**Баимбетова Рамина СИБ-22**

**Билет-16**

1. **Абелевы группы. Примеры**

Абелева группа есть группа, в которой групповая операция является коммутативной. Конечнопорождённые абелевы группы изоморфны произведениям циклических групп. Конечные абелевы группы изоморфны произведениям конечных циклических групп.

Примеры:

* Любое кольцо является коммутативной (абелевой) группой по своему сложению. В том числе и вещественные числа с операцией сложения.
* Обратимые элементы коммутативного кольца образуют абелеву группу по умножению. Например, вещественные числа, не равные нулю, с операцией умножения.
* Группа параллельных переносов в линейном пространстве.
* Любая циклическая группа *G* является коммутативной(абелевой), потому что для любых *x* и *y* из *G* верно, что *xy* = *aman* = *am*+*n* = *an*+*m* = *anam* = *yx*. В частности, целые числа **Z** образуют коммутативную группу по сложению, также как и вычеты по модулю **Z**/*n***Z**.

Основополагающая теорема о структуре конечной абелевой группы утверждает, что любая конечная абелева группа может быть разложена в прямое произведение своих циклических подгрупп порядков являющихся степенями простых чисел. Это следствие общей теоремы о структуре конечнопорождённых абелевых групп для случая, когда G не имеет элементов бесконечного порядка. Zmn изоморфно произведению Zm и Zn тогда и только тогда когда m и n взаимно просты. Следовательно, можно записать абелеву группу G в форме прямого произведения двумя различными способами:

Где числа k1,…,ku степени простых

Где k1 делит k2, который делит k3 и так далее до ku.

Например, Z/15Z = Z/15 может быть разложено в прямое произведение двух циклических подгрупп порядков 3 и 5: Z/15 = {0, 5, 10} ⊕ {0, 3, 6, 9, 12}. То же можно сказать про любую абелеву группу порядка пятнадцать, приходим к выводу, что все абелевы группы порядка 15 изоморфны.

**2. Основная теорема арифметики и ее приложения**

Основная теорема арифметики утверждает:

Любое целое число, большее единицы, может быть разделено на простые множители, причем это разложение будет единственным (изменение порядка следования множителей не в счет).

Докажем данную теорему. Возьмем целое число a, которое будет больше 1, и докажем, что его вообще можно разложить на множители. Возьмем наименьший положительный делитель данного числа, не равный единице, и обозначим его p1. Исходя из теоремы, доказательство которой мы приводили в статье о таблице простых чисел, данное число будет простым. Тогда, согласно определению делимости, должно существовать такое целое число, для которого a=p1⋅a1. Если a1 будет больше 1, то должно существовать число, являющееся его наименьшим простым делителем, значит, a1=p2⋅a2 и =p1⋅p2⋅a2.