Glimpse of abstract algebra with a view toward mathematical competitions

Donghui Kim

Monday, February 19, 2018

1 Foundations

On a set X and for a non-negative integer n, the n-ary operation on X is a function $X^n \longrightarrow X$. Note that zero-ary operation exists only for those non-empty X. 2-ary operation is also called a **binary** operation. A non-empty set with operations are called an **algebraic structure**. Consider a binary operation $\circ$. $\circ(a, b)$ is usually written as $a \circ b$ or even simply ab for brevity. Binary operation $\cdot$ on X is said to be **associative** if $(a \circ b) \circ c = a \circ (b \circ c)$ for every $a, b, c \in X$. An algebraic structure with an associative binary operation is called a **semigroup**.

For a binary operation $\cdot$ on X, an element $e \in X$ such that $\forall x \in X(e \cdot x = x \cdot e = x)$ is called the **identity** of $\cdot$.

Theorem 1. *If there is an identity of an operation on a set, then the identity is unique.*

Proof. Let e and f be identities. Then

$$e = ef = f$$

□

A semigroup is called a **monoid** if there is an identity. A **group** is a monoid in which every elements are invertible. If the operation is commutative, the group is said to be **abelian** or **additive**.

Example 1.1. The followings are some algebraic structures.

(1) $(\mathbb{N}, +)$ is a semigroup but not monoid. However, the structure can be extended to a group.

(2) $(\mathbb{N}, \times)$ is a monoid but not a group Moreover, it cannot be extended to a group.

(3) $(\mathbb{N}_0, \times)$ is a monoid but not a group

(4) For any set, the set of all functions from X to X forms a monoid.

(5) For any set, the set of all bijections from X to X forms a group.

(6) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are additive groups with addition.

(7) For any set S and a group G, the set of all functions $S \longrightarrow G$ form a group with pointwise operation; $f : S \longrightarrow G$ and $g : S \longrightarrow G$ then $(f \cdot g) : x \mapsto f(x) \cdot g(x)$.

(8) $M_n(\mathbb{R})$ is the set of $n \times n$ array of real numbers. The elements in $M_n(\mathbb{R})$ are called the $n \times n$ square real matrices. For $M \in M_n(\mathbb{R})$ and $1 \leq i, j \leq n$, M_{ij} denotes the i row, j^{th} column entry of M. Therefore, matrices can be viewed as a real valued function on $\{1, 2, \ldots, n\}^2$. Hence $M_n(\mathbb{R})$ forms a group.

(9) $\mathbb{R}[x]$, the set of all polynomial with real coefficients is an additive group with addition. However, it is just a monoid but not a group with multiplication.

1. Let G be a group and g, $h \in G$. Prove the followings.

(1) $g^{-1^{-1}} = g$.
(2) $(gh)^{-1} = h^{-1}g^{-1}$.
(3) $gh = h \implies g = e$ and $gh = g \implies h = e$ where e is the identity.

A function between groups which commutes with the operation is called a (group) homomorphism.

Precisely, let $(G, \cdot)$ and $(H, *)$ be groups. A function $f : G \longrightarrow H$ is a group homomorphism is the following diagram commutes.

$$\begin{array}{ccc} G \times G & \xrightarrow{\;\cdot\;} & G \\ \big\downarrow{\scriptstyle f \times f} & & \big\downarrow{\scriptstyle f} \\ H \times H & \xrightarrow{\;*\;} & H \end{array}$$

which means $f \circ \cdot = * \circ (f \times f)$ where $f \times f : G \times G \longrightarrow H \times H$, $(a, b) \mapsto (f(a), f(b))$.

2. Prove that group homomorphisms preserves identities and inverses. That is, for any group homomorphism $f : G \longrightarrow H$, where G and H are groups with identities e and e', respectively,

$$f(e) = e',\ f\left(a^{-1}\right) = f(a)^{-1}$$

For a homomorphism $f : G \longrightarrow H$, if for every homomorphisms $g, h : H \longrightarrow K$, $g \circ f = h \circ f \implies g = h$, f is called an **epimorphism**. If for every $g, h : K \longrightarrow G$, if $f \circ g = f \circ h \implies g = h$, we call h a **monomorphism**.

An invertible homomorphism is called an **isomorphism**. By inverse, we mean inverse homomorphism. Two groups are said to be isomorphic if there exists an isomorphism.

3. Let $f : G \longrightarrow H$ be a group homomorphism. Prove that a group homomorphism is an isomorphism if and only if it is a bijection as a function.

A relation R between two sets A and B is nothing but a subset of $A \times B$.

$$R \subseteq A \times B = \{(a, b) | a \in A, \, b \in B\}$$

When $(a, b) \in R$, we say that a and b are related under R and we write aRb. A relation $\sim$ between two identical sets A are called a relation on A.

Let $\sim$ be a relation on A. $\sim$ is said to be **reflective** if for each $a \in A$, $a \sim a$. It is said to be **symmetric** if for each a and $b \in A$, $a \sim b \implies b \sim a$. It is said to be **transitive** if for each $a, \, b,$ and $c \in A$, $a \sim b \wedge b \sim c \implies a \sim c$.

A reflective, symmetric, transitive relation is called an **equivalence relation**.

For a set X, a subset of the powerset of X whose members are non-empty, pairwise disjoint with union equal to X is called a **partition**.

Let X be a set and $\sim$ be an equivalence relation for an element $x \in X$, the set

$$[x]_\sim := \{x' \in X | x' \sim x\}$$

is called the **equivalence class** of x (under $\sim$). Then the set

$$X/\sim - \{[x]_\sim | x \in X\}$$

forms partition.

Conversely, for a partition P of X, the relation $\sim_P$ be

$$x \sim_P y :\equiv \exists C \in P \textbf{s.t.} \, \{x, y\} \subseteq C$$

Then it becomes an equivalence relation.

4. Let X be a set and $\mathcal{E}$ be the set of all equivalence relations and $\mathcal{P}$ be the set of all partitions. Prove that the map

$$X/\bullet : \mathcal{E} \longrightarrow \mathcal{P}, \, \sim \mapsto X/\sim$$

is a bijection.

For a group G, a subset with the induced operation which forms a group is called a **subgroup**. If H is a subgroup of G, then we write $H < G$.

Let $f : G \longrightarrow H$ be a group homomorphism. The inverse image of the identity of H is called the **kernel** of f.

5. Let G be a group.

(1) Prove that if $H \subseteq G$ is nonempty and for every $g, h \in H$, $gh^{-1} \in H$, then H is a subgroup.

(2) Prove that a kernel of a homomorphism $G \longrightarrow H$ is a subgroup of G.

For a group G and a subgroup H and element g of G, the set

$$gH = \{gh|h \in H\}$$

is called a **left coset** or simply a **coset**. Similarly, $Hg = \{hg|h \in H\}$ is called a **right coset**.

$$G/H = \{gH|h \in G\}$$

is called the quotient of G by H and $|G/H|$ is called the index of the subgroup H and written $[G : H]$.

Two sets A and B are said to be **equinumerous** if there is a bijection between them.

6. Let G be a group and H be a subgroup.

(1) Prove that all cosets are equinumerous.

(2) G/H is a partition of G

(3) (Lagrange's theorem) Prove that the index of H is a divisor of the order of G provided that $|G| < \infty$.

Let S be a subset of G. The smallest subgroup of G which contains S is called the group **generated** by S.

For additive group, for positive integers m and n, we define $(m-n)g = mg - ng$. For multiplicative group, we define $g^{m-n} = g^m \left(g^n\right)^{-1}$.

If a group is generated by an element, then it is said to be **cyclic**. The order of $\langle g \rangle$ is also called the order of g which is written as $\mathrm{ord}(g)$.

7. Let G be a group with identity 1.

(1) Prove that the group generated by g is

$$\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$$

(2) Let the order of g is finite. Prove that $g^{\mathrm{ord}(g)} = 1$.

(3) $g^n = 1 \leftrightarrow \mathrm{ord}(g)|n$.

(4) (Euler) If G is finite, then $g^{|G|} = 1$.

Let G be a group and $g \in G$ is an element and A, B are sets.

We define $gA = \{ga|a \in A\}$, $AB = \{ab|a \in A \wedge b \in B\}$. Note that products between sets and elements also has associative property. This intuitively clear fact will not proved rigorously although the proof is somewhat involved.[1] The following example should be suffices to illustrate the situation

$$((xy)H)z = x(y(Hz)) = \{xyhz | h \in H\}$$

A subgroup N of G is said to be **normal** if for every elements $x \in G$, $xN = Nx$.

8. Let H be a subgroup of G. Prove that the followings are all equivalent.

a. H is a normal subgroup of G.
b. $\forall x \in G, xHx^{-1} = H$
c. $\forall x \in G, (xH)(yH) = (xyH)$.
d. H is a kernel of a homomorphism $f : G \longrightarrow T$ for some group T.

Theorem 2. *Let G and H be groups with homomorphism $\phi : G \longrightarrow H$. Then $\phi(G) \simeq G/\ker\phi$ is canonical. $g\,|\phi\rangle \mapsto \phi(g)$.*

Hence for epimorshism $\phi : G \longrightarrow \operatorname{Ran}\phi$, we have the following commuting diagram.

$$\begin{array}{ccc} G & \xrightarrow{\ \phi\ } & \operatorname{Ran}\phi \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \tilde{\phi}} & \\ G/\ker\phi & & \end{array}$$

Let R be an abelian group with $+$. Suppose that there is another operation $\cdot$ on R which forms a semi-group and distributes over addition. Then the structure is called a **ring**.

If the multiplication is commutative, we say R is commutative. If the multiplicative structure is monoid, then we say R is unital.

9. Let R be a ring.

(1) Prove that $0x = x \cdot 0 = 0$.
(2) Prove that $x(-y) = (-x)y = -(xy)$.

10. Let R be a ring such that $x^2 = x$ for every element of $x \in R$. Prove that R is commutative.

Example 1.2. Some examples of rings

[1] Actually, the term 'associative' is not properly defined where the intention is clear from the context.

(1) $\mathbb{Z}$ with usual operations.

(2) $M_n(\mathbb{R})$, a unital ring.

(3) $\mathbb{R}[x]$, a unital commutative ring.

For a ring R, if for every $r \in R$, $rI \subset I$ is called a **left ideal** where I is nonempty. **Right ideal** is defined similarly. A left and right ideal is simple called an **ideal**.

In a ring R and ideal I, $R/I = \{x + I | x \in \mathbb{R}\}$ is the quotient ring of R by I.

In a ring R and a set S, the ideal generated by S is the smallest ideal which contains S.

11. For a ring R and an ideal I, prove that R/I is a ring with induced operations.

If a ring R, if $lr = 0$ but $l \neq 0$ and $r \neq 0$, then l and r are called a left and right zerodivisor, respectively.

In a commutative ring, $m = qd$, $d \neq 0$ then m is called a **multiple** of d and d is said to be a **divisor** of m and q is called the quotient when m is divided by q. In this case $d|m$.

12. Find all zero divisors of $M_2(\mathbb{C})$.

2 Unital commutative rings

In this section, we will basically discuss on a unital commutative ring. A divisor of the unity is said to be (multiplicatively) **invertible**. An element u is called a unit if it is multiplicatively invertible. The set of all units in a unital commutative ring R forms a group R^* which is called the **multiplicative group** of R. For any a and b, there is a unit u such that $b = ua$, then b is said to be **associated** with a.

The only element associated with 0 is zero itself. For any nonzero element a, b is associated with a iff $a|b \wedge b|a$.

13. Prove that in a unital commutative ring, the associativity between elements is an equivalence relation.

A divisor d of a which is not associated with a nor a unit is called a **proper divisor**.

An element r which is nonzero, non unit is said to be irreducible if it has no proper divisors.

A nonzero, nonunit element p is said to be **prime** if

$$p|ab \implies p|a \vee p|b$$

14. In a commutative ring R, prove the followings

(1) $x \neq 0 \iff x|0$

(2) $1|x$ provided $|R| \neq 1 \wedge 1 \in R$.

(3) $a|b \wedge b|c \implies a|c$.

A unital commutative ring with no zero divisor is called an **integral domain**.

Theorem 3. *In an integral domain, every prime element is irreducible.*

An integral domain with the following property is called a **unique factorization domain**

> Every nonzero element can be written as a finite product of irreducible elements and it is unique up to associativity and ordering.

A ring $S \subseteq R$ is called a subring if it is a ring operation induced from R. When R is unital, we say S is sub unital ring if it is subring and $1_R \in S$. Note that a subring which is unital by itself may not be a sub unital ring.

15. Find a subring of $\mathbb{Z}/10\mathbb{Z}$ which is unital but does not have $\overline{1}$.

For a unital commutative ring K and its sub unital ring R and $\alpha \in K$,

$$R[\alpha] = \left\{ \sum_{j=0}^{n} r_j \alpha^j | n = 0, 1, 2, \ldots, r_j \in R \right\}$$

16. Let $R = \mathbb{Z}[\sqrt{-5}]$.

(1) Find all units.

(2) Prove that 6 can be factored into two essentially different way.

3 UFD

Theorem 4. *In a UFD, every irreducible element is a prime element.*

Proof. Let r be an irreducible element.

By definition, r is non-zero, non-unit. Suppose that $r|ab$. We need to prove either $r|a$ or $r|b$ to complete the proof. Let q be such that $ab = qr$. If ab were zero, there would be nothing to prove. So suppose that $ab \neq 0$. Then a and b are factored into a finite products of irreducible elements possibly including empty product which produces 1. qr also can be written as a products of irreducibles which should contain r. Since we are working in UFD, among irreducibles whose product is ab should contain r up to associativity which should come from either factorization of a or b. Hence we should have either $r|a$ or $r|b$. $\square$

17. In an integral domain, prove that if every nonzero element is expressed in a product of irreducible elements and every irreducible elements are prime elements, the domain is actually UFD.

In a commutative ring R, if there exists $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ such that

(1) If $ab \neq 0$, then $\varphi(a) \leq \varphi(ab)$.

(2) For each a, $b \neq 0$, there exists q, r such that $a = qb + r$ and $r = 0 \vee (r \neq 0 \wedge \varphi(r) < \varphi(b))$.

then R is called an Euclidean ring. An integral domain which is Euclidean, is called a Euclidean domain.

A commutative ring with unity in which every nonzero elements are units is called a **field**.

18. Prove that $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

In a field, the smallest natural number p such that $p = 0$ is called a characteristic of the field. Otherwise we say the characteristic of the field is zero.

19. Prove that the characteristic of a field is prime number.

A field homomorphism is a unital ring homomorphism which means that the map commutes with operations and maps unity to unity.

20. Let F and K be a field.

(1) Prove that if there is a field homomorphism $F \longrightarrow K$, then the characteristic of F and K coincide.

(2) There is a unique field homomorphism $\mathbb{Z}/p\mathbb{Z} \longrightarrow F$ if F has characteristic p.

(3) There is a unique field homomorphism $\mathbb{Q} \longrightarrow F$ if F has characteristic zero.

Example 3.1. The followings are examples of Euclidean domains.

1. $\mathbb{Z}$. A Euclidean function takes absolute values.
2. $F[x]$ where F is a field and x is an indeterminate. A Euclidean function takes the degree as the value.

In a UFD, the greatest common divisor makes sense. Let a and b be elements in a UFD where not both equals to zero. g is called the greatest common divisor of a and b if is it a common divisor and any other common divisors are divisors of g. We can prove the existence of g using prime factorization of the ring. We can specify greatest common divisor up to multiple of units which supports the usage of the definite article.

Two elements a and b are said to be coprime if they are not both equal to zero and the only common divisors are the units.

Theorem 5 (Bézout's theorem)**.** *In a Euclidean domain, for every a, b there exists a solution for the equation*

$$ax + by = g$$

where g is the GCD of a and b. Especially, if a and b are coprime, then the unity can be expressed as a linear combination of a and b.

Proof. Apply Euclidean algorithm.

Without loss of any generality, we may assume that $b \neq 0$. Let q_1, r_1 be such that $a = q_1 b + r_1$ where $\varphi r_1 < \varphi b$. If $r_1 = 0$, then we stop and let $k = 0$. b is the GCD of a and b. If $r_1 \neq 0$ let $b = q_2 r_1 + r_2$ where $\varphi r_2 < \varphi r_1$. If $r_2 = 0$, then we stop and let $k = 1$. Like this manner, for each positive integer n, if $r_n \neq 0$, let $r_{n-1} = q_{n+1} r_n + r_{n+1}$ and if $r_{n+1} = 0$ then stop the process and set $k = n$.

Setting $r_0 = b$, we have r_k as GCD of A and B and r_k can be expressed as a linear combination of a and b i.e. for some x, y,

$$r_k = ax + by$$

□

Proposition 3.1. *In a Euclidean domain with Euclidean function f, let $\varepsilon = f(1)$.*

1. *$f(u) = \varepsilon$ is equivalent to u is a unit.*
2. *For each nonzero a and a proper divisor d, $f(d) < f(a)$.*

Proof. Since $n = 1n$, $f(1) \leq f(n)$. Therefore ε is minimum of f.

If $f(n) = \varepsilon$, then n is a unit. To see this suppose that n cannot divide 1, then there should exists r such that $f(r) < f(n)$. Conversely, if n is a unit, then $f(u)$ should equals to ε since $1 = uu^{-1}$ implies $f(u) \leq f(1)$.

Now let d be a proper divisor of $a \neq 0$. $a = qd$ and q is also a properdivisor of a. Now divide d by a. $d = ka + r$. Since d is a proper divisor, we have $r \neq 0$. Hence $f(r) < f(a)$. And $r = d - ka = d - kqd = d(1 - kq)$ and q is not a unit, $1 - kq \neq 0$ hence $f(d) \leq f(r) < f(a)$. □

Theorem 6. *A Euclidean domain is a ufd.*

Proof. Let R be a Euclidean domain with a Euclidean function φ. It suffices to show that every element can be factored into irreducibles and each irreducible element is prime.

Suppose that there are some non-zero elements which cannot be factored into irreducibles. Pick k which is so with minimal Euclidean function value. Note that k is non-unit, non-zero, reducible. Let d be its proper divisor and $k = qd$. Then by the minimality of k, and by proposition 3.1, q and d can be written as a product of irreducibles which is an absurdity. Hence every nonzero elements can be factored into irreducibles.

Now let r be an irreducible and $r|ab$ but $r \nmid a$. Since r is irreducible, r and a are coprime. Let u, v be $ur+va=1$. Then $b=bur+abv$ so $r|b$. This completes the proof. □

As for the case of groups, there goes an isomorphism theorem for rings.

Let R and S be rings and $f : R \longrightarrow S$ be a ring homomorphism. Then the kernel of f is an ideal of R and,

$$R/\ker f \simeq f(R)$$

where the canonical isomorphism is given by $r+\ker f \mapsto f(r)$.

Consider a unital commutative ring S. We may treat polynomials over S formally. However, in this article, we shall adapt usual informal definition. A polynomial $f(x)$ over a sub unital ring R of S is called a minimal polynomial of an element $\alpha \in S$ if evaluation of $f(x)$ at $x=\alpha$ vanishes and the degree of $f(x)$ is minimal among nonzero polynomials with this property. A polynomial is said to be monic if it is nonzero and the leading coefficient is a unit. On the other hand, for an element $\alpha \in S$, we define $R[\alpha]$ to be the smallest sub unital ring of S which contains $R \cup \{\alpha\}$. Equivalently, $R[\alpha]$ is the set of all values of evaluation of polynomials $R[x]$ at $x=\alpha$.

In a unital commutative ring R, an ideal generated by an element $f \in R$ is $\langle f \rangle = Rf$.

Theorem 7. *For a commutative ring with unity S and a unital subring R and an element $\alpha \in S$, if the minimal polynomial of α is monic then*

$$R[\alpha] \simeq R[x]/\langle f(x) \rangle$$

Proof. Let $\varphi : R[x] \longrightarrow S$ be the evaluation homoorphism such that $x \mapsto \alpha$. Then $R[\alpha]$ is the range of φ. By isomorphism theorem, it suffices to show that $\ker\varphi = \langle f(x) \rangle$.

Clearly $\langle f(x) \rangle \subseteq \ker\varphi$. To see $\ker\varphi \subseteq \langle f(x) \rangle$, let $g(x) \in \ker\varphi$. Since $f(x)$ is monic, we can find $q(x)$ and $r(x)$ such that

$$g(x) = q(x)f(x) + r(x), \deg r(x) < \deg f(x)$$

To do this, one just need to perform the usual polynomial long division because $f(x)$ is monic. Then the minimality of degree of $f(x)$ asserts that $r(x)=0$. Hence $g(x) \in \langle f(x) \rangle$. □

Wherefore we do not distinguish these two structures.

4 Gaussian integers

Contents of this section is mainly obtained from [Art91].

A number $x+yi$ is called a Gaussian integer if $x, y \in \mathbb{Z}$.

21. Prove that the ring of Gaussian integers is Euclidean.

22. Prove the followings.

(1) A nonzero integer d is a divisor of an integer n in $\mathbb{Z}$ if and only if it is so in $\mathbb{Z}[i]$.

(2) A nonzero integer d is a divisor of $m+ni$ if and only if $d|m$ and $d|n$.

Theorem 8. *The following all holds.*

(i) p is a positive prime in $\mathbb{Z}$. Either p is a prime in $\mathbb{Z}[i]$ or a norm of a prime in $\mathbb{Z}[i]$.

(ii) π is a prime in $\mathbb{Z}[i]$. The norm of π is either a integer prime or a square of integer prime.

(iii) An integer prime is Gaussian prime if and only if it is 3 modulo 4.

(iv) For an integer prime p, the followings are all equivalent.

(a) p is a norm of a Gaussian prime.

(b) p is a sum of two squares.

(c) -1 is a quadratic residue modulo p

(d) $p \equiv 1, 2$ modulo 4.

Theorem 9. *The equation $x^2 + y^2 = n$ has an integer solution if and only if every prime p which is congruent 3 modulo 4 has an even exponent in the factorization of n.*

23. Find all primitive Pythagorean triples.

Theorem 10. *Every finite subgroup of a multiplicative group of a field is cyclic.*

Proof. Let F be a field and G be a finite subgroup of F^*. Then every element of G is of finite order which is a divisor of $n = |G|$.

For each $d|n$, let G_d be the set of element of order d. Suppose that $G_d \neq \emptyset$. Let $\alpha \in G_d$. Then $\langle\alpha\rangle \subseteq \left|\left\{x \in G | x^d = 1\right\}\right|$. Since F is a field, we have $\left|\left\{x \in G | x^d = 1\right\}\right| \leq d$. Noting that $|\langle\alpha\rangle| = d$, we have $\langle\alpha\rangle = \left\{x \in G | x^d = 1\right\}$. It follows that $|G_d| = \varphi(d)$.

Therefore for each $d|n$, we have either $|G_d| = 0$, or $|G_d| = \varphi(d)$. Now

$$n = |G| = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n$$

and the equality condition gives that $|G_d| = \varphi(d)$ for each $d|n$. Especially, $|G_n| = \varphi(n)$ so there are exactly $\varphi(n)$ generators of G. □

24. Prove that for every prime p such that $p \equiv -1(\text{mod}7)$, there exists a natural number n such that $n^3 + n^2 - 2n - 1$ is a multiple of p. (Korea Winter School 2014)

5 Algebraic Integers

Contents of this section is mainly obtained from [AD08].

A complex number is said to be algebraic if it is a root of a polynomial in $\mathbb{Q}[x]$. An algebraic number is called an **algebraic integer** if its minimal monic polynomial is actually i $\mathbb{Z}[x]$.

Let d be a square free integer including all negative integers. (So, -4 is excluded.) The field $F = \mathbb{Q}[\sqrt{d}]$ is called a **quadratic number field**.

25. Answer.

(1) Determine all algebraic integers which are rational numbers.

(2) Prove that Gaussian integers are algebraic integers.

(3) Prove that in the quadratic number field $F = \mathbb{Q}[\sqrt{d}]$, $\delta = \sqrt{d}$, $\alpha = a + b\delta$ is an algebraic integer if and only if $2a$ and $a^2 - b^2 d$ are integers.

Theorem 11. *Algebraic integers forms a ring.*

26. Consider the sequence $(x_n)_{n \geq 0}$ defined by $x_0 = 4$, $x_1 = x_2 = 0$, $x_3 = 3$ and $x_{n+4} = x_{n+1} + x_n$. Prove that for any prime p, the number x_p is a multiple of p. (AMM 1998)

27. Determine whether

$$\sqrt{1001^2 + 1} + \sqrt{1002^2 + 1} + \cdots + \sqrt{2000^2 + 1}$$

be a rational number or not? (China TST 2005)

6 Vector spaces

Let F be a field. Consider an additive group V and $\mathrm{End}(V)$ be the ring of endomorphisms on V. With a unital ring homomorphism $\varphi : F \longrightarrow \mathrm{End}(V)$, V is called a vector space over F.

A basis of V over F is a maximal linearly independent set $B \subseteq V$.

Let me accept the following theorem.

Theorem 12. *The followings holds.*

1. *For every finitely generated vector space V, there is a basis.*

2. *For every finitely generated vector space V, there is a definite number of elements for every basis, called the dimension.*

3. *If AC holds, then every vector space has a basis.*

28. Prove that there exists a non-linear Cauchy function. That is to say, prove that there exists $f : \mathbb{R} \longrightarrow \mathbb{R}$ such that for every $x, y \in \mathbb{R}$, $f(x+y) = f(x) + f(y)$ but there is $r \in \mathbb{R}$ such that $f(r) \neq f(1)r$.

An **incidence geometry** $G = (P, L)$ is a pair of sets called the set of all points and lines equipped with a relation I between P and L such that

i. For every distinct pair of points $\{P, Q\}$ there exists exactly one line $\ell \in L$ which passes through each member of the pair.

ii. For every line l, there exists at least two distinct points on it.

iii. There exists at least three points which does not lie on a line.

Let F be a field and V be a two dimensional vector space. Prove that ordinary one dimensional affine spaces form a model of incidence geometry with additional parallel postulate.

> For every line l and a point P not on l, there exists unique line passing through P and pallel to l.

A **projective geometry** $G = (P, L)$ is a pair of sets called the set of all points and lines equipped with a relation I between P and L such that

i. For every distinct pair of points there exists exactly one line which passes through each of the members of the pair.

ii. For every distinct pair of lines there exists exactly one point which laid on both of them.

iii. There are four points such that no line passes through more than two of them.

A projective geometry is a fortiori an incidence geometry.

Let G be an incident geometry with parallel postulate. Let P_∞ be the set of equivalence class of the parallel lines. Extent L to L' by pairing l with its equivalence class, $(l, [l])$. These lines in L' are called augmented lines. Two augmented lines posses each ordinary points on it and the equivalence class. Now, attach one more line l_∞ which passes only those P_∞. Then the geometry with points $P \cup P_\infty$ and $L' \cup l_\infty$ forms a projective geometry. This process is called the projective completion.

29. There are 21 towns. Each airline runs direct flights between every pair of towns in a group of five. What is the minimum number of airlines needed to ensure that at least one airline runs direct flights between every pair of towns? (Russia 1988 grade 8)

Exercises

30. Find all integral solutions of the equation $x^2 + 1 = y^3$. [Ros14, 603p]

31. Find all integral solutions of $x^2 + y^2 = z^3$. [Ros14, 604p]

32. Let α and π relatively prime Gaussian integers. Prove that

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$$

when π is a prime in $\mathbb{Z}[i]$. [Ros14, 604p]

33. Define $a_1 = 0, a_2 = 2, a_3 = 3, a_{n+3} = a_n + a_{n+1}$ Prove that $\forall$ prime number p we have $p|a_p$ (AOPS user CeuAzul)

34. Let $f(x) = x^8 + 4x^6 + 2x^4 + 28x^2 + 1$. Let $p > 3$ be a prime and suppose there exists an integer z such that p divides $f(z)$. Prove that there exist integers z_1, z_2, …, z_8 such that if

$$g(x) = (x - z_1)(x - z_2) \cdots (x - z_8)$$

then all coefficients of $f(x) - g(x)$ are divisible by p. (IMO shortlist 1992)

35. Let $n > 1$ be an integer. In a circular arrangement of n lamps $L_0, \ldots, L_{n-1}$, each of of which can either ON or OFF, we start with the situation where all lamps are ON, and then carry out a sequence of steps, $Step_0, Step_1, \ldots$. If L_{j-1} (j is taken mod n) is ON then $Step_j$ changes the state of L_j (it goes from ON to OFF or from OFF to ON) but does not change the state of any of the other lamps. If L_{j-1} is OFF then $Step_j$ does not change anything at all. Show that:

(a) There is a positive integer $M(n)$ such that after $M(n)$ steps all lamps are ON again.

(b) If n has the form 2^k then all the lamps are ON after $n^2 - 1$ steps.

(c) If n has the form $2^k + 1$ then all lamps are ON after $n^2 - n + 1$ steps.

(IMO shortlist 1993)

36. The sequence $a_0,\ a_1,\ a_2,\ \ldots$ is defined as follows: $a_0 = 2, \quad a_{k+1} = 2a_k^2 - 1 \quad$ for $k \geq 0$. Prove that if an odd prime p divides a_n, then 2^{n+3} divides $p^2 - 1$. (IMO shortlist 2003)

37. Let p be a positive prime integer and k be a positive integer. Suppose that there are $p^{2k} + p^k + 1$ towns. Each airline runs direct flights between every pair of towns in a group of $p^k + 1$. What is the minimum number of airlines needed to ensure that at least one airline runs direct flights between every pair of towns?

References

[AD08] Titu Andreescu and Gabriel Dospinescu. *Problems from the book.* XYZ press, 2008.

[Art91] Michael Artin. *Algebra.* Prentice Hall, 1991.

[Ros14] Kenneth H. Rosen. *Elementary Number Theory.* Pearson, sixth edition, 2014.