нуля, то оба элемента равны **с точностью до обратимого элемента**, *т.е. существует* $\varepsilon \in U(A)$, *такой, что* $a = \varepsilon b$.

(iii) Элемент p $\in$ *A называется* **неприводимым**, *если он не является ни нулевым, ни обратимым и если его единственными делителями являются 1 и p. Более точно: p неприводим тогда и только тогда, когда d | p* $\Rightarrow$ *d ~ 1 или d ~ p. Это свойство равносильно тому, что идеал Ap является максимальным в множестве* **однопорожденных** *(т.е главных) идеалов в A, отличных от A и {0}.*

(iv) Если кольцо A без делителей нуля, то p — неприводимый элемент тогда и только тогда, когда из p = de следует, что d или e — обратимый элемент в A.

1.2 Что такое факториальное кольцо?

Теперь можно дать точное определение структуры колец, обобщающей в какой-то мере структуру кольца $\mathbb{Z}$ целых чисел.

(4) Определение (факториальность).

Кольцо A называется факториальным, если оно не имеет делите лей нуля и если оно удовлетворяет основной теореме арифметики, что, формально, выражается следующим образом:

(i) Наличие разложения на неприводимые множители:

$$\forall a \in A^* \ U(A),\ \exists p_1, p_2, \ldots, p_n, \text{неприводимые и такие, что } a = p_1 p_2 \ldots p_n.$$

(ii) Единственность такого разложения:

$$p_1 p_2 \ldots p_n \sim_A q_1 q_2 \ldots q_m (p_i, q_j \text{неприводимые} \Rightarrow n = m \text{ и } \exists \sigma, \text{перестановка на } [1, n], \text{ такая, что } p_i \sim_A q_{q(i)} (1 \leqslant i \leqslant n).$$

В дальнейшем мы рассмотрим критерии, позволяющие распознать факториальность кольца. В настоящий момент читатель должен поверить, что это понятие не «бессодержательное», т.е. класс факториальных колец сравнительно широк. Прежде, чем продолжать дальнейшее изучение делимости, укажем одно арифметическое приложение факториальности.

1