MA-219 Linear Algebra

1. Algebraic Structures

August 11, 2003 ; Submit solutions **before 11:00AM ; August 18, 2003.**

1.1. (Relations) Let X and Y be sets. A relation R between X and Y is a subset $R \subseteq X \times Y$, i.e. an element $R \in \mathfrak{P}(X \times Y)$. For the expression "$(x, y) \in R$" we shall write "$xRy$" and say that "*$x$ is related to y with respect to R*", $x \in X$, $y \in Y$. In the case $Y = X$ we say that $R \subseteq X \times X$ is a relation on X.

a). The map $\mathfrak{P}(X \times Y) \to \mathfrak{P}(Y)^X$ defined by $R \mapsto \big(x \mapsto \{y \in Y \mid xRy\}\big)$ is bijective. Write down the inverse of this map. (**Remark:** With this bijection, one can identify every relation $R \subseteq X \times Y$ between X and Y as a map from X into $\mathfrak{P}(Y)$.)

A relation $R \in \mathfrak{P}(X \times X)$ on X is called an equivalence relation if it satisfies:

(1) (Reflexivity) : xRx for all $x \in X$.
(2) (Symmetry) : xRy implies yRx, where $x, y \in X$.
(3) (Transitivity): xRy and yRz implies xRz, where $x, y, z \in X$.

Let $\mathfrak{E}(X) \subseteq \mathfrak{P}(X \times X)$ denote the set of all equivalence relations on X.

b). The restriction of the map $\alpha : \mathfrak{P}(X \times X) \to \mathfrak{P}\big(\mathfrak{P}(X)\big)$, $R \mapsto \big\{\{y \in X \mid xRy\} \mid x \in X\big\}$ is injective on the subset $\mathfrak{E}(X)$.

A partition $\mathfrak{Z}$ of the set X is a subset $\mathfrak{Z} \subseteq \mathfrak{P}(X)$ of non-empty disjoint subsets of X such that their union is X. Therefore $\mathfrak{Z} \in \mathfrak{P}\big(\mathfrak{P}(X)\big)$. Let $\mathfrak{Z}(X) \subseteq \mathfrak{P}\big(\mathfrak{P}(X)\big)$ denote the set of all partitions of X.

c). In the situation of **b)**: α maps $\mathfrak{E}(X)$ bijectively onto $\mathfrak{Z}(X)$, i.e. to each equivalence relation R on X, α associates a unique partition $\alpha(R)$ of X and conversely.

The partition $\mathfrak{Z}(R)$ corresponding to the equivalence relation R on X is usually denoted by X/R and is called the quotient set of X with respect to the equivalence relation R. The elements $[x] := [x]_R := \{y \in X \mid xRy\} \in X/R$ are called the equivalence classes of x with respect to R.

1.2. Let G be a (multiplicatively written) monoid. An element $x \in G$ is called invertible if there exists $x' \in G$ such that $x'x = e = xx'$. In this case the inverse x' is uniquely determined by x and is denoted by x^{-1}. Let $G^\times$ denote the set of all invertible elements of G.

(1) $e \in G^\times$.
(2) If $x, y \in G^\times$, then $xy \in G^\times$ and $(xy)^{-1} = y^{-1}x^{-1}$.
(3) $G^\times$ is a group under the induced binary operation of G.
(4) G is a group if and only if $G = G^\times$.

– The group $G^\times$ is called the group of invertible elements of G or the unit group of G. For example, in a field K with respect to multiplication the unit group is $K^\times = K - \{0\}$. For the monoid $(X^X, \circ)$ of the set of all maps of a set X into itself, the unit group is $(X^X)^\times = \mathfrak{S}(X)$ the set of all permutations of X (proof!).

1.3. Let $G \subseteq \mathbb{Z}$ be a subset of integers which contains atleast one positive integer and atleast one negative integer. Suppose that G is closed under the usual addition in $\mathbb{Z}$ i.e. $a + b \in G$ whenever $a, b \in G$. Prove that $(G, +)$ is a group. (**Hint:** Use T1.3.)

1.4. a). For $a, b \in \mathbb{R}$, let $f_{a,b} : \mathbb{R} \to \mathbb{R}$ be defined by $f_{a,b}(x) := ax + b$, $x \in \mathbb{R}$. Then $G := \{f_{a,b} \mid a, b \in \mathbb{R},\ a \neq 0\}$ with the composition as a binary operation is not a commutative group. (This is the well-known affine group of $\mathbb{R}$ and is denoted by $\mathrm{A}_1(\mathbb{R})$; Its elements are called the affine linear maps.)

b). Let G be a finite group with the identity element e. Suppose that $|G| = n$ and $(a_1, \dots, a_n) \in G^n$. Then there exist r, s with $0 \leq r < s \leq n$ such that $a_{r+1} \cdots a_s = e$. (**Hint:** The $n+1$ products $a_1 \cdots a_s$, $s = 0, \dots, n$, cannot be pairwise distinct.)

1.5. Let X be a set.

a). The power set $\mathfrak{P}(X)$ of a set X with the union as addition and the intersections as multiplication is never a field. – which elements in $\mathfrak{P}(X)$ are 0 and 1. (This is infact almost never a ring!)

b). Show that $\mathfrak{P}(X)$ with the symmetric difference $\triangle$ as addition and the intersection $\cap$ as multiplication is a commutative ring with $\emptyset$ as the zero element 0 and X as the unit element 1. This ring is called the set-ring of X. If $|X| = 1$, then this ring is a field with two elements; in the other case the set-ring of X is not a field. (**Hint:** For verification of the ring-axioms use indicator functions and their rules, See T1.1.)

On the other side one can see (simple) test-exercises; their solutions need not be submitted.

Test-Exercises

T1.1. (Indicator functions) Let X be a set. For a subset $A \in \mathfrak{P}(X)$, let A' be the complement of A in X and let $e_A : X \to \{0, 1\}$, $e_A(x) = 1$ if $x \in A$ and $e_A(x) = 0$ if $x \notin A$, denote the indicator function of A. For $A, B \in \mathfrak{P}(X)$, prove that: $e_{A\cap B} = e_A e_B$, $e_{A\cup B} = e_A + e_B - e_A e_B$, $e_{A\setminus B} = e_A(1-e_B)$. In particular, $e_{A'} = 1 - e_A$ and $e_{A \triangle B} = e_A + e_B - 2e_A e_A$.

T1.2. Let $f : X \to Y$ be a map and let $f_* : \mathfrak{P}(X) \to \mathfrak{P}(Y)$, $f^* : \mathfrak{P}(Y) \to \mathfrak{P}(X)$ be the maps induced by f, $A \mapsto f(A)$, $A \subseteq X$, respectively $B \mapsto f^{-1}(B)$, $B \subseteq Y$.

a). The following are equivalent: (i) f is injective. (ii) f_* is injective. (iii) f^* is surjective.
b). The following are equivalent: (i) f is surjective. (ii) f_* is surjective. (iii) f^* is injective.
c). If f bijective, then so are f_* and f^* ; moreover, they are inverses of each other.

T1.3. a). (Well-ordering principle) Prove that the *principle of mathematical induction* is equivalent to the following statement: *If X is a non-empty subset of $\mathbb{N}$, then X has a smallest element*, i.e. *there exists an element $x_0 \in X$ such that $x_0 \leq x$ for all $x \in X$.*
b). (Division algorithm) Let a and b be integers with $b \neq 0$. Then there exist unique integers q and r such that $a = qb + r$, with $0 \leq r \leq |b|$.

T1.4. a). Let $a, n \in \mathbb{N}$ with $a, n \geq 2$. If $a^n - 1$ is prime, then $a = 2$ and n prime. In particular, $a^n - 1$ is a Mersenne's prime number. (**Remark:** The problem of primality of $a^n - 1$ is thus reduced to that of the primality of $2^p - 1$.) [1])
b). Let $a, n \in \mathbb{N}^*$ with $a \geq 2$. If $a^n + 1$ is prime, then a is even and n is a power of 2. [2])
c). For $a, m, n \in \mathbb{N}^*$ with $a \geq 2$ and $d := \gcd(m, n)$, $\gcd(a^m - 1 , a^n - 1) = a^d - 1$. (**Hint:** It is easy to reduce to the case $d = 1$. Then $(a^m - 1)/(a - 1) = a^{m-1} + \cdots + a + 1$ and $(a^n - 1)/(a - 1) = a^{n-1} + \cdots + a + 1$ are relatively prime.)

T1.5. a). Let $n, k \in \mathbb{N}^*$ be relatively prime. Then n divides $\binom{n}{k}$ and k divides $\binom{n-1}{k-1}$. (For $n, k \in \mathbb{N}$, $\binom{n}{k} := \dfrac{n(n-1)\cdots(n-k+1)}{k!}$ is the coefficient of X^k in $(1+X)^n$ and is called the k-th binomial coefficient. **Hint:** The formula: $k\binom{n}{k} = n\binom{n-1}{k-1}$!)
b). Let p be a prime number. For $r, k \in \mathbb{N}$ with $r < k < p$, the integer $\binom{p+r}{k}$ is divisible by p. In particular, the number $\binom{p}{k}$ if divisible by p for $0 < k < p$.

T1.6. a). Let $a, b \in \mathbb{N}^*$. Then $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.
b). Let $a_1, \ldots, a_n \in \mathbb{N}^*$ be positive natural numbers, $n \geq 1$, and $a := a_1 \cdots a_n$ be their product. The following statements are equivalent:
(i) $a_1, \ldots, a_n$ are pairwise relatively prime, i.e. $\gcd(a_i, a_j) = 1$ for all $1 \leq i, j \leq n, i \neq j$.
(ii) If a natural number c divides each of the number $a_1, \ldots, a_n$, then a divides the number c .
(iii) $\operatorname{lcm}(a_1, \ldots, a_n) = a$.
(iv) $\gcd(a/a_1, \ldots, a/a_n) = 1$.
(v) There exist integers $s_1, \ldots, s_n$ such that $\dfrac{1}{a} = \dfrac{s_1}{a_1} + \cdots + \dfrac{s_n}{a_n}$.
c). Let $a_1, \ldots, a_n \in \mathbb{N}^*$. Then there exist integers $u_1, \ldots, u_n \in \mathbb{Z}$ such that $\gcd(a_1, \ldots, a_n) = u_1 a_1 + \cdots + u_n a_n$. In particular, $a_1, \ldots, a_n$ are relatively prime if and only if there exist integers $u_1, \ldots, u_n \in \mathbb{Z}$ such that $1 = u_1 a_1 + \cdots + u_n a_n$. (**Hint:** Use $\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$.)
d). Find integers u_1, u_2, u_3 such that $u_1 \cdot 88 + u_2 \cdot 152 + u_3 \cdot 209 = 1$.

[1]) (Mersenne's numbers) The numbers $M_p := 2^p - 1$, where p prime, are called Mersenne's numbers. It was asserted by MERSENNE in 1644 that $M_p := 2^p - 1$ is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and composite for the other 44 values of p less than 257. The first mistake in Mersenne's statement was found about 1886 (EULER stated in 1732 that M_{41} and M_{47} are prime, but this was a mistake), when PERVUSIN and SEELHOLF discovered that M_{61} is prime. Subsequently four further mistakes were found and it need no longer be taken seriously. In 1876 LUCAS found a method for testing whether M_p is prime and used it to prove M_{127} is prime. This remained the largest known prime until 1951. In spite of many Mersenne primes that have been verified, no one has ever proved that there are infinitely many of them! In 1953 RAPHAEL M. ROBINSON had used the Swac computer to find a number of considerably larger primes and found that M_{2281} is a prime number of 687 digits. In 1963 the postage-meter stamp was used by the University of Illinois to honour the discovery of the prime M_{11213}. In 1978 two 18-year olds from Harward, California – LAURA NICKEL and CURT NOLL – used 440 hours of computer time to find the 6533-digit prime number M_{21701}. The biggest Mersenne number which is prime (till today!) is the Mersenne number corresponding to the prime $p = 756839$.

[2]) (Fermat's numbers) Numbers of the form $F_m := 2^{2^m} + 1$, $m \in \mathbb{N}$, are called Fermat's numbers. For $m = 0, 1, 2, 3, 4$ these numbers are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ and are prime numbers. The Fermat's numbers are of great interest in many ways; it was proved by GAUSS that: *if F_n is a prime p, then a regular polygon of p sides can be inscribed in a circle by Euclidean methods.* Since $F_{m+1} = 2 + F_0 \cdots F_m$, any two distinct Fermat's numbers are relatively prime. FERMAT conjectured that all were prime. EULER, however, in 1732 found that $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ divides $5^4 \cdot 2^{28} + 2^{32}$ and $5^4 \cdot 2^{28} - 1$ and hence also divide their difference $2^{32} + 1 = F_5$. In fact $F_5 = (641) \cdot (6700417)$. In 1880 LANDRY proved that $F_6 = 2^{2^6} + 1 = (274177) \cdot (67280421310721)$. More recently writers have proved that F_n is composite for $7 \leq n \leq 16$, $n = 18, 19, 23, 36, 38, 39, 55, 63, 73$ and many other larger values of n. MOREHEAD and WESTERN proved F_7 and F_8 are composite without determining a factor. No factor is known for F_{13} and F_{14}, but in all the other cases proved to be composite a factor is known. No Prime F_n has been found beyond F_4, so that Fermat's conjecture has not proved a very happy one. It is perhaps more probable that the number of primes F_n is finite (This is what is suggested by considerations of probability.)