кольцо P^{*} определяется по правилу:

$$(\forall n \in Z)(\varphi(n) = n\mathbf{e})\ .(11)$$

Равенства (4), (5), (6), специфика которых и предопределила правило (11), показывают, что это отображение "сохраняет" кольцевые операции. Действительно, пусть n, $m \in Z$ и $n+m=r$; $n \cdot m = s$. Тогда:

$$\varphi(n+m)=\varphi(r)=r\mathbf{e}=(n+m)\mathbf{e}=(n\mathbf{e})+(m\mathbf{e})=\varphi(n)+\varphi(m).$$

Аналогичным образом,

$$\varphi(n\cdot m)=\varphi(s)=s\mathbf{e}=(n\cdot m)\mathbf{e}=(n\mathbf{e})\cdot(m\mathbf{e})=\varphi(n)\cdot\varphi(m);$$
$$\varphi(-n)=(-\varphi(n)).$$

Кроме того, из определения (11) следует, что $\varphi(1)=\mathbf{e}; \varphi(0)=\mathbf{o}$. Очевидно также, что отображение φ является гомоморфизмом "на".

Для наглядности желательно изобразить действие гомоморфизма φ на диаграмме (см. рис. 2).

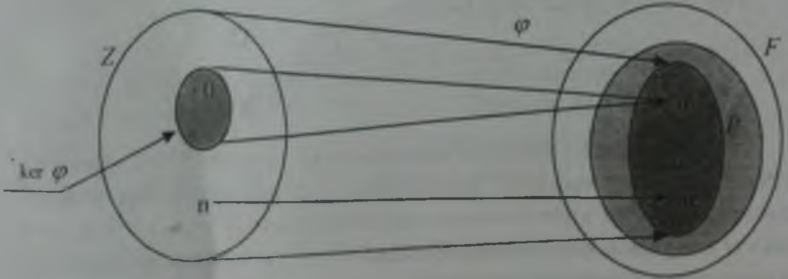

Рис 2

II. Отображение кольца $P[x]$ в кольцо $P[\alpha]$ определим по правилу:

$$(\forall\ h(x) \in \mathrm{P}[x])(\psi(h(\mathrm{x})) = h(a)). \quad (12)$$

Равенства (8), (9), (10), которые и в этом случае подсказали правило (12) определения , показывают, что "сохраняет" кольцевые операции кольца $P[x]$. Действительно, пусть $\mathrm{s}(x);\mathrm{r}(\mathrm{x}) \in \mathrm{P}[x]$ и $\mathrm{s}(x) + \mathrm{r}(\mathrm{x}) = \mathrm{g}(x);\ \mathrm{s}(x) \cdot \mathrm{r}(x) = \mathrm{h}(x)$.

Тогда:

$$(\mathrm{s}(x) + \mathrm{r}(x)) = \psi(\mathrm{g}(x)) = \mathrm{g}(\alpha) = \mathrm{s}(\alpha) + \mathrm{r}(\alpha) = \psi(\mathrm{s}(x)) + \psi(\mathrm{r}(x)).$$

Аналогично,

$$(\mathrm{s}(x) \cdot \mathrm{r}(x)) = \psi(\mathrm{h}(x)) = \mathrm{h}(\alpha) = \mathrm{s}(\alpha) \cdot \mathrm{r}(\alpha) = \psi(\mathrm{s}(x)) \cdot \psi(\mathrm{r}(x));$$
$$(-\mathrm{s}(x)) = -\psi(\mathrm{s}(x)).$$

Из (12) непосредственно следует, что, как и в I, $(0) = \mathbf{o}$; $\psi(1) = \mathbf{e}$ и что ψ - гомоморфизм "на" и что на P отображение ψ действует тождественным образом (см. рис. 3).

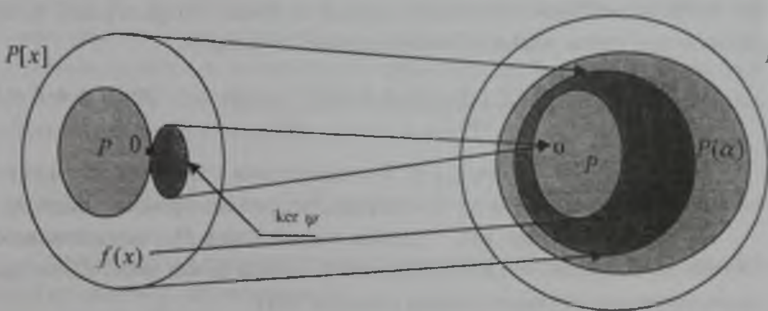

Рис 3

Далее, согласно схеме **S**, описываем ядра гомоморфизмов φ и ψ, при этом рассматриваем только случай в.2, ввиду очевидности случая в.1.

$$\text{I.}\quad \ker\varphi = \left\{ \mathrm{n} \middle/ \mathrm{n} \in \mathrm{Z} \,\&\, \varphi(\mathrm{n}) = 0 \right\} = \left\{ \mathrm{n} \middle/ \mathrm{n} \in \mathrm{Z} \,\&\, \mathbf{n e} = \mathbf{o} \right\}.$$

Таким образом, целое число n попадает в ядро тогда и только тогда, когда единичный элемент **e** поля F, будучи сложенным сам с собой n раз, даст нулевой элемент **o** этого поля. Учитывая, что ядро кольцевого гомоморфизма является идеалом и что кольцо Z является кольцом главных идеалов, получаем: $\ker\varphi = (p)$ для некоторого $p \in \mathrm{Z}$. Желательно вместе со студентами восстановить доказательство этого важного факта, напомнив, что число p, порождающее идеал $\ker\varphi$, выбирается как наименьшее положительное число, принадлежащее этому идеалу (т. е. определяется однозначно), а затем показать, что p является простым числом. При доказательстве первого утверждения использовать алгоритм деления с остатком в кольце Z, а второго – целостность этого кольца. Следует отметить, что при доказательстве второго утверждения (проводимого методом от противного), сделав естественный переход от равенства $p = \mathrm{r}\cdot\mathrm{s}$ $(1<\mathrm{r}<p;\ 1<\mathrm{s}<p)$ к равенству $p\mathbf{e} = (\mathrm{r}\cdot\mathrm{s})\mathbf{e}$, редкие студенты способны правильно обосновать равенство $(\mathrm{r}\cdot\mathrm{s})\mathbf{e} = (\mathrm{r}\mathbf{e})\cdot(\mathrm{s}\mathbf{e})$, основой которого также служит обобщенный закон ассоциативности.

В заключение необходимо объяснить студентам, что простое число p, определенное выше, заключает в себе важнейшую информацию о поле F в целом, в том смысле, что хотя число p определялось, исходя из элемента **e**, как наименьшее число слагаемых, равных **e**, сумма которых равна **o**, подобным свойством обладает любой элемент a поля F:

$$\underbrace{\mathrm{a}+\mathrm{a}+\ldots+\mathrm{a}}_{p\ \text{раз}} = \underbrace{\mathbf{e}\cdot\mathrm{a}+\mathbf{e}\cdot\mathrm{a}+\ldots+\mathbf{e}\cdot\mathrm{a}}_{p\ \text{раз}} = \underbrace{(\mathbf{e}+\mathbf{e}+\ldots+\mathbf{e})}_{p\ \text{раз}}\cdot\mathrm{a} = (p\mathbf{e})\cdot\mathrm{a} = \mathbf{o}\cdot\mathrm{a} = \mathbf{o}$$

т. е. $p\mathrm{a} = \mathbf{o}$ для любого $\mathrm{a} \in \mathrm{F}$. В соответствии с этим, число p и называется характеристикой поля F и определяет тип его простого подполя.

II. Описание идеала ker кольца многочленов $P[x]$ осуществляется по тому же сценарию что и описание $\ker\varphi$ кольца целых чисел Z благодаря наличию аналогичных свойств у кольца $P[x]$:

$$\ker\psi = \left\{ \mathrm{h}(x) \middle/ \mathrm{h}(x) \in \mathrm{P}(x) \,\&\, \psi(\mathrm{h}(x)) = \mathbf{o} \right\} = \left\{ \mathrm{h}(x) \middle/ \mathrm{h}(x) \in \mathrm{P}(x) \,\&\, \mathrm{h}(\alpha) = \mathbf{o} \right\},$$

т. е. $\mathrm{h}(x) \in \ker\psi$ тогда и только тогда, когда значение многочлена $\mathrm{h}(x)$ в точке α равно **o** (т. е. элемент α является корнем этого многочлена). В силу того, что идеал ker является главным, существует многочлен

$f(x) \in \ker\psi$ такой, что $\ker\psi = (f(x))$. Как и в п.I напоминается, что $f(x)$ выбирается, как нормированный многочлен наименьшей степени; доказывается, что он определяется однозначно и что он неприводим над полем P.

В заключение желательно объяснить студентам, что, подобно простому числу p из п.I, нормированный, неприводимый над P, многочлен $f(x)$ заключает в себе важную информацию о строении поля $P(\alpha)$ и, в связи с этим, называется характеристическим многочленом.

Далее, используя теорему о гомоморфизмах, получаем:

I. $P^* \cong Z/(p)$. Так как p^* - подкольцо поля F, то изоморфное ему кольцо $Z/(p)$ является областью целостности. На этом этапе полезно восстановить вместе со студентами тот факт, что всякий ненулевой элемент этого фактор-кольца обратим. Для этого проще всего воспользоваться следствием из алгоритма Евклида о представимости наибольшего общего делителя двух целых чисел в виде линейной комбинации этих чисел с целыми коэффициентами. Действительно, если $\mathrm{n} + (\mathrm{p}) \neq (\mathrm{p})$, то $(\mathrm{n}; \mathrm{p}) = 1$, т. е. существуют такие целые числа $u, v \in Z$, что $(u \cdot \mathrm{n}) + (v \cdot p) = 1$. Аналогом этого равенства в фактор-кольце будет равенство:

$$(u + (p)) \cdot (\mathrm{n} + (p)) + (v + (p)) \cdot (\mathrm{o} + (p)) = 1 + (p)$$

или $(u + (p)) \cdot (\mathrm{n} + (p)) = 1 + (p)$, которое показывает, что элемент $u + (p)$ является обратным к $\mathrm{n} + (p)$. Отсюда следует, что $Z/(p)$, а следовательно и p^*, является полем. А так как P, в соответствии с определением 1г, наименьшее подполе поля F и $P^* \subseteq P$, то $P^* = P$.

Таким образом, в случае поля F характеристики $p \neq 0$, простое подполе этого поля, с точностью до изоморфизма, совпадает с полем вычетов кольца целых чисел по модулю p, т. е. поля

$$Z/(2);\ Z/(3);\ Z/(5);\ \dots;\ Z/(p);\ \dots$$

с точностью до изоморфизма исчерпывают типы простых подполей полей не- нулевой характеристики.

II. $P[\alpha] \cong P[x]/(f(x))$. Совершенно аналогичным п.I образом показывается, что $P[x]/(f(x))$ - поле и, следовательно, по тем же причинам, что и в п.I, $P(\alpha) = P[\alpha]$. Элемент α, в этом случае, называется алгебраическим над полем P, а степень полинома $f(x)$-его степенью. Описание простого алгебраического расширения $P(\alpha)$ наиболее информативно дается в терминах векторного пространства:

Если α - алгебраический над полем P элемент степени n, то $P(\alpha)$ - векторное пространство над полем P размерности n, причем элементы $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ составляют его базис (над P).

В случае в.1 схемы S на основе того, что

а) наименьшим полем, включающим в себя целостное кольцо, является поле частных этого кольца;

б) поля частных изоморфных целостных колец являются изоморфными; заключаем

I. Простое подполе P поля F изоморфно полю рациональных чисел.

II. Простое алгебраическое расширение $P(\alpha)$ поля P посредством элемента α изоморфно полю рациональных функций от одной переменной x.

ЛИТЕРАТУРА

1. Дроботун Б.Н. К вопросу построения фактор-систем // Наука и техника Казахстана. -2001. -№1. - С. 73–79.

2. Ван дер Варден Б. Л. Алгебра. -М.: Наука, 1979. -624 с.

3. Куликов Л. Я. Алгебра и теория чисел. -М.: Высшая школа, 1979. -559 с.