MA-224 - WEEK 43
THE GROUP P_n AND LAGRANGE´S THEOREM

SVERRE LUNØE–NIELSEN

Contents

1. Introduction

We will discuss topics from [1, §16.3-4]. Last week we learned about basic concepts in group theory. In this week we will study a group of integers with group operation being modular multiplication modulo n, in addition to a fundamental theorem about the number of elements in a finite group.

2. Basic arithmetic

We collect some basic arithmetic facts to begin with. Much of this should be known from earlier.

2.1. **The euclidean algorithm.** Let x and n be any positive integers. An algorithm for findind the remainder of integer division x by n was written down by Euclid. Here it is, fashionably implemented in Python:

```
def remainder(x,n):
    r = x
    while r >= n:
        r -= n
    return r
```

In fact, if q is the number of iterations performed in the loop of the algorithm, you will find that

$$x = q \cdot n + r\,.$$

Date: October 26, 2022.

In fact, the numbers q and r are unique such that the above formula holds and $0 \leq r < n$.

Definition 2.1. *Let m and n be natural numbers. The **greatest common divisor** of m and n is the largest natural number which divides both m and n. We denote this number by* $\gcd(m, n)$*.*

The algorithm known as the *euclidean algorithm* computes greatest common divisors.

Let $m > n > 0$ be natural numbers. The greatest common divisor of m and n is equal to the greatest common division of $m-n$ and n, or in other words: $\gcd(m, n) = \gcd(m-n, n)$. Since $n > 0$, then $m-n < m$. If $m - n = n$, then $\gcd(m, n) = \gcd(m - n, n) = \gcd(n, n) = n$. On the other hand, if $m - n > n$, we may repeat the procedure using the pair $(m - n, n)$. The largest number in the pair will become strictly smaller for each iteration. Since we always take the difference between inequal numbers, we can assume that neither m nor n is 0. Therefore, the procedure must stop at some point where $m = n > 0$.

```
def euclidean_algorithm(m, n):
    while m != n:
        if m > n:
            m -= n
        else:
            n -= m
    return m
```

2.2. **Bézout's identity.** Let m, n be integers. Then Bézouts identity is the statement that there exists integers x og y such that

$$xm + yn = \gcd(m, n) \,.$$

This fact follows from the euclidean algorithm and can be proved by induction on the number of steps in the algorithm: Let m_k and n_k be the pair of integers at the kth step of Euclid's algorithm. If $k = 1$ is the index of the start of the process, then $m_1 = m$ and $n_1 = n$. Let $B(k)$ be the statement that $m_k = x_k m + y_k n$ and $n_k = z_k m + w_k n$ for some integers x_k, y_k, z_k, w_k. Then $B(1)$ is true with $x_1 = w_1 = 1$ and $y_1 = z_1 = 0$. For the induction step, assume that $B(k)$ is true for $k \geq 1$. If $m_k > n_k$, according to the euclidean algorithm, we then choose

$$\begin{aligned} m_{k+1} &= m_k - n_k = (x_k - z_k)m + (y_k - w_k)n \\ n_{k+1} &= n_k = z_k m + w_k n \end{aligned}$$

for the next step. Therefore $B(k + 1)$ is true if we choose

$$\begin{aligned} x_{k+1} &= x_k - z_k & \qquad z_{k+1} &= z_k \\ y_{k+1} &= y_k - w_k & \qquad w_{k+1} &= w_k \,. \end{aligned}$$

Similarly if $n_k > m_k$. If the algorithm terminates at $k = N$, we then have that $B(N)$ is true which means that $\gcd(m, n) = m_N = x_N m + y_N n$, which is Bézout's identity.

This procedure is called the *extended euclidean algorithm.*

```
def extended_euclidean_algorithm(m,n):
    x,y = (1,0)
    z,w = (0,1)
    while m != n:
        if m > n:
            m -= n
            x -= z
            y -= w
        else:
            n -= m
            z -= x
            w -= y

    # Return the gcd together with x, y
    # such that gcd(m,n) = xm + yn
    return (m,x,y)
```

Remark 2.2 Be aware that x and y in this formula are not unique.

2.3. **Modular exponentiation.** Let a, b and $n > 1$ be integers. By the division algorithm, we can write $a = un + r$ and $b = vn + s$ where $0 \leq u, v < n$. Then

$$ab = (un + r)(vn + s) = uvn^2 + (us + vr)n + rs \equiv rs \mod (n) .$$

In other words, if we want to compute the product $ab \mod (n)$, we can start by first reducing a and b modulo n, then multiply together the results.

This comes in handy when we are computing powers modulo n since we can always keep the numbers involved in our calculations less than n, as the next example shows.

Example 2.3 We wish to compute $37^3 \mod (13)$. By reducing modulo 13 whenever possible, our computation breaks into the following steps:

$$\begin{aligned} 37^3 = 37 \cdot 37 \cdot 37 &\equiv 11 \cdot 11 \cdot 11 \mod (13) \\ &= 121 \cdot 11 \\ &\equiv 4 \cdot 11 \mod (13) \\ &= 44 \\ &\equiv 5 \mod (13) . \end{aligned}$$

The rule is that whenever we see a number which is larger or equal to 13, we reduce it modulo 13 before we proceed with multiplication. This way, all of our numbers are kept at a managable size.

3. Multiplicative modular inverses

Let $m < n$ be integers such that $\gcd(m, n) = 1$. Bézout's identity says that there exists x, y such that $xm + yn = 1$, or equivalently, there exists an integer x such that $xm \equiv 1 \mod (n)$.

If x' is another integer such that $x'm \equiv 1 \mod (n)$, then by subtracting both sides we get $(x - x')m \equiv 0 \mod (n)$. Since $\gcd(m, n) = 1$, it follows that $x - x' \equiv 0 \mod (n)$. Therefore, multiplicative inverses to m are unique modulo n.

Not all integers $\mathrm{mod}(n)$ have multiplicative inverses, the easiest example is $m = 0$. Another non-trivial example is $m = 2$ and $n = 4$. However, if we restrict attention to those integers which is coprime to n, it turns out that we get a group.

Definition 3.1. *Let $n > 0$. Define*

$$P_n = \{k \in \mathbb{Z} \mid 1 \leq k < n, \ \gcd(k, n) = 1\}$$

to be the set consisting of all natural numbers which are coprime to and less than n.

Lemma 3.2. *The set P_n becomes a group under integer multiplication modulo n.*

Proof. If $x, y \in P_n$ then the product xy is also going to be coprime to n, i.e. $\gcd(xy, n) = 1$. If $k > n$ and $\gcd(k, n) = 1$ then also $\gcd(k-n, n) = 1$ like in Euclid's algorithm. Therefore P_n is closed under multiplication modulo n. Inverse elements exist because of Bézout's identity which says that there exists integers s and t such that $sk+tn = \gcd(k, n) = 1$, or equivalently: There exists an integer s such that $sk = 1 \mod (n)$. This integer belongs to the set P_n because $\gcd(s, n)$ is a divisor of $\gcd(sk, n) = 1$. $\square$

4. Cosets of groups and Lagrange's theorem

Definition 4.1. *Let $H \subset G$ be a subgroup of G, and let $g \in G$ be any element. The subset*

$$gH = \{g \cdot h \mid h \in H\} \subset G$$

is called the ***coset*** *of g and H in G.*

Lemma 4.2. *Let G be a group and $H \subset G$ a subgroup. Then any two cosets of $H \subset G$ are either equal or disjoint.*

If H is a subgroup of G, then all cosets of H have the same number of elements as the subgroup H. I.e. $|gH| = |H|$ for all subgroups $H \subset G$ and elements $g \in G$.

Proof. The property of belonging to the same coset defines a relation among elements of g which is obviously reflexive and symmetric. Let $g_1, g_2 \in G$ and assume that $x, y \in g_1H$ and $y, z \in g_2H$. This means that there exists elements $h_1, h_2, h_3, h_4 \in H$ such that

$$\begin{aligned} x &= g_1h_1, \text{ since } x \in g_1H \\ y &= g_1h_2, \text{ since } y \in g_1H \\ y &= g_2h_3, \text{ since } y \in g_2H \\ z &= g_2h_4, \text{ since } z \in g_2H \end{aligned}$$

Therefore $g_1h_2 = g_2h_3$ from which we get $g_2 = g_1h_2h_3^{-1}$. Using this, the last line from the list above says that $z = g_2h_4 = (g_1h_2h_3^{-1})h_4 = g_1(h_2h_3^{-1}h_4)$. Since the product in the last parenthesis is an element of H, we have shown that $z = g_1h$ so $z \in g_1H$ is in the same coset as x. Therefore, the relation is also associative. Therefore it is an equivalence relation with equivalence classes equal to the set of cosets of H. We know that equivalence classes are either equal or disjoint, so the same holds for cosets.

Let $g_1, g_2 \in G$ be any two elements. Define a function of sets

$$f : g_1H \to g_2H$$

by the formula $f(x) = g_2 \cdot g_1^{-1} \cdot x$. Then $f(x)$ belong to G, and since any $x \in g_1H$ can be written as $x = g_1 \cdot h$ for some $h \in H$, it follows that $f(x) = g_2 \cdot g_1^{-1} \cdot g_1 \cdot h = g_2 \cdot h$ is in the coset g_2H. The same construction produces a function in the opposite direction

$$g : g_2G \to g_1H\,,$$

which is obviously inverse to f. It follows that $|g_1H| = |g_2H|$. The coset eH of the neutral element is just the subgroup H, so for any $g \in G$ we get that $|H| = |gH|$. □

Note that the cosets is a partition of G into equally sized subsets of which only one of them, $eH = H$ is a subgroup. The others are disjoint from H, so they are not subgroups since they do not contain the neutral element $e \in H$.

Definition 4.3. *Let $H \subset G$ be a subgroup. The index of H in G is denoted by $[G : H]$, and is defined to be the number of different cosets gH in G:*

$$[G : H] = \big|\{gH \mid g \in G\}\big|$$

Example 4.4 Let $G = \mathbb{Z}/6 = \{0, 1, 2, 3, 4, 5\}$ be the cyclic group of order 6, and let $H = \{0, 2, 4\}$ be the subgroup generated by $2 \in \mathbb{Z}/6$

Here is an explicit list of all the cosets of H:

$$\begin{aligned}
0 + H &= \{0, 2, 4\} \\
1 + H &= \{1, 3, 5\} \\
2 + H &= \{2, 4, 0\} \\
3 + H &= \{3, 5, 1\} \\
4 + H &= \{4, 0, 2\} \\
5 + H &= \{5, 1, 3\}
\end{aligned}$$

We see from the list that there are only two different cosets: $0 + H$ and $1 + H$, so $[\mathbb{Z}/6 : \mathbb{Z}/3] = 2$. We see from this that the formula

$$|\mathbb{Z}/6| = |\mathbb{Z}/3| \cdot [\mathbb{Z}/6 : \mathbb{Z}/3]$$

holds in our case.

Theorem 4.5 (Lagrange's theorem)**.** *Let G be a finite group, and let $H \subset G$ be a subgroup. Then $|G| = |H| \cdot [G : H]$.*

Proof. We know from Lemma 4.2 that the cosets form a partition of G and that all cosets have the same number of elements. It follows that

$$|G| = \sum_{gH} |gH| = \sum_{gH} |H| = |H| \cdot (\sum_{gH} 1) = |H| \cdot [G : H].$$

□

References

[1] Ralph P. Grimaldi, *Discrete and combinatorial mathematics: an applied introduction.*, Pearson Education, 2013.

Email address: `sverre.lunoe-nielsen@uia.no`