Факториальные кольца.

Определим некоторые операции над идеалами (хотя непосредственно в этой лекции они и не понадобятся).

Определение 1. Пусть I_1, I_2 — идеалы в кольце R. Положим $I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$, $I_1 I_2 = \{\sum_{i=1}^{k} a_i b_i \mid a_i \in I_1, b_i \in I_2\}$, $I_3 = \{a \mid a \in R, aI_1 \subset I_2\}$.

Упражнение 1. Это идеалы, причём $I_1 I_3 \subset I_2$.

Определение 2. Идеал I кольца R называется *максимальным*, если любой идеал, который строго содержит I, совпадает с R.

Определение 3. Идеал I кольца R называется *простым*, если из $ab \in I$ следует, что либо $a \in I$, либо $b \in I$.

Примеры. Идеал $(p) \subset \mathbb{Z}$ максимален тогда и только тогда, когда p — простое число. Это также необходимое и достаточное условие простоты идеала для кольца $\mathbb{Z}$. (Собственно говоря, простые идеалы потому так и называются.) Простые идеалы не всегда максимальны; так, например, идеал $(x) \subset \mathbb{Z}[x]$ прост, но не максимален. Наоборот, максимальный идеал прост (докажите!).

Определение 4. Пусть I — идеал кольца R. Будем говорить, что $a, b \in R$ *лежат в одном классе вычетов по модулю* I, если $a - b \in I$. Обозначим множество классов вычетов через R/I. На этом множестве можно ввести структуру кольца. Это кольцо называется *факторкольцом кольца* R *по идеалу* I.

Упражнение 2. Объясните, как именно устроена структура кольца на R/I.

Примеры. В этих терминах идеал прост тогда и только тогда, когда факторкольцо по нему не содержит делителей нуля. Идеал максимален тогда и только тогда, когда факторкольцо по нему не содержит нетривиальных идеалов. Факторкольцо кольца $\mathbb{R}[x]$ по идеалу (x^2+1), изоморфно $\mathbb{C}$ (если говорить немного неформально, то i соответствует класс вычетов, содержащий x).

В прошлый раз обсуждалось, почему целостное кольцо главных идеалов факториально. На лекции не было объяснено, почему разложение существует. Один из возможных путей ответа на этот вопрос указан в материалах по прошлой лекции (а именно, там было доказано, что в кольце главных идеалов не существует бесконечной строго возрастающей цепочки идеалов). Другой способ основан на использовании одного из следствий так называемой *аксиомы выбора.*

Лемма Цорна. Пусть P — множество всех подмножеств множества S. Пусть $Y \subset P$ таково, что вместе с любой возрастающей цепочкой подмножеств множества S оно содержит их объединение:

$$(X_1 \subset X_2 \subset \dots,\ X_i \in Y) \Rightarrow (\bigcup_i X_i \in Y).$$

Тогда Y содержит по крайней мере один максимальный элемент M, т. е. элемент, для которого нет $N \in Y$, $M \subset N$.

Упражнение 3. Используйте лемму Цорна для доказательства существования разложения (вместо того, чтобы использовать утверждение об обрыве цепочек).

Итак, целостное кольцо главных идеалов факториально. Верно ли обратное? Нет. Мы докажем сейчас, что кольцо многочленов с целыми коэффициентами факториально. Напомним, что оно не является кольцом главных идеалов.

Мотивировкой дальнейших действий является следующая простая идея. Многочлен с целыми коэффициентами можно временно счесть многочленом с рациональными коэффициентами. Многочлены с рациональными коэффициентами мы умеем раскладывать на неприводимые множители. После этого надо вынести общие знаменатели из всех множителей и получить разложение с целыми коэффициентами. Как формализовать это рассуждение?

Определение 5. Для рационального числа α и простого числа p определим $\mathrm{ord}_p(\alpha)$ — *порядок* p *в* α. А именно, это такое целое число r, что $\alpha = p^r c/d$, c и d не делятся на p. Для многочлена с рациональными коэффициентами $f(x) = a_0 + a_1 x + \dots + a_n x^n$ определим *порядок* p *в* f формулой $\mathrm{ord}_p(f) = \min_k \mathrm{ord}_p(a_k)$. Наконец, определим *содержание многочлена* f формулой $\mathrm{cont}(f) = \prod_p p^{\mathrm{ord}_p(f)}$.

Упражнение 4. $\frac{f(x)}{\operatorname{cont}(f)} = g(x)$, где $g(x)$ — многочлен с целыми коэффициентами, которые взаимно просты в совокупности.

Теорема 1. Для любых двух многочленов $f(x), g(x)$ с рациональными коэффициентами имеет место равенство $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$. (Многочлен fg есть произведение $\operatorname{cont}(fg)$ и многочлена со взаимно простыми коэффициентами. Если мы докажем, что произведение $\frac{f}{\operatorname{cont}(f)}\frac{g}{\operatorname{cont}(g)}$ имеет взаимно простые коэффициенты, то теорема будет доказана (почему?). Поэтому всё следует из *леммы Гаусса*: если у произведения двух многочленов с целыми коэффициентами наибольший общий делитель больше единицы, то это верно и для одного из сомножителей. Ясно, что эту лемму достаточно доказать в другой формулировке: если у произведения двух многочленов все коэффициенты делятся на простое число p, то и у одного из сомножителей это так. Научное доказательство этого утверждения таково: «приведём всё по модулю p», т. е. рассмотрим факторкольцо кольца многочленов с целыми коэффициентами по идеалу (p). Оно отождествляется с кольцом многочленов $(\mathbb{Z}/p\mathbb{Z})[x]$. Но кольцо $\mathbb{Z}/p\mathbb{Z}$ — поле, поскольку идеал (p) в $\mathbb{Z}$ максимален. Значит, кольцо многочленов с коэффициентами в $\mathbb{Z}/p\mathbb{Z}$ целостно. Однако наше условие означает, что произведение двух элементов этого кольца равно нулю. Поэтому один из них равен нулю, что и требовалось.)

Следствие. Многочлен положительной степени, неприводимый в $\mathbb{Z}[x]$, неприводим и в $\mathbb{Q}[x]$.

Теорема 2. Кольцо $\mathbb{Z}[x]$ факториально. Неприводимые элементы в нём суть неприводимые над $\mathbb{Q}$ многочлены с содержанием 1 и простые целые числа. (Действительно, чтобы получить такое разложение, разложим над рациональными числами и «вынесем» из каждого сомножителя его содержание. Произведение этих содержаний будет равно содержанию исходного многочлена, т. е. будет целым числом. Осталось разложить его на множители. Докажем единственность. По определению, кольцо факториально, если разложение единственно с точностью до перестановки сомножителей и умножения на обратимые элементы. Пусть есть два разложения над целыми числами. Рассмотрим их как разложения над рациональными числами и заметим, что если один многочлен с целыми взаимно простыми коэффициентами получается из другого с тем же свойством умножением на рациональное число, то это число равно ± 1, т. е. является обратимым элементом в $\mathbb{Z}$.)

Примеры. Многочлен $f(x) = 2$ неприводим в $\mathbb{Z}[x]$. Многочлен $f(x) = 6$ приводим. Кстати, критерий Эйзенштейна, который сформулирован в упражнениях, этим многочленом успешно опровергается. Чтобы он был верен, надо либо потребовать, чтобы наибольший общий делитель коэффициентов многочлена был равен единице, либо говорить о неприводимости в $\mathbb{Q}[x]$ (и тогда в доказательстве использовать, что из разложения над $\mathbb{Q}$ можно получить разложение над $\mathbb{Z}$).

Аналогично можно доказать более общее утверждение.

Упражнение 5. Если кольцо R факториально, то кольцо $R[x]$ также факториально. (Главное здесь — определить, что именно заменит поле рациональных чисел («поле частных кольца»).)