MATH 415
Modern Algebra I

Lecture 14: Follow-up on Exam 1. Advanced algebraic structures.

Follow-up on Exam 1

Problem 1a. Consider a binary operation $*$ on $\mathbb{R}$ given by $x * y = \sqrt[3]{x^3 + y^3}$ for any $x, y \in \mathbb{R}$. Is $(\mathbb{R}, *)$ a semigroup? Is it a group?

First we check that the operation $*$ is well defined: $x, y \in \mathbb{R} \implies x * y \in \mathbb{R}$.

Then we observe that $(x * y)^3 = x^3 + y^3$ for all $x, y \in \mathbb{R}$. Consider a function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$. We obtain that $f(x * y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$. This means that f is a homomorphism of the binary structure $(\mathbb{R}, *)$ to the binary structure $(\mathbb{R}, +)$. It is easy to see that f is bijective. It follows that $(\mathbb{R}, *)$ is a group and that it is isomorphic to the group $(\mathbb{R}, +)$.

Problem 1b. Consider a binary operation $*$ on $\mathbb{R}$ given by $x * y = y$ for all $x, y \in \mathbb{R}$. Is $(\mathbb{R}, *)$ a semigroup? Is it a group?

Clearly, $x * y \in \mathbb{R}$ for all $x, y \in \mathbb{R}$ so that the operation is well defined. Further, for any $x, y, z \in \mathbb{R}$ we have $(x * y) * z = y * z = z$ and $x * (y * z) = x * z = z$. Hence $(x * y) * z = x * (y * z)$, the operation is associative.

By definition of the operation, every element is a left identity. It follows that there is no right identity (and hence this is not a group). Indeed, if e_ℓ is any left identity and e_r is any right identity, then $e_r = e_\ell * e_r = e_\ell$.

Problem 3b. We have the following information on a group G and its subgroups H_1 and H_2:

- the order of G is either 15 or 20 or 25,
- H_1 and H_2 are proper subgroups of different orders and neither of them contains the other,
- the intersection $H_1 \cap H_2$ is a nontrivial subgroup of G.

Find the order of $H_1 \cap H_2$.

Let n denote the order of the group G, let m_1 and m_2 denote orders of the subgroups H_1 and H_2, and let k denote the order of the intersection $H_1 \cap H_2$. We are given that $n = 15$ or 20 or 25, that $m_1 < n$ and $m_2 < n$, that $m_1 \neq m_2$, and that $k > 1$.

By Lagrange's Theorem, the order of a subgroup divides the order of the group. In particular, m_1 and m_2 are proper divisors of n. Since neither of the subgroups H_1 and H_2 contains the other, their intersection $H_1 \cap H_2$ is a proper subgroup of H_1 and of H_2. By Lagrange's Theorem, k is a proper divisor of m_1 and of m_2. Since $k > 1$, it follows that neither m_1 nor m_2 is a prime number or 1.

Now we obtain that n cannot be 15 or 25 as any proper divisor of these numbers is either prime or 1. Therefore $n = 20$. The number 20 has only two proper divisors which are composite numbers: 4 and 10. Hence one of them is m_1 and the other is m_2. Finally, k is a common divisor of 4 and 10. Since $k > 1$, we obtain that $k = 2$.

Remark. The group G in this problem can be, for example, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$. Then $H_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \{0\}$, $H_2 = \{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_5$ and $H_1 \cap H_2 = \{0\} \times \mathbb{Z}_2 \times \{0\}$.

Problem. Find two non-abelian groups of order 24 that are not isomorphic to each other.

It is known that groups of order 24 form 15 isomorphism classes. Three of them are abelian groups, represented by $\mathbb{Z}_3 \times \mathbb{Z}_8$, $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

The other 12 classes are non-abelian groups. Representatives for some of them are: S_4, $A_4 \times \mathbb{Z}_2$, $S_3 \times \mathbb{Z}_4$, $S_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_{12}, $D_4 \times \mathbb{Z}_3$, and $SL(2, \mathbb{Z}_3)$.

Rings

Definition. A **ring** is a set R, together with two binary operations usually called **addition** and **multiplication** and denoted accordingly, such that

- R is an abelian group under addition,
- R is a semigroup under multiplication,
- multiplication distributes over addition.

The complete list of axioms is as follows:

(A0) for all $x, y \in R$, $x + y$ is an element of R;

(A1) $(x + y) + z = x + (y + z)$ for all $x, y, z \in R$;

(A2) there exists an element, denoted 0, in R such that $x + 0 = 0 + x = x$ for all $x \in R$;

(A3) for every $x \in R$ there exists an element, denoted $-x$, in R such that $x + (-x) = (-x) + x = 0$;

(A4) $x + y = y + x$ for all $x, y \in R$;

(M0) for all $x, y \in R$, xy is an element of R;

(M1) $(xy)z = x(yz)$ for all $x, y, z \in R$;

(D) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for all $x, y, z \in R$.

Fields

Definition. A **field** is a set F, together with two binary operations called **addition** and **multiplication** and denoted accordingly, such that

- F is an abelian group under addition,
- $F \setminus \{0\}$ is an abelian group under multiplication,
- multiplication distributes over addition.

In other words, the field is a commutative ring with unity ($1 \neq 0$) such that any nonzero element has a multiplicative inverse.

Examples. • Real numbers $\mathbb{R}$.

- Rational numbers $\mathbb{Q}$.
- Complex numbers $\mathbb{C}$.
- $\mathbb{Z}_p$: congruence classes modulo p, where p is prime.
- $\mathbb{R}(X)$: rational functions in variable X with real coefficients.

Vector spaces over a field

Definition. Given a field F, a **vector space** V over F is an additive abelian group endowed with a mixed operation $\phi : F \times V \to V$ called **scalar multiplication** or **scaling**.

Elements of V and F are referred to respectively as **vectors** and **scalars**. The scalar multiple $\phi(\lambda, v)$ is denoted λv.

The scalar multiplication is to satisfy the following axioms:

(V0) for all $v \in V$ and $\lambda \in F$, λv is an element of V;
(V1) $\lambda(v + w) = \lambda v + \lambda w$ for all $v, w \in V$ and $\lambda \in F$;
(V2) $(\lambda + \mu)v = \lambda v + \mu v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V3) $\lambda(\mu v) = (\lambda\mu)v$ for all $v \in V$ and $\lambda, \mu \in F$;
(V4) $1v = v$ for all $v \in V$.

(Almost) all linear algebra developed for vector spaces over $\mathbb{R}$ can be generalized to vector spaces over an arbitrary field F. This includes: linear independence, span, basis, dimension, determinants, matrices, eigenvalues and eigenvectors.

Examples of vector spaces over a field F:

- The space F^n of n-dimensional coordinate vectors $(x_1, x_2, \dots, x_n)$ with coordinates in F.
- The space $\mathcal{M}_{n,m}(F)$ of $n \times m$ matrices with entries in F.
- The space $F[X]$ of polynomials $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in F.
- Any field F' that is an extension of F (i.e., $F \subset F'$ and the operations on F are restrictions of the corresponding operations on F'). In particular, $\mathbb{C}$ is a vector space over $\mathbb{R}$ and over $\mathbb{Q}$, $\mathbb{R}$ is a vector space over $\mathbb{Q}$.

Linear independence over $\mathbb{Q}$

Since the set $\mathbb{R}$ of real numbers and the set $\mathbb{Q}$ of rational numbers are fields, we can regard $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Real numbers $r_1, r_2, \dots, r_n$ are said to be **linearly independent over** $\mathbb{Q}$ if they are linearly independent as vectors in that vector space.

Example. 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$.

Assume $a \cdot 1 + b\sqrt{2} = 0$ for some $a, b \in \mathbb{Q}$. We have to show that $a = b = 0$.

Indeed, $b = 0$ as otherwise $\sqrt{2} = -a/b$, a rational number. Then $a = 0$ as well.

In general, two nonzero real numbers r_1 and r_2 are linearly independent over $\mathbb{Q}$ if r_1/r_2 is irrational.

Linear independence over $\mathbb{Q}$

Example. 1, $\sqrt{2}$, and $\sqrt{3}$ are linearly independent over $\mathbb{Q}$.

Assume $a + b\sqrt{2} + c\sqrt{3} = 0$ for some $a, b, c \in \mathbb{Q}$.
We have to show that $a = b = c = 0$.

$$\begin{gathered} a + b\sqrt{2} + c\sqrt{3} = 0 \implies a + b\sqrt{2} = -c\sqrt{3} \\ \implies (a + b\sqrt{2})^2 = (-c\sqrt{3})^2 \\ \implies (a^2 + 2b^2 - 3c^2) + 2ab\sqrt{2} = 0. \end{gathered}$$

Since 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$, we obtain $a^2 + 2b^2 - 3c^2 = 2ab = 0$. In particular, $a = 0$ or $b = 0$.

Then $a + c\sqrt{3} = 0$ or $b\sqrt{2} + c\sqrt{3} = 0$. However 1 and $\sqrt{3}$ are linearly independent over $\mathbb{Q}$ as well as $\sqrt{2}$ and $\sqrt{3}$. Thus $a = b = c = 0$.

Finite fields

Theorem 1 Any finite field F has nonzero characteristic.

Proof: Consider a sequence $1, 1+1, 1+1+1, \dots$ Since F is finite, there are repetitions in this sequence. Clearly, the difference of any two elements is another element of the sequence. Hence the sequence contains 0 so that the characteristic of F is nonzero.

Theorem 2 The number of elements in a finite field F is p^k, where p is a prime number.

Proof: Let p be the characteristic of F. By the above, $p > 0$. As we know from the previous lecture, p is prime. Let F' be the set of all elements $1, 1+1, 1+1+1, \dots$ Clearly, F' consists of p elements. One can show that F' is a subfield (canonically identified with $\mathbb{Z}_p$). It follows that F has p^k elements, where $k = \dim F$ as a vector space over F'.

Algebra over a field

Definition. An **algebra** A over a field F (or F-**algebra**) is a vector space over F with a multiplication which is a bilinear operation on A. That is, the product xy is both a linear function of x and a linear function of y.

To be precise, the following axioms are to be satisfied:

(A0) for all $x, y \in A$, the product xy is an element of A;
(A1) $x(y+z) = xy+xz$ and $(y+z)x = yx+zx$ for $x, y, z \in A$;
(A2) $(\lambda x)y = \lambda(xy) = x(\lambda y)$ for all $x, y \in A$ and $\lambda \in F$.

An F-algebra is **associative** if the multiplication is associative. An associative algebra is both a vector space and a ring.

An F-algebra A is a **Lie algebra** if the multiplication (usually denoted $[x, y]$ and called **Lie bracket** in this case) satisfies:

(Antisymmetry): $[x, y] = -[y, x]$ for all $x, y \in A$;
(Jacobi's identity): $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in A$.

Examples of associative algebras:

- The space $\mathcal{M}_n(F)$ of $n \times n$ matrices with entries in F.
- The space $F[X]$ of polynomials $p(x) = a_0 + a_1 X + \cdots + a_n X^n$ with coefficients in F.
- The space of all functions $f : S \to F$ on a set S taking values in a field F.
- Any field F' that is an extension of a field F is an associative algebra over F.

Examples of Lie algebras:

- $\mathbb{R}^3$ with the cross product is a Lie algebra over $\mathbb{R}$.
- Any associative algebra A with a Lie bracket (called the **commutator**) defined by $[x, y] = xy - yx$.