Продолжение…

Теперь рассмотрим множество $Z_m^+ = Z_m \setminus \{0\}$ всех *ненулевых* элементов группы Z_m с заданной на нем операцией *умножения по модулю* m:

$$a \otimes b = ab \pmod{m}.$$

Для ее выполнения необходимо произвести обычное умножение целых чисел a и b, произведение разделить на m и в качестве результата операции взять остаток от деления. Эта операция ассоциативна в силу ассоциативности умножения целых чисел. Нейтральным элементам в ней является единица.

В качестве примера зададим такую операцию для $m = 7$ в форме таблицы Кэли:

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Здесь для каждого элемента можно найти обратный следующим образом: в строке, соответствующей интересующему нас элементу, отыскиваем нейтральный элемент (здесь, как следует из таблицы, это есть1); номер столбца и есть элемент, обратный данному. Поэтому получим

$$1^{-1} = 1,\ 2^{-1} = 4,\ 3^{-1} = 5,\ 4^{-1} = 2,\ 5^{-1} = 3,\ 6^{-1} = 6.$$

Возьмем теперь в качестве примера множество Z_6^+ и построим для него таблицу Кэли:

$\otimes$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

В этой таблице обнаруживаем две особенности.

Во-первых, появился элемент, не входящий в Z_6^+, а именно, нуль. Следовательно, здесь не выполняется условие замкнутости операции $\otimes$.

Во-вторых, не в каждой строк есть единица, а значит, не каждый элемент имеет обратный. Следовательно, система $\langle Z_6^+, \otimes \rangle$ не является даже полугруппой.

Можно показать, что Z_m^+ является группой относительно операции умножения по модулю m тогда и только тогда, когда m является *простым* числом.

Многие математические конструкции, которые естественно возникают в информатике, являются кольцами или включают в себя кольца как подструктуры.

Дадим определение кольца.

Кольцом называется некоторое множество R с *двумя* определенными на нем операциями: умножения $\otimes$ и сложения $\oplus$, такими что

а) $\otimes$ ассоциативна;

б) $\oplus$ ассоциативна;

в) $\oplus$ коммутативна;

г) $\oplus$ имеет нейтральный элемент, который называется *нулем* и обозначается 0:

$$0 \oplus a = a \oplus 0 = a; \tag{7.18}$$

д) существуют *противоположные* $(-a)$ элементы к элементам a относительно $\oplus$:

$$(-a) \oplus a = 0; \tag{7.19}$$

е) операция $\otimes$ *дистрибутивна* по отношению к операции $\oplus$, т.е.

$$\left.\begin{aligned} a \otimes (b \oplus c) &= (a \otimes b) \oplus (a \otimes c), \\ (a \oplus b) \otimes c &= (a \otimes c) \oplus (b \otimes c) \end{aligned}\right\} \tag{7.20}$$

для всех $a, b, c \in R$.

Очевидно, тип кольца $\langle R, \otimes, \oplus \rangle$ есть (2,2).

Таким образом, кольцо является *коммутативной группой* по *сложению*. По *умножению* оно в общем случае является *некоммутативной полугруппой*.

Если умножение $\otimes$ коммутативно, то кольцо называется *коммутативным*. В этом случае оно по умножению представляет собой *коммутативную полугруппу*.

Если существует единица 1 относительно умножения, то кольцо называется *кольцом с единицей*. Очевидно, в этом случае оно по умножению является *моноидом*.

Примеры колец:

1) $\langle \mathbb{Z}, \times, + \rangle$ - множество всех целых чисел $\mathbb{Z}$ с операциями обычного умножения и сложения.
2) Множество четных целых чисел относительно обычных умножения и сложения.
3) Множество квадратных матриц $M_n(\mathbb{R})$ порядка n с действительными элементами и матричными операциями сложения и умножения.

Полем $\langle F, \oplus, \otimes \rangle$ **называется множество** F **с двумя определенными на нем бинарными операциями – сложением** $\oplus$ **и умножением** $\otimes$**, которые удовлетворяют следующим свойствам:**

а) $\oplus$ **ассоциативна;**

б) $\oplus$ **коммутативна;**

в) $\oplus$ **имеет нейтральный элемент, который называется нуль 0:** $x \oplus 0 = x$ **для всех** $x \in F$;

г) **для каждого** $x \in F$ **существует противоположный элемент** $y = -x$ **такой, что** $x \oplus y = 0$;

д) $\otimes$ **ассоциативна;**

е) $\otimes$ **коммутативна;**

ж) $\otimes$ **имеет нейтральный элемент единица** $1 \neq 0$;

з) **для каждого** $x \in F \setminus \{0\}$ **существует обратный элемент** $y = x^{-1}$ **такой, что** $x \otimes y = 1$;

и) **операция** $\otimes$ **дистрибутивно по отношению к** $\oplus$**, т.е.**

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \qquad \text{для всех } x, y, z \in F.$$

- $\langle \mathbb{R}, \times, + \rangle$ - поле действительных чисел,
- $\langle \mathbb{C}, \times, + \rangle$ - поле комплексных чисел,
- $\langle \mathbb{Q}, \times, + \rangle$ - поле рациональных чисел.

Все перечисленные здесь поля имеют бесконечное количество элементов, Однако, могут существовать поля и с конечным количеством элементов.

Поле с q элементами называется *конечным полем* или *полем Галуа* и обозначается как $GF(q)$.

Естественно возникает вопрос: какое наименьшее количество элементов может содержать конечное поле? Иными словами, что представляет собой наименьшее поле?

Поле, по определению, обязательно должно содержать в своем составе *нулевой* элемент и *единичный* элемент. На самом деле этого уже достаточно для задания поля, если сложение и умножение определить таблицами Кэли:

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

Так определенные сложение и умножение являются *сложением по модулю* 2 и *умножением по модулю* 2 (конъюнкцией). Заметим, что из равенства $1 \oplus 1 = 0$ следует, что

$$-1 = 1,$$

т.е. противоположным к элементу 1 является тот же элемент 1.

Из равенства $1 \otimes 1 = 1$ следует, что

$$1^{-1} = 1,$$

т.е. обратным к элементу 1 также является элемент 1.

Используя эти свойства, легко проверить, что за исключением деления на нуль вычитание и деление всегда определены.

Итак, алфавит из двух символов 0 и 1 вместе со сложением по модулю 2 и умножением по модулю 2 (конъюнкцией) представляет собой поле Галуа $GF(2)$. Проверка показывает, что *не существует* другого поля с *двумя* элементами.

Эварист Галуа – краткая биография

Эварист Галуа родился в 1811 году в небольшом французском городке, мэром которого был его отец. С раннего детства стало понятно: в семье подрастает вундеркинд. Во время учебы в престижном колледже Луи-ле-Гран мальчик радовал своими успехами и преподавателей, и родных. На него возлагали большие надежды, ведь паренек делал сложнейшие переводы с греческого, за что получил немало наград. Однако со временем Эварист понял, что его предназначение - точные науки.

Эварист Галуа – краткая биография

- Его страстью стала математика и юноша решил поступить в Политехническую школу. Однако ни с первого, ни со второго раза ему так и не удалось поступить в ВУЗ. Он приводил в замешательство экзаменаторов, которые не могли понять его способ решения задач. Им они казались не последовательными и даже вызывали смех. Во второй раз гений не выдержал и кинул в одного из членов комиссии тряпку, после чего хлопнул дверью и ушел. Его невероятно разозлило, что его логические шаги в решении задач экзаменаторам никак не понять.
- Юный математик не опустил руки и принялся за самостоятельное обучение. Уже через пару лет, когда ему было всего лишь 18 лет, Эварист отправил свою научную работу в Парижскую академию для участия в конкурсе. Однако по непонятным причинам он был исключен из конкурса. Позже выяснилось, что его работа попросту была утеряна.

- Юный математик не опустил руки и принялся за самостоятельное обучение. Уже через пару лет, когда ему было всего лишь 18 лет, Эварист отправил свою научную работу в Парижскую академию для участия в конкурсе. Однако по непонятным причинам он был исключен из конкурса. Позже выяснилось, что его работа попросту была утеряна.
- Тогда гений под руководством своего учителя Ришара отправил еще 3 работы секретарю академии. Невероятно, но история вновь повторилась: секретарь скоропостижно скончался, а работы Галуа так и не были найдены.
- За 4 года он достиг отличных результатов и приступил к разгадке алгебраических уравнений в радикалах. На тот момент над решением этой задачи уже более 3 веков бились ученые со всего мира. И вот, парень, который изучал математику всего каких-то 4 года нашел решение невыполнимой задачи.
- Страсть к математике завладела им и вскоре он сделал величайшие открытия, которые сделали его основоположником современной высшей алгебры.

- **К**огда Галуа заканчивал работу над теорией групп, в его жизнь ворвались политические события. В июле 1830 года республиканцы — противники восстановленной монархии вышли на улицы; Карл X был вынужден эмигрировать. В то время как революционно настроенные студенты заперли внутри школы по приказу директора. Возмущённый Галуа пытался сбежать, но ему это не удалось В последовавшие за революцией месяцы Галуа посещал собрания республиканцев, встречался с их лидерами и, по-видимому, принимал участие в волнениях и демонстрациях, лихорадивших Париж. Он вступил в артиллерию Национальной гвардии — подразделение милиции, состоявшее почти исключительно из республиканцев. В декабре Галуа написал в одну из парижских газет письмо, в котором называл директора школы предателем, имея в виду его поведение во время июльской революции; неудивительно, что после этого Галуа исключили.
- В противоположность традиционной легенде, Галуа вовсе не производит впечатления жертвы обстоятельств. Напротив, он, похоже, был сорвиголовой и постоянно попадал в переделки. Из письма математика Софи Жермен следует, что Галуа регулярно присутствовал на заседаниях Академии наук и обычно всячески нападал на выступающих. Когда Галуа исключили из Школы, он переехал в парижский дом своей матери, но ей оказалось трудно с ним ужиться, и она уехала.
- Для Галуа кульминация бурной весны 1831 года наступила 9 мая во время банкета республиканцев, которые праздновали оправдание девятнадцати артиллерийских офицеров, обвинённых в заговоре против правительства. В своих мемуарах Александр Дюма-отец, который присутствовал на этом банкете, пишет, что Галуа встал и предложил тост за Луи-Филиппа, при этом одновременно с бокалом он поднял кинжал. На следующий день Галуа арестовали, и он провёл больше месяца в тюрьме св. Пелагеи.
- Самой большой неприятностью было то, что статьи, написанные Галуа в течение 1831 года, не напечатали. В исполненном горечи предисловии к тюремным запискам он утверждал: «Мне некого благодарить ни за совет, ни за поддержку. Благодарность была бы ложью».

- В ночь перед дуэлью Галуа лишь отредактировал две рукописи и изложил их содержание и содержание ещё одной статьи в длинном письме к Шевалье. Одна из рукописей была той самой статьёй, которую отклонил Пуассон, другая — отрывок статьи, ранее опубликованной в *Bulletin* Феруссака. Третью рукопись не нашли, и её содержание известно лишь из краткого изложения в письме; по-видимому, она касается интегралов от общих алгебраических функций.
- Сохранившиеся рукописи Галуа говорят о том, что, и попав в тюрьму, он продолжал вести математические изыскания и не оставлял их вплоть до самой смерти. То, что он мог продуктивно работать в таких условиях, свидетельствует о необыкновенной силе его воображения и интеллекта. Каковы бы ни были обстоятельства, в которых жил Галуа, нет сомнения, что ему принадлежит одна из самых оригинальных идей в математике.
- Теория групп является одной из самых плодотворных областей математики. Белл был прав, когда писал, что она на сотни лет дала математикам пищу для исследования она ныне даёт возможность проникнуть в сущность таких различных областей, как теория чисел, кристаллография, физика элементарных частиц и возможные позиции кубика Рубика.