Lecture 4: Abstract algebra: Groups, Rings and Finite Fields.

1. Binary operations.

A binary operation "*" on a set $S$ associates to each pair $(a, b) \in S \times S$ an element $a \ast b \in S$. The operation is called associative if $a \ast (b \ast c) = (a \ast b) \ast c$, for all $a, b, c \in S$, and commutative if $a \ast b = b \ast a$, for all $a, b \in S$. If there exist an element $e$ such that $a \ast e = e \ast a = a$ for all $a \in S$, then $e$ is called an identity element. If the identity exists, then it is unique. In this case, if for an element $a \in S$ there exists $b \in S$ such that $a \ast b = b \ast a = e$, then $b$ is called the inverse of $a$ and it is denoted by $a^{-1}$. If an element has an inverse, then the inverse is unique.

As a warmup, let us start with the following simple example.

Problem 1. (Putnam A1, 2001)

Consider a set $X$ and a binary operation $\ast$ on $X$. Assume that $(a \ast b) \ast a = b$, for all $a, b \in X$. Show that $a \ast (b \ast a) = b$, for all $a, b \in X$. 

-1-
Solution.
Substituting \( b \ast a \) for \( a \), we have

\[
((b \ast a) \ast b) \ast (b \ast a) = b, \quad \text{and thus } a \ast (b \ast a) = b,
\]

for all \( a, b \in X \). \( \Box \)

**Problem 2.**

On a set \( N \) an operation \( \ast \) is given satisfying the properties

(i) there exists an element \( e \in N \) such that \( x \ast e = x \), for all \( x \in N \);

(ii) \( (x \ast y) \ast z = (z \ast x) \ast y \), for all \( x, y, z \in N \).

Prove that the operation is both associative and commutative.

**Solution.**

Substituting \( y = e \) in the second equality (ii), we get

\[
(x \ast e) \ast z = (z \ast x) \ast e \quad \text{or} \quad x \ast z = z \ast x,
\]

which proves that \( \ast \) is commutative. We shall use it to prove associativity. Indeed, we have:

\[
(x \ast y) \ast z = (z \ast x) \ast y = (y \ast z) \ast x = x \ast (y \ast z), \quad \forall x, y, z \in N.
\]

\( \Box \)
Problem 3. (Putnam 1972)

Let $S$ be a set and $*$ a binary operation on $S$ satisfying the laws:

(i) $x \ast (x \ast y) = y$, for all $x, y \in S$.
(ii) $(y \ast x) \ast x = y$, for all $x, y \in S$.

Show that $*$ is commutative but not necessarily associative.

Solution. Using the first law, we can write:

$$y \ast (x \ast y) = (x \ast (x \ast y)) \ast (x \ast y).$$

Now, using the second law, we get:

$$(x \ast (x \ast y)) \ast (x \ast y) = x,$$

so $y \ast (x \ast y) = x$. Now, we have

$$y \ast x = y \ast (x \ast y) = x \ast y,$$

which proves the commutativity.

For the second part, let $S$ be the set of all integers, $\mathbb{Z}$, endowed with the law $x \ast y = -x - y$. We have

$$x \ast (x \ast y) = -x \ast (x \ast y) = -x - (-x - y) = y,$$

and

$$(y \ast x) \ast x = -(y \ast x) - x = -(-y - x) - x = y.$$

Also, $(1 \ast 2) \ast 3 = 0$ and $1 \ast (2 \ast 3) = 4$, and we are done. $\square$
2. Groups.

Definition.

A group is a set of transformations of some space that contains the identity transformation and is closed under composition and under the operation of taking the inverse.

A more abstract definition of a group is as follows. A set $G$ endowed with a binary operation $\cdot$ is called a group if it satisfies:

1. **Associativity:** $x(yz) = (xy)z$, $\forall x, y, z \in G$.

2. **Identity element:** $e \in G$ such that for any $x \in G$,
   \[xe = ex = x.\]

3. **Existence of inverse:** for every $x \in G$ there is $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = e$.

- A group is called **abelian** if $xy = yx$, $\forall x, y \in G$.
- A group is called **cyclic** if it is generated by a single element, that is, if it consists of the identity element and powers of some element.
- The order of an element $g$ in a group $G$, denoted by $\text{o}(g)$, is the least positive integer $n$ such that $g^n = e$. If $G$ is a finite group, then $\text{o}(g) \mid |G|$. 

**Definition.**
Let $G$ be a group and $H \leq G$, $H \neq \emptyset$. We say that $H$ is a **subgroup** of $G$ if for all $x, y \in G$, we have $xy^{-1} \in H$. We write $H$ is a subgroup of $G$ as $H \leq G$. Also, $H$ is called a **proper subgroup** of $G$ if $H \neq G$.

**Theorem. (Lagrange)**
Let $(G, \cdot)$ be a finite group and $H$ is a subgroup of $G$. Then $|H|$ divides $|G|$ (i.e., $\text{ord}(H)$ divides $\text{ord}(G)$).

**Theorem. (Cauchy)**
Let $(G, \cdot)$ be a finite group and $p$ is a prime number such that $p \mid |G|$ (i.e., $p$ divides $\text{ord}(G)$). Then the number of solutions of the equation $x^p = e$ is a multiple of $p$.

**Consequence 1.**
If $(G, \cdot)$ is a finite group and $p$ is a prime such that $p \mid |G|$ (i.e., $p$ divides $\text{ord}(G)$), then there exists $x \in G$ such that $\text{ord}(x) = p$.

**Consequence 2.**
If $(G, \cdot)$ is a finite group and $p$ is a prime such that $p \mid |G|$, then the number of subgroups of order $p$ is congruent with 1 modulo $p$. 
Problem 4
Let \((G, \cdot)\) be a group such that \((xy)^2 = x^2y^2\), for all \(x, y \in G\). Show that \(G\) is abelian.

Solution.
We have \((xy)^2 = xyxy = x^2y^2\). If we multiply by \(x^{-1}\) on the left, we have \(x^{-1}xyxy = x^{-1}x^2y^2\) or equivalently, \(yxy = xy^2\) or \(yxy = yx^2\). Now, multiplying with \(y^{-1}\) to the right, we have \(yxyy^{-1} = xy^2y^{-1}\) or equivalently, \(yx = xy\) and we are done. \(\square\)

Problem 5
Let \((G, \cdot)\) be a group such that \(x^2 = e\), for all \(x \in G\). Show that \(G\) is abelian. Here \(e\) is the identity element in \(G\). Moreover if \(G\) is finite, then there exists \(k \in \mathbb{N}\) such that \(\text{ord}(G) = 2^k\).

Solution.
Clearly from \(x^2 = e\), it follows that \(x = x^{-1}\), for all \(x \in G\). This can be rewritten as \(xyxy = e\). Multiplying by \(x^{-1}\) to the left, we have \(x^{-1}xyxy = x^{-1}x^2y\) or \(yxy = x^{-1}\). Now, multiplying with \(y^{-1}\) to the right, we have \(yxyy^{-1} = x^{-1}y^{-1}\) or \(yx = x^{-1}y^{-1} = xy\), which is exactly what we wanted to prove. The second part is a bit tricky! We shall
use Cauchy's theorem. Indeed, let us assume by contradiction that \( \text{ord}(g) \) is not a power of 2. Then, there exists \( p \in \mathbb{N}, p \) prime, \( p \geq 3 \) such that \( p \mid \text{ord}(g) \). Using Consequence 1 of Cauchy's theorem, we obtain the existence of an element \( a \in G \), with \( \text{ord}(a) = p \). Then \( a^p = e \), and since \( a^2 = e \), we have \( a^{(p+1)} = e \), or \( a^{p-2} = e \), false! Thus, \( \exists n \in \mathbb{N} \) such that \( \text{ord}(g) = 2^n \). \( \square \)

**Problem 6.** (Putnam B3, 1972)

A group has elements \( g, h \) satisfying:

\[
ghg = h^2g \quad \Rightarrow \quad g^3 = 1 \quad (1 \text{ is the identity in the group}) \quad h^n = 1, \text{ for some odd } n.
\]

Prove that \( h = 1 \).

**Solution.**

Firstly, we show that \( gh^2 = h^2g \). Indeed, we have

\[
gh^2 = (ghg)g^2h = (h,g^2h)g^2h = (h,g^2)(h^2g^2) = h^2g. \text{ From here, it follows that } ghg^2 = h^2g^3 = h^2.
\]

Hence \( gh^{2n} = h^{2n} \). Now, we choose \( n \) such that \( h^{2n} = h \).

Then \( ghg^2 = h \), or \( gh = hg \). This implies that \( h = h^2 \)

and thus \( h = 1 \). \( \square \)
Problem 7

Let $G$ be a group with the following properties:

(i) $G$ has no element of order 2;
(ii) $(xy)^2 = (yx)^2$, for all $x, y \in G$.

Show that $G$ is abelian.

Solution.
The idea is to apply (ii) for the elements $x$ and $yx^{-1}$. Indeed, we have

$$xyx^{-1} \cdot yx^{-1} = yx^{-1} \cdot yx^{-1} x$$

which is equivalent with $xy^2 x^{-1} = y^2$. This implies that $xy^2 = y^2 x$. Using this fact, we rewrite the identity from the statement as

$$xyx^{-1} y^{-1} x^{-1} y^{-1} = e.$$

We have

$$e = xyxyx^{-1} y^{-1} x^{-1} y^{-1} = xyxyx^{-2} yx^{-2} yx^{-2} yx^{-2} y^{-2} y$$

$$= xyxyy^{-2} x^{-2} yxxy y^{-2} x^{-2} = (xyxy y^{-2} x^{-2})^2.$$

Since there are no elements of order 2, we get $xyxy y^{-2} x^{-2} = e$ and hence $xyxy = x^2 y^2$ and by canceling with $x$ and $y$, we get $xy = yx$. □
Problem 8. (Vojtech Jarník International Contest, 2005)
Let $G$ be a finite group of order $n$. Show that every element of $G$ is a perfect square if and only if $n$ is odd.

Solution.

$\Rightarrow$ If any element in $G$ is a perfect square, then the function $f: G \to G$ defined by $f(a) = a^2$ is surjective and therefore $f$ is also injective. In particular, if $a^2 = e$, then $a = e$. This shows that $G$ cannot have elements of order 2.

$\Leftarrow$ If $n$ is odd, then $n = 2k - 1$. Consider an element $x \in G$. Then $x^n = e$ and thus $(x^k)^2 = x$, so $x$ is a perfect square.

Problem 9. (Romanian Olympiad, 2002)
Show that the groups $(\mathbb{R}^*, \cdot)$ and $(\mathbb{R}^* \times \mathbb{R}^*, \cdot)$ are not isomorphic, where $\mathbb{R}^* \times \mathbb{R}^*$ is the direct product endowed with the law $(x, y) \cdot (x', y') = (xx', yy')$, for all $x, y, x', y' \in \mathbb{R}$.

Solution. Assume by contradiction that there exists an isomorphism $f: (\mathbb{R}^* \times \mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$. Clearly $f(1, 1) = 1$.

Let us consider the following points:
$x_1 = (1,1), x_2 = (-1,-1), x_3 = (1,-1)$ and $x_4 = (-1,1)$.

Clearly, they are distinct two by two, and thus $f(x_k)$ are distinct two by two.

On the other hand, since $x_k^2 = (1,1)$, $k=1,2,3,4$ and $f$ is a homomorphism (group), we have

$$f(x_k^2) = f^2(x_k) = 1, \quad k=1,2,3,4.$$ 

This implies that the equation $x^2 = 1$ has for distinct solutions in $\mathbb{R}$ which is false. $\Box$

Thus, $(\mathbb{R}^* \times \mathbb{R}^*, \cdot) \not\cong (\mathbb{R}^*, \cdot)$

Problem 10.

Let $G$ be a group which commutative with 2002 elements and $e$ is the identity element in the group. Prove that there exists $x \in G \setminus \{e\}$ such that $x^2 = e$. Is $x$ unique?

Solution.

We know that $x^2 = e$ iff $x = x^{-1}$. The set $G \setminus \{e\}$ has an odd number of elements. Assume by contradiction that $x \neq x^{-1}$ for $x \in G \setminus \{e\}$. This means that one can group in pairs the elements $(x, x^{-1})$ in $G \setminus \{e\}$, and this implies that $G$ has an even number of elements which is absurd. For the uniqueness, let us assume by contradiction that there exists an element $y \neq x$ such that $y^2 = x^2 = e$. This is equivalent with $(xy)^2 = e$, and thus $H = \{e, x, y, xy\}$ is a subgroup of $G$. By
Lagrange's theorem, \( \text{ord}(H) \) divides \( \text{ord}(G) \) on 4/2002, false! Therefore, the element \( x \in G \cdot \text{f.e.f} \) exists such that \( x^2 = e \) and moreover it is unique. \( \square \)

**Problem 11.**

Let \( (G, \cdot) \) be a finite group. If \( m \) and \( n \) are divisors of the group order, then the equations \( x^m = e \) and \( x^n = e \) have one common solution if and only if \( (m, n) = 1 \).

**Solution.**

Let us observe that \( x = e \) is the common solution of the equations given in the problem.

\[ \Rightarrow \] Assume \( (m, n) = 1 \). This implies that \( \exists k, l \in \mathbb{Z} \) such that \( km + ln = 1 \). Let \( a \) be a common solution of the two equations. Then, we have \( a^m = a^n = e \) and thus \( a = a^{-1} a^m a^{-n} = e \).

\[ \Leftarrow \] Let \( (m, n) = d \). If \( d \geq 2 \), then there exists a prime number \( p \) such that \( p \) divides \( d \). By Consequence 1 of Cauchy's theorem, there exists \( b \in G \cdot \text{f.e.f} \) such that \( \text{ord}(b) = p \). This implies \( b^d = e \) and since \( b^d = e \), it follows that the equation \( x^d = e \) does not have an unique solution, false! Therefore \( d = 1 \) and we are done. \( \square \)
Problem 12.
Let \((G, \cdot)\) be a group with 10 elements in which there exists elements \(a, b \in G\) distinct such that \(a^2 = b^2 = e\). Show that \(G\) is not an abelian group.

Solution.
Assume by contradiction that \(G\) is abelian. This implies that \(ab \in \{e, a, b, ab\}\), and thus \(H = \{e, a, b, ab\}\) is a subgroup of \(G\). By Lagrange's theorem, \(\text{ord}(H) / \text{ord}(G)\), or equivalently \(4/10\), false! \(\square\)

Problem 13. (Romanian Olympiad, 2006)
Let \(G = \{A \in M_2(\mathbb{R}) \mid \det(A) = \pm 1\}\) and \(H = \{A \in M_2(\mathbb{R}) \mid \det(A) = 1\}\).
Show that \(G\) and \(H\) endowed with matrix multiplication cannot be isomorphic as groups.

Solution.
Firstly, it is easy to check that \(G\) and \(H\) are groups. Assume by contradiction that \(G\) and \(H\) are isomorphic. Let us look at the equation \(X^2 = I_2\). In \(H\), by the Cayley-Hamilton equality, we have only two solutions \(X = \pm I_2\). On the other hand, if we look in \(G - H\), any matrix of the form
\[
X = \begin{pmatrix}
0 & a \\
1 & 0
\end{pmatrix}, \quad a \in \mathbb{C}^*
\]
is a solution to \(X^2 = I_2\). Therefore \(G \ncong H\). \(\square\)
3. Rings.

Rings mimic in the abstract setting the properties of the sets of integers, polynomials, or matrices.

**Definition.** A ring $R$ is a set endowed with two operations “+” (addition) and “·” (multiplication) such that $(R,+)$ is an Abelian group with identity element 0 and the multiplication satisfies:

1. **Associativity:** $x(yz) = (xy)z$, for all $x, y, z \in R$.
2. **Distributivity:**
   - $x(y+z) = xy + xz$ and
   - $(x+y)z = xz + yz$, for all $x, y, z \in R$.

A ring is called commutative if the multiplication is commutative. It is said to have an identity if there exists $1 \in R$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$. An element $x \in R$ is called invertible if there exists $x^{-1} \in R$ such that $xx^{-1} = x^{-1}x = 1$.

**Problem 14.**

Let $x$ and $y$ be elements in a ring with identity. Prove that if $1-xy$ is invertible, then $1-yx$ is also invertible.

**Solution.**

Let $v$ be the inverse of $1-xy$. Then, we have $v(1-xy) = (1-xy)v = 1$, and this implies $vxy = xyv = 0 = 1$. 

-13-
Now, we compute
\[(1 + yo) (1 - yx) = 1 - yx + yo - yox xyx = 1 - yx + yo - y(x+1)x = 1.\] A similar computation shows that
\[(1 - yx) (1 + yo) = 1.\]
It follows that 1 - yx is invertible and its inverse is 1 + yo.

\[\square\]

**Problem 15.**

Let \( R \) be a ring with identity with the property that 
\[(xy)^2 = x^2y^2 \] for all \( x, y \in R \). Show that \( R \) is commutative.

**Solution.**

We substitute \( x \) by \( x+1 \) in the equality given in our statement, and we have:
\[0 = (x+1)y = (x+1)^2 y^2 = (xy)^2 + xy^2 + yxy + y^2 - x^2y^2 - 2xy^2 - y^2 = yxy - xy^2.\]

Hence, \( xy^2 = yxy \), for all \( x, y \in R \). Now, we substitute in this relation \( y \) by \( y+1 \), and we get
\[x(y+1)^2 = (y+1)x(y+1)\] which is equivalent with
\[xy^2 + 2xy + x = yxy + xy + xy + x.\]
Using the equality \( xy^2 = yxy \), we obtain \( xy = yx \), as desired. \( \square \)
Problem 16.
Let \( R \) be a ring with identity such that \( x^6 = x \) for all \( x \in R \). Prove that \( x^2 = x \) for all \( x \in R \). Prove that such a ring is commutative.

Solution.
We have that \( x^6 = (-x)^6 = -x \), and thus \( 2x = 0 \), for any \( x \in R \). Now, let's consider the element \( x+1 \). Applying the condition from the hypothesis for \( x+1 \), we have

\[
(x+1)^6 = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x^4 + x^2 + x + 1.
\]

Hence, \( x^4 + x^2 = 0 \), or \( x^4 = -x^2 = x^2 \). Then, we have

\[
x^6 = x^2 x^4 = x^2 x^2 = x^4 = x^2,
\]
and thus \( x^2 = x \). Now, from the equality \( (x+y)^2 = x+y \) we deduce \( xy + yx = 0 \), so \( xy = -yx = yx \), for any \( x, y \in R \) and we are done. \( \square \)

Problem 17. (Iran Competition for Students, 1988)
Let \( R \) be a ring with unit, \( \text{char}(R) = 2 \), such that for any \( x \neq 1 \) and \( y \neq 1 \), we have \( xy = xy^2 \). Show that the ring \( R \) is commutative.
Solution.

We will show that any element \( y \in R \) satisfies \( y = y^2 \), \( \forall y \in R \) and based on problem 16, it will follow that \( R \) is commutative.

Indeed, let \( x \in R, x \neq 0, x \neq 1 \). Since \( \text{char}(R) = 2 \), there exists an element \( x_1 \in R, x_1 \neq 0, x_1 \neq 1 \) such that \( x = 1 + x_1 \). From the hypothesis, we know that \( (1+x_1)y = (1+x_1)y^2 \), for all \( y \in R \). But, \( x_1 y = x_1 y^2 \), and thus \( y = y^2 \), for all \( y \in R \), and therefore \( R \) is commutative. ◻

Problem 18. (International Mathematics Competition, 2000)

Let \( (A, +, \cdot) \) be a ring of characteristic 0, and consider elements \( x, y, z \in A \) which are idempotents such that \( x + y + z = 0 \). Show that \( x = y = z = 0 \).

Solution.

We have \( x + y = -z \) which implies that \( (x + y)^2 = -z^2 = z = -x - y \). This implies that \( x^2 + xy + yx + y^2 = -x - y \) and since \( x^2 = x \) and \( y^2 = y \), we have \( 2x + 2y + xy + yx = 0 \) (*)

This implies that \( 2x^2 + 2xy + x^2 + yx = 0 \) and using again the fact that \( x^2 = x \), we get \( 2x + 2xy + xy + yx = 0 \) or \( 2x + 3xy + xy = 0 \). Now, multiplying by \( x \) to the right, we have \( 2x^2 + 3xy + xy = 0 \) or \( 2x^2 + 4xy = 0 \).
Now, from $2x + 3xy + yx = 0 = 2x + 4xy$, we have $x + 2xy = 0$ (we used the fact that char $(A) = 0$). Going even further, we have $2xy = -x$ or equivalently $(2xy)(2xy) = x^2 = x$ or $4xyxy = x^2 = x$. But, $4xyxy = 4xyy = 4xy = -2x$, and thus $x = -2x$, or $3x = 0$ and therefore $x = 0$. Similarly, one can show that $y = 2 = 0$. □

Problem 19. (International Mathematics Competition, 1993)

Let $(A, +, \cdot)$ be a ring such that $x^2 = 0$, for all $x \in A$. Show that for all $x, y, z \in A$, we have $xyz + xyz = 0$.

Solution.

From $(x + y)^2 = x^2 + y^2 + xy + yx = 0$, we have $xy = -yx$, for arbitrary $x, y, z$. This implies that

$$xyz = x(yz) = -((yz))x = -(y(2x)) = (2x)y = 2(xy)$$

$$= -((xy)z) = -xyz,$$

and we are done. □

Problem 20.

Let $R$ be a nontrivial ring with identity, and let $M = \{x \in R / x^2 = x\}$ the set of its idempotents. Prove that if $M$ is finite, then it has an even number of elements.
Solution.

First, we show that if \( x \) is idempotent, then \( 1-x \) is an idempotent as well. Indeed,

\[
(1-x)^2 = 1 - 2x + x^2 = 1 - 2x + x = 1 - x.
\]

Thus, there is an involution on \( M \), \( x \mapsto 1-x \). This involution has no fixed points, because if it has, then \( x = 1-x \) implies \( x^2 = x - x^2 \) or \( x = x - x = 0 \), which implies 0 = 1, false! This means that this involution pairs the elements of \( M \), and thus the cardinality of \( M \) is even. \( \square \)