Abstract Algebra, Class Notes

Eugen J. Ionaşcu

Contents

List of Figures

List of Tables

Preface

These notes are mostly intended to bring a personal take on some of the topics taught nowadys in the undergraduate abstract algebra (I and II) courses. We are following in footsteps of the classic textbook of [1].

Chapter 1

Concept of a group and examples

> Any new concept must be described as a special case of a more general concept: " a square is a quadrilateral (general concept) with four congruent sides and one right angle (special case)". Aristotle (Criterion of hierarchy)

1.1 Definition and motivation

In mathematics, we like to develop important deductions from a given set of assumptions. These arguments are usually called *theorems*. Sometimes the set of assumptions are essentially the same but the settings may appear to be different.

Example 1. For instance, let us look into the set of functions $S_1 := \{f^{(n)}\}_{n\in\mathbb{N}}$, where $f : \mathbb{R} \setminus \{-3/5\} \to \mathbb{R} \setminus \{-3/5\}$, defined by $f(x) = -\frac{3x+2}{5x+3}$ for every $x \in \mathbb{R} \setminus \{-3/5\}$. Can we be more specific about the set S_1? Well, let's calculate $f \circ f$. We observe that

$$(f \circ f)(x) = -\frac{-3\frac{3x+2}{5x+3} + 2}{-5\frac{3x+2}{5x+3} + 3} = -\frac{x}{-1} = x \Rightarrow f \circ f = id.$$

So, the set $S_1 = \{id, f\}$. A function like this is called an *involution* (it is its own inverse).

Example 2. Let us consider the matrix $A = \begin{bmatrix} 3 & 2 \\ -5 & -3 \end{bmatrix}$ and let us find $S_2 = \{A^n\}_{n\in\mathbb{N}}$. Can we be more specific about the set S_2? If we calculate A^2 we obtain $-I$, where as usual $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Then, the set $S_2 = \{I, A, -A, -I\}$.

Example 3. We let $T_1 = \{1, -1\}$ and $T_2 = \{1, i, -i, -1\}$ (subsets of complex numbers). What will make the two sets T_1 and T_2 similar to the sets S_1 and S_2? The answer to this question involves a more precise definition of the word "similar". The key word here is *operation*, like addition, multiplication, division, etc. The operation on S_1 is the composition of functions, i.e., $\circ$, and the operation on S_2 is the usual multiplication of matrices. The table for each of these operations is included below:

$\circ$	id	f
id	id	f
f	f	id

$\cdot$	I	A	-I	-A
I	I	A	-I	-A
A	A	-I	-A	I
-I	-I	-A	I	A
-A	-A	I	A	-I

These tables are called *Cayley tables*. Now we can be more precise about our question and ask, "What natural operation can we consider on the sets T_1 and T_2 that will make them like S_1 and S_2 respectively?" What common properties can we find in these two essentially different examples?

Example 4. Consider $g : \mathbb{R} \setminus \{1, 2\} \to \mathbb{R} \setminus \{1, 2\}$, defined by $f(x) = \frac{x-3}{x-2}$ for every $x \in \mathbb{R} \setminus \{1, 2\}$. Show that g is one-to-one and onto and the operation of composition on the set $\{id, g, g^2\}$ has the following table:

$\circ$	id	g	g^2
id	id	g	g^2
g	g	g^2	id
g^2	g^2	id	g

. If we take $\omega = \frac{-1+\sqrt{3}i}{2}$, check that a similar table can be obtained if we take the usual multiplication of complex numbers on the set $\{1, \omega, \omega^2\}$.

Example 5. Let us use the classical notation $\mathbb{Z}_5$ for the set of classes $\hat{i}$ of integers that give remainders i when divided by 5: $\mathbb{Z}_5 := \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$. It is natural to define the operation $\hat{i} + \hat{j} = \widehat{(i + j)}$. What is the table of this operation on $\mathbb{Z}_5$, and are there any similarities in properties with the ones we have seen before? Is it possible to generalize this to $\mathbb{Z}_n$?

Example 6. For $n \in \mathbb{N}$, the set $\{1, 2, 3, ..., n\}$ is denoted by $[n]$. We will denote by $\mathcal{S}_n$ the set of all permutations of $[n]$, in other words, all 1-1 maps from $[n]$ into $[n]$ (automatically these are also onto, so $\mathcal{S}_n$ is the set of all bijections on $[n]$). We will write a permutation $\pi : [n] \to [n]$ by simply listing the ordered n-tuple $[\pi(1), \pi(2), ..., \pi(n)]$. For $n = 3$, we have

$$\mathcal{S}_3 = \{[1, 2, 3], [2, 1, 3], [1, 3, 2], [2, 3, 1], [3, 1, 2], [3, 2, 1]\}.$$

Since permutations are functions, we can use the operation on $\mathcal{S}_n$ of composition of functions, since the composition of two 1-1 functions is also 1-1 (please check). What is the Cayley table that we obtain with this operation on $\mathcal{S}_3$? If we introduce

the notations, $id = [1,2,3]$, $\tau = [2,1,3]$ and $\sigma = [3,1,2]$, can the table be written just in terms of these three permutations? For this purpose let us observe that $\tau^2 = [2,1,3] \circ [2,1,3] = [1,2,3] = id$, $\sigma^3 = [3,1,2] \circ [3,1,2] \circ [3,1,2] = [1,2,3] = id$, $\tau\sigma = [2,1,3] \circ [3,1,2] = [3,2,1]$ and so $(\tau\sigma)^2 = 1$. We observe that $\sigma\tau = [3,1,2] \circ [2,1,3] = [1,3,2]$ which shows that $\tau\sigma \neq \sigma\tau$. We also have $(\sigma\tau)^2 = id$ which implies $\sigma\tau = \tau\sigma^2$. Hence, the Cayley table can be determined from these relations

$$\tau^2 = id,\ \sigma^3 = id, \quad \text{and} \quad \sigma\tau = \tau\sigma^2$$

$\circ$	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
id	id	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	id	$\tau\sigma^2$	τ	$\tau\sigma$
σ^2	σ^2	id	σ	$\tau\sigma$	$\tau\sigma^2$	τ
τ	τ	$\tau\sigma$	$\tau\sigma^2$	id	σ	σ^2
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	τ	σ^2	id	σ
$\tau\sigma^2$	$\tau\sigma^2$	τ	$\tau\sigma$	σ	σ^2	id

We notice here that the order of the composition is important. We say that the operation is not *commutative*.

Example 7. We consider all matrices 2×2 with determinant non-zero and entries from $\mathbb{Z}_2$ (multiplication on $\mathbb{Z}_n$ is as before: $\hat{i}\hat{j} = \widehat{(ij)}$, $i, j = 0, 1, ..., n-1$). Check that with the multiplication of matrices we obtain a similar structure as in Example 6.

Example 8. Let us denote the set $\mathbb{R} \setminus \{0, 1\}$ by A, define the functions on A with values on A: $f_1(x) = \frac{1}{x}$, $f_2(x) = 1 - x$, $f_3(x) = \frac{1}{1-x}$, $f_4(x) = \frac{x-1}{x}$ and $f_5(x) = \frac{x}{x-1}$. Check that with the composition of functions we obtain a similar structure as in Example 6.

Taking into account all these examples, the following concepts are arising as important.

Definition 1.1.1. *We say an* **operation** $*$ *is defined on a set A if we are given a function $f : A \times A \to A$ such that $a * b = f(a, b)$ for every a and b in A.*

Definition 1.1.2. *We say that $(G, *)$ is a* **group** *(or G has an algebraic structure of group with the operation $*$) if $*$ is an operation on G with the following properties:*

(i) there exists an element e of G, called **identity element**, *such that for all $g \in G$, we have $e * g = g * e = g$*

(ii) the operation $*$ is associative, i.e., for all a, b and c in G we have $a*(b*c) = (a * b) * c$

(iii) for every element of G, say g, there exists an element commonly denoted g^{-1} (called the inverse of g) such that $g * g^{-1} = g^{-1} * g = e$.

If in addition, we have $a * b = b * a$ for all a and b, the group is call **commutative** *or* **abelian**.

If the group $(G, *)$ has finitely many elements we say $(G, *)$ is a *finite group*. We usually simplify the notation $(G, *)$ to G when the operation is understood. All the examples we have seen so far are instances of finite groups. If G is finite, the cardinality of the set G is called the **order** of the group G. Hence, we have seen examples of finite groups of orders between 2 and 6. Except the group in Examples 6 and 7, all of the other groups are abelian.

Definition 1.1.3. *We say that two groups $(G_1, *)$ and $(G_2, \circ)$ are* **isomorphic** *if there exists a map $h : G_1 \to G_2$ which a bijection and such for every a and b in G_1, we have $h(a * b) = h(a) \circ h(b)$.*

So basically, when we used the word "similar" we meant isomorphic groups. The associative property is not easy to check and most of the time it is inherited from the associativity of the usual addition of real numbers (which we will assume is true) or the associativity of the multiplication of real numbers.

The proof of associativity property for the composition of functions reduces to two lines: for all x we have

$$[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = [f \circ (g \circ h)](x) \Rightarrow$$
$$(f \circ g) \circ h = f \circ (g \circ h).$$

Problem 1.1.4. *Show that an involution $f : A \to A$, with A a finite set with an odd number of elements, has a fixed point (i.e. there exists an element in A, say x, such that $f(x) = x$).*

Problem 1.1.5. *Consider the set of ordered pairs $K := \{(0,0), (0,1), (1,0), (1,1)\}$ with the operation of addition on components modulo 2. Construct the Cayley table for this operation on S and prove we have a group of order 4 which is not isomorphic with the ones in Examples 2 and 3. (This group goes by the name of Klein's group or $\mathbb{Z}_2 \times \mathbb{Z}_2$)*

Problem 1.1.6. *Let us define on $A := \mathbb{C}\backslash\{0, 1\}$ (the set of complex numbers except 0 and 1) the following six functions id, $f_1(z) = 1 - z$, $f_2 = \frac{1}{z}$, $f_3(z) = \frac{z}{z-1}$, $f_4(z) = \frac{z-1}{z}$ and $f_5(z) = \frac{1}{1-z}$, for all $z \in A$. Show that the set $G := \{id, f_1, f_2, f_3, f_4, f_5\}$ together with the operation of composition of functions forms a group isomorphic to the one in Examples 6 and 7.*

Problem 1.1.7. *If we take $G = (0, \infty)$ and define the operation $a \star b = a^b$, show that $(G, \star)$ is not a group.*

Problem 1.1.8. *If we take $G = (0, \infty)$ and define the operation $a \star b = ab$ (usual multiplication of positive numbers), show that $(G, \star)$ is an abelian infinite group.*

Problem 1.1.9. *Consider $\mathbb{R}$ with usual operation of addition. Show that $(\mathbb{R}, +)$ is an infinite abelian group isomorphic to the one in Problem 1.1.8.*

Definition 1.1.10. *We say that a group $(G, *)$ is* **cyclic** *if there exists an element x (called a* **generator***) such that every element in the group, say y, can be written as x^m for some $m \in \mathbb{Z}$, i.e., $y = x^m$ (by convention $x^0 = e$, e is the identity element, and $x^{-n} = (x^{-1})^n$ for all $n \in \mathbb{N}$).*

Problem 1.1.11. *Prove that $\mathbb{Z}_n$ with the usual operation of addition modulo n is an abelian finite group of order n which is also cyclic.*

Problem 1.1.12. *Prove that $(\mathbb{R}, +)$ is not cyclic but $(\mathbb{Z}, +)$ is.*

Definition 1.1.13. *Suppose a group $(G, *)$ has identity element e. For an element $x \in G$, if there exists $n \in \mathbb{N}$ such that $x^n = e$ then the smallest n with this property is called* **the order** *of the element x.*

For instance, in the symmetric group $\mathcal{S}_3$, τ has order 2 and σ has order 3.

1.2 Properties of groups and isomorphisms

Most of the time if the operation of the group $(G, \star)$ is understood we usually drop the symbol $\star$ and simply use multiplicative notation: $a \star b$ will be simply written as ab.

It turns out that the identity element in a group is unique and an element cannot have two different inverses. Let's record and prove this next.

Proposition 1.2.1. *Given a group G with identity element e then:*

(i) e is unique, i.e., if e' is an element such that $e'x = xe' = x$ for every $x \in G$, then $e' = e$;

(ii) if $x \in G$, then x^{-1} is unique, i.e., if $y \in G$ has the property that $yx = xy = e$ then $y = x^{-1}$.

Proof (i) Since e satisfies $xe = ex = x$ for every $x \in G$, in particular $e'e = ee' = e'$. Similarly, since $e'x = xe' = x$ for every $x \in G$, in particular $e'e = ee' = e$. Therefore, $e' = e'e = e$.

(ii) Because $xy = yx = e$ then if we multiply by x^{-1} on the left we get $x^{-1}(xy) = x^{-1}e = x^{-1}$. The operation is associative and so $x^{-1} = x^{-1}(xy) = (x^{-1}x)y = ey = y$ which is exactly what we needed to show. □

Proposition 1.2.2. *The concepts of identity element, inverse of an element, order of an element, order of the group, cyclic, abelian, and finite/infinite, are all invariant under isomorphisms. In other words, for example, the identity element is mapped into the identity element by an isomorphism of groups or a cyclic group is mapped into a cyclic group by an isomorphism of groups, etc.*

The proof of this theorem is left as an exercise.

Problem 1.2.3. *Show that a group G of order n is cyclic if and only if it contains an element of order n.*

Problem 1.2.4. *Every cyclic group is commutative.*

Problem 1.2.5. *All cyclic groups of order n are isomorphic to $\mathbb{Z}_n$ (we say, there is essentially -up to isomorphism-only one cyclic group of order n).*

Proposition 1.2.6. *Given arbitrary elements a, b and c in a group G,*

(i) $(ab)^{-1} = b^{-1}a^{-1}$

(ii) $ab = ac$ implies $b = c$ (left simplification/cancelation)

(iii) $f : G \to G$, defined by $f(x) = x^{-1}$ for all x is a bijection (inversion), and it is an isomorphism iff G is commutative.

Proof

Problem 1.2.7. *A group is commutative iff for all a, b in the group $(ab)^2 = a^2b^2$.*

Problem 1.2.8. *A group is abelian iff for all a, b, c, d and x in the group, the following implication is true*

$$axb = cxd \Rightarrow ab = cd.$$

$$abab = abab \implies bab = abb \implies ba = ab$$

Problem 1.2.9. *A group is commutative iff for all a, b in the group $(ab)^{-1} = a^{-1}b^{-1}$.*

Definition 1.2.10. *Suppose S is a non-empty subset of a group $(G, *)$ ($S \subset G$) and $\star$ is an operation on S also. If $(S, \star)$ is a group, we say in this case that S is a* **subgroup** *of G. We usually write $S \preceq G$ if S is a subgroup of G. S is called* **proper** *subgroup if $S \leq G$ but $S \neq G$. S is called non-trivial if $|S| > 1$ (cardinality is more than one).*

Problem 1.2.11. *If S is a subgroup of G, then the identity element of S is the identity element of G and the inverse of $s \in S$ in S is the same as the inverse of s in G.*

Problem 1.2.12. *List all the subgroups of the groups of $\mathbb{Z}_{12}$.*

Proposition 1.2.13. *(i) A non-empty subset S of a group G is a subgroup if and only if S is closed under the operation in G and taking inverses (for all a and b in S we have $ab \in S$ and $a^{-1} \in S$).*

(ii) A non-empty subset S of a group G is a subgroup if and only if for all a and b in S we have $ab^{-1} \in S$.

(iii) If G is finite, then $S \neq \emptyset$ is a subgroup of G iff it closed under under the operation in G .

The proof of this theorem is left as an exercise.

Definition 1.2.14. *Given a group $(G, *)$ and $x \in G$. We denote by $\langle x \rangle$ the set $\{x^k |\ k \in \mathbb{Z}\}$ (using multiplicative notation, as defined in (1.1.10)). This is called the* subgroup generated *by x.*

Theorem 1.2.15. *Show that if $n \in \mathbb{N}$ we have:*

(i) for $S \preceq \mathbb{Z}_n$, nontrivial, then $S = \langle d' \rangle$ where d' is the smallest non-zero element of S and d' divides n;

(ii) if $S = \langle d \rangle = \langle d' \rangle$ in $\mathbb{Z}_n$ and d is a divisors of n, then d is equal to d', where d' is the smallest non-zero element in S;

(iii) if $S = \langle d \rangle$ then $\gcd(d, n) = d'$, where d' is the smallest non-zero element in S;

(iv) the set of subgroups of $\mathbb{Z}_n$ is in one-to-one correspondence to the set of divisors of n.

Proof of (ii) in Theorem 1.2.15. Clearly since d' is the smallest non-zero element of S and d cannot be zero, $d \geq d'$. By the Division Algorithm, we must have $d = d'q + r$, with $0 \leq r < d'$ and q a positive integer. If $r > 0$, this implies $r \in S$, which is smaller than d', a contradiction. Hence $r = 0$ and thus $d = d'q$.

On the other hand, d divides n which means $n = dt = d'qt$ for some integer t. Because d' is in $S =< d >$ we can write $d' = kd + nl$ for some integers k and l. Substituting we have $d' = kqd' + lqtd'$ and if we divide by d', we obtain $1 = (k + lt)q$. This shows that q divides 1 and so $q = 1$. Therefore, we have $d = d'$. □

Proof of (iii) in Theorem 1.2.15. As in the previous proof, we can similarly conclude that $d = d'q$. From (i), d' divides n and so $n = d't$ for some integer t.

Since d' is in S, we can write $d' = du + nv$ for integers u and v. Substituting we get $d' = d'qu + d'tv$ which implies $1 = qu + tv$. Hence, we have $\gcd(q,t) = 1$ and then

$$\gcd(n,d) = \gcd(d't, d'q) = d' \gcd(t,q) = d'. \blacksquare$$

Problem 1.2.16. *Find all the generators of* $\mathbb{Z}_n$. *(***Hint:** *Show that this set consists of all* $k \in \{1, 2, ..., n-1\}$ *such that* $\gcd(k,n) = 1$, *i.e., the greatest common divisor of* k *and* n *is* 1. *)*

Problem 1.2.17. *The set of all generators of* $\mathbb{Z}_n$ *is denoted by* $U(\mathbb{Z}_n)$ *and if equipped with the operation of multiplication modulo* n *we obtain a group.*

Problem 1.2.18. *If* $n = 12$ *show that* $U(\mathbb{Z}_{12})$ *is isomorphic to the group in Problem 1.1.5.*

If a natural number n is written in its prime factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \tag{1.1}$$

where p_i are distinct primes and $\alpha_i \in \mathbb{Z}$ $(i = 1, 2..., s)$, then the number of divisors of n is given by the function τ, $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1)$. For example, $\tau(100) = \tau(2^2(5^2)) = 3(3) = 9$. We have then 9 subgroups of $\mathbb{Z}_{100}$:

$$\{0\}, \langle 1\rangle = \mathbb{Z}_{100}, \langle 2\rangle, \langle 4\rangle, \langle 5\rangle, \langle 10\rangle, \langle 20\rangle, \langle 25\rangle, \text{ and } \langle 50\rangle.$$

Problem 1.2.19. *Find how many subgroups we have in* Z_{2016} *and how many have order* 63.

Problem 1.2.20. *List all the subgroups of* $\mathcal{S}_3$ *(the group of permutations of* 3 *objects).*

Definition 1.2.21. *Given a group* $(G, *)$ *an element* $x \in G$ *and* $H \preceq G$, *we define* xH *to be the set* $\{xh | h \in H\}$ *called the* ***left coset*** *of* H *in* G *with respect to* x. *Similarly, we define* Hx *to be the set* $\{hx | h \in H\}$ *called the* ***right coset*** *of* H *in* G *with respect to* x.

Example: If the group is $\mathcal{S}_3 = \{id, \tau, \sigma, \tau\sigma, \sigma\tau, \sigma^2\}$ and $H = \{id, \tau\}$ we have $\sigma H = \{\sigma, \sigma\tau\}$ and $H\sigma = \{\sigma, \tau\sigma\}$. Also, if we do $\sigma^2 H = \{\sigma^2, \sigma^2\tau\}$. Because $\sigma^2\tau = \tau\sigma$, we notice that H, σH and $\sigma^2 H$ are all disjoint sets and their union is $\mathcal{S}_3$.

Definition 1.2.22. *Given a set* A *and a family of subsets* $\{X_j\}_j$ *of* A, *we say that this family is a* ***partition*** *of* A *if*

(a) $X_j \cap X_k = \emptyset$ *for all two distinct indices* j *and* k, *and*

(b) $A = \bigcup_j X_j$.

We observe that in the previous example, the family $\{H, \sigma H, \sigma^2 H\}$ is a partition of $\mathcal{S}_3$. If we take $S = \langle \sigma \rangle$ the subgroup of $\mathcal{S}_3$ generated by σ, then

$$\tau S = \{\tau, \tau\sigma, \tau\sigma^2\} = \{\tau, \tau\sigma, \sigma\tau\}.$$

Hence, the family $\{S, \tau S\}$ forms a partition of $\mathcal{S}_3$ also. This property is happening in general.

We remind the reader that if A and B are two finite sets then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

In particular if A and B are disjoint, then $|A \cup B| = |A| + |B|$. By induction, if we have a finite set A and a partition of A say, $\{X_j\}_{j=1...m}$ of A, then

$$|A| = |X_1| + |X_2| + ... + |X_m|.$$

Proposition 1.2.23. *Given a subgroup H of a group G then*

(i) for every x and y in G, then either $xH = yH$ or if $xH \neq yH$ then $xH \cap yH = \emptyset$;

(ii) for every x and y in G, then there exists a bijection between xH and yH;

(iii) and $G = \bigcup_{x \in G} xH$.

(iv) If G is finite, the order of H divides the order of G (Lagrange's Theorem).

Proof of (i) Proposition 1.2.23. We need to show that if $xH \cap yH \neq \emptyset$, then $xH = yH$. So, suppose $xh_1 = yh_2$ for some h_1 and h_2 in H. Then, $y = xh_1h_2^{-1}$ and since H is a subgroup $h_1h_2^{-1} \in H$. Let's denote $h_1h_2^{-1}$ by t. Then, to show that $yH \subset xH$, we take and arbitrary h and calculate $yh = (xt)h = x(th)$. Because $th \in H$, we see that $yx \in xH$. Similarly, we prove that $xH \subset yH$. □

Proof of (ii) Proposition 1.2.23. Let us define $f : xH \to yH$, by $f(xh) = yh$ for all $h \in H$. We need to make sure this is well-defined: $xh_1 = xh_2$ implies $yh_1 = yh_2$. If $xh_1 = xh_2$ we can simplify x and obtain $h_1 = h_2$ and this implies $yh_1 = yh_2$. The map f is one-to-one since $yh_1 = yh_2$ implies $h_1 = h_2$ which shows that $xh_1 = xh_2$. The function f is onto since for every yh we can define xh and have $f(xh) = yh$. □

Proof of (iii) Proposition 1.2.23. This is done by double inclusion. The inclusion $\supseteq$ is clear. The inclusion $\subseteq$ is also true since every x is in xH because $e \in H$. □

Proof of (iv) Proposition 1.2.23. If G is finite, then H is finite. Let us denote the cardinality of G by n. By (ii), each two left cosets xH and yH have the same number of elements, say k ($k \geq 1$ since H is not empty). By (iii), the set $G \setminus H$ is either empty or not. If it is empty then $G = H$ and so $n = k$; the conclusion of

the statement in (iv) follows. If not, we can choose an element from $G \setminus H$, say x_1. Then H and x_1H are not equal because $x_1 \in x_1H$ and $x_1 \notin H$. By (i), we must have $H \cap x_1H = \emptyset$. We can then proceed as before and look into the set $G \setminus (H \cup x_1H)$. If this set is empty, then

$$G = H \cup x_1H \Rightarrow |G| = n = |H| + |x_1H| - |H \cap x_1H| = k + k - 0,$$

or $n = 2k$ and the conclusion in (iv) follows. If not, we proceed as before by choosing an element $x_2 \in G \setminus (H \cup x_1H)$. Then x_2H is different of H and x_1H and so by (i), x_2H is disjoint of these two sets. We look at the set $G \setminus (H \cup x_1H \cup x_2H)$. If this set is empty, then

$$G = H \cup x_1H \cup x_2H \Rightarrow |G| = n = |H| + |x_1H| + |x_2H| = k + k + k,$$

or $n = 3k$ and the conclusion in (iv) follows. If the set is not empty, we continue this process until the sets H, x_1H, x_2H,..., x_sH form a partition G. We know that this process is going to continue since the cardinality of the sets x_iH is not zero. Hence $(s+1)k = n$, which proves (iv). □

Corollary 1.2.24. *Given a finite group G of order n and $x \in G$, then*

(i) the order of x divides the order of G: $|\langle x \rangle|$ divides n;

(ii) $x^n = e$, e the identity element of G.

Problem 1.2.25. *If G is a finite group and $x \in G$, then $|\langle x \rangle|$ is the order of x.*

Definition 1.2.26. *Given a natural number n, we denote by $\varphi(n)$ the cardinality of the group $U(\mathbb{Z}_n)$.*

By Problem 23, we have

$$\varphi(n) = |\{k | k \in \{1, 2, ..., n-1\} \text{ such that } \gcd(k, n) = 1\}|. \tag{1.2}$$

Clearly, if n is a prime then $\varphi(n) = n - 1$. There is a formula for this function in terms of the prime factorization of n given in (1.1):

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_2^{\alpha_s} - p_s^{\alpha_s - 1}) \tag{1.3}$$

Theorem 1.2.27. *(***Euler***) If a and n are natural numbers such that $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1$ (mod n).*

Corollary 1.2.28. *(***Fermat's Little Theorem***) If a and p are natural numbers such that p does not divide a, then $a^{p-1} \equiv 1$ (mod p).*

Let us look at an example to see how do we apply Theorem 1.2.27. If $n = 2016$ then $\varphi(2016) = \varphi(2^5(3^2)(7)) = (2^5 - 2^4)(3^2 - 3)(6) = 2^6(3^2) = 576$. So, any number relatively prime with 2016, in particular any prime different of 2, 3 and 7, say p, satisfies $p^{576} \equiv 1 \pmod{2016}$. Hence $2017^{576} \equiv 1 \pmod{2016}$. An application of Corollary 1.2.28 can be that $576^{2016} \equiv 1 \pmod{2017}$.

Bibliography

[1] Joseph A. Gallian, *Contemporary abstract algebra*, Second Edition, D.C. Heat and Company

[2] Kiran Kedlaya, Bjorn Poonem, and Ravi Vakil, *The William Lowel Putnam mathematical competition 1985-2000*, MAA Problem Books, The Mathematical Association of America 2002