Math 55a, Assignment #1, Sept. 19, 2003

Peano's Axioms. The five axioms of Giuseppe Peano are as follows.

(1) The set $\mathbb{N}$ of natural numbers contains an element 1.

(2) There is an *immediate successor* $x' \in \mathbb{N}$ defined for every element $x \in \mathbb{N}$.

(3) 1 is not an immediate successor of any element of $\mathbb{N}$.

(4) Two distinct elements of $\mathbb{N}$ have distinct immediate successors.

(5) If a subset E of $\mathbb{N}$ contains 1 and contains the immediate successor of every one of its elements, then E must be all of $\mathbb{N}$.

Problem 1. Use the five axioms of Guiseppe Peano to show that an element x of $\mathbb{N}$ is the immediate successor of some element of $\mathbb{N}$ if and only if it is not equal to 1. (Intuitively, this simply says that $x - 1$ is a natural number if and only if x is a natural number different from 1.)

Problem 2. Addition in $\mathbb{N}$ is defined by $x + 1 = x'$ and $x + y' = (x + y)'$. Use the five axioms of Giuseppe Peano to show that addition is commutative in the sense that $x + y = y + x$ for any $x, y \in \mathbb{N}$ according to the definition of addition defined above. (Of course, this is just the commutative law for addition of natural numbers.)

Problem 4. Let k be a positive integer. Let $p_1, \cdots, p_k$ be distinct prime numbers and $n_1, \cdots, n_k$ be positive integers. Let r be a prime number. Let $m = p_1^{n_1} \cdots p_k^{n_k}$. Assume that one of $n_1, \cdots, n_k$ is not divisible by r. Show that the r-th root of m is irrational.

Problem 5. Let E be a countable set of distinct real numbers $\{a_n\}_{n=1}^{\infty}$ with both an upper bound and a lower bound. For $k \in \mathbb{N}$ let $E_k = \{a_n\}_{n=k}^{\infty}$ and $b_k = \sup E_k$. Let $F = \{b_k\}_{k=1}^{\infty}$ and $c = \inf F$. Show that for every $\varepsilon > 0$ there exist at most a finite number of elements x of E with $x > c + \varepsilon$ and there exist an infinite number of elements y of E with $y > c - \varepsilon$.

Problem 6. Let E, F, G be subsets of the set $\mathbb{R}_{>0}$ of all positive real numbers such that both E and F admit an upper bound and G admits a positive number as a lower bound. Let $E + F$ be the set of all positive numbers $x + y$ with $x \in E$ and $y \in F$. Let $E \ominus F$ be the set of all real numbers $x - y$ with

$x \in E$ and $y \in F$. Let $E \cdot F$ be the set of all positive numbers $x \cdot y$ with $x \in E$ and $y \in F$. Let $\frac{E}{G}$ be the set of all positive numbers $\frac{x}{z}$ with $x \in E$ and $z \in G$. Verify the following relations.

$$\sup(E+F) = \sup E + \sup F.$$
$$\sup(E \ominus F) = \sup E - \inf F.$$
$$\sup(E \cdot F) = (\sup E)(\sup F).$$
$$\sup\left(\frac{E}{G}\right) = \frac{\sup E}{\inf G}.$$

Problem 7. A (Dedekind) cut (of the set $\mathbb{Q}_{>0}$ of all positive rational numbers) is defined as a nonempty proper subset E of $\mathbb{Q}_{>0}$ not containing its least upper bound such that $x < y, y \in E \Rightarrow x \in E$. The product $E \cdot F$ of two cuts E and F is defined as the cut consisting of all elements $x \cdot y$ with $x \in E$ and $y \in F$. Let $\mathbf{1}$ be the cut consisting of all rational number x with $0 < x < 1$. Let E^F the cut consisting of all positive rational numbers z with $z < x^y$ for some $x \in E$ and some $y \in F$.

(a) Verify that for every cut E there exists a cut F such that $E \cdot F = \mathbf{1}$.

(b) Verify that for any three cuts E, F, G the two cuts $\left(E^F\right)^G$ and $E^{(F \cdot G)}$ are equal.

Definition of Metrics of Fields. Let F be a field. A function $\varphi : F \to \mathbb{R}$ is called a *metric* of the field F if the following properties hold.

(1) (positivity) $\varphi(x) > 0$ for $0 \neq x \in F$ and $\varphi(0) = 0$.

(2) (triangle inequality) $\varphi(x+y) \leq \varphi(x) + \varphi(y)$.

(2) (multiplicativity) $\varphi(xy) = \varphi(x)\varphi(y)$.

A metric φ of the field F is called *nontrivial* if $\varphi(x) \neq 1$ for some $0 \neq x \in F$. A metric φ of the field F is called *non-Archimedean* if the following stronger form of the triangle inequality $\varphi(x+y) \leq \max(\varphi(x), \varphi(y))$ holds for $x, y \in F$. Otherwise, it is called *Archimedean.* A metric φ of a field F is non-Archimedean if and only if $\varphi(n \cdot 1) \leq 1$ for every element of $n \in \mathbb{N}$, where the factor 1 in $n \cdot 1$ is the unit element of the field F (and $n \cdot 1$ can be alternatively described as the sum of n copies of the unit element 1 of F.)

Problem 8. Show that a metric φ of a field F is non-Archimedean if and only if $\varphi(n \cdot 1) \leq 1$ for every element of $n \in \mathbb{N}$, where the factor 1 in $n \cdot 1$ is the unit element of the field F (and $n \cdot 1$ can be alternatively described as the sum of n copies of the unit element 1 of F.)

Problem 9. Show that every nontrivial Archimedean metric φ of the field $\mathbb{Q}$ of all rational numbers must of the form $\varphi(x) = |x|^\gamma$ for some $0 < \gamma \leq 1$.

Hint: Choose $a \in \mathbb{N}$ such that $\varphi(a) > 1$ and choose $0 < \gamma \leq 1$ with $\varphi(a) = a^\gamma$. For any $n \in \mathbb{N}$, by expressing $a = \sum_{j=1}^k c_j a^j$ with $0 \leq c_j < a$ and applying φ to both sides, show that $\varphi(n) \leq C n^\gamma$ for some constant C independent of n. Replacing n by n^m for m sufficiently large m shows that C can be taken to be 1. Applying φ to the special case $n = a^k - b$ with $0 < b \leq a^k - a^{k-1}$ to conclude that $\varphi(n) \geq C' n^\gamma$ for some constant C' independent of n. Replacing n by n^m for a sufficiently large m shows that C' can be taken to be 1.

Problem 10. For every prime number p and any $0 < \theta < 1$, let $\varphi_{p,\theta}$ be the metric of the field $\mathbb{Q}$ of all rational numbers defined by $\varphi_{p,\theta}\left(p^\ell \frac{m}{n}\right) = \theta^\ell$ for all integers m, n, ℓ with $n \neq 0$ and m, n both indivisible by p. Show that every nontrivial non-Archimedean metric φ of the field $\mathbb{Q}$ of all rational numbers must of the form $\varphi = \varphi_{p,\theta}$ for some prime number p and some $0 < \theta < 1$.

Hint: Choose a prime number p with $\varphi(p) < 1$. Using the existence of $a, b \in \mathbb{Z}$ with $1 = ap^k + bq^\ell$ for any $k, \ell \in \mathbb{N}$ and any prime number $q \neq p$ to show $\varphi(q) = 1$. Apply φ to $p^\ell \frac{m}{n}$.

Problem 11. A norm $\psi(\cdot)$ which makes $\mathbb{Q}$ is a normed vector space over $\mathbb{Q}$ must be of the form $\psi(x) = C|x|$ for some positive constant C. More precisely, if $\psi : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ such that, for $x, y \in \mathbb{Q}$,

(i) $\psi(x) \geq 0$,

(ii) $\psi(x) = 0$ if and only if $x = 0$,

(iii) $\psi(\alpha x) = |\alpha| \, \psi(x)$ for $\alpha \in \mathbb{Q}$,

(iv) $\psi(x + y) \leq \psi(x) + \psi(y)$,

then there exists a positive number C such that $\psi(x) = C|x|$ for $x \in \mathbb{Q}$.

Problem 12. (This problem on metrics is taken from one method developed for the comparison of DNA segments.) Let $\mathcal{A}$ be a finite set of objects which we call an *alphabet* (in practice, the 20-letter amino acid alphabet of proteins). Let $d(a, b)$ be a distance function on $\mathcal{A}$ for $a, b \in \mathcal{A}$ (in practice, the cost of a mutation from a to b). Let $g(a)$ be a positive-valued function on $\mathcal{A}$ for $a \in \mathcal{A}$ (in practice, the positive cost of inserting or deleting the letter a). For two finite sequences $\mathbf{a} = (a_1, a_2, \cdots, a_m)$ and $\mathbf{b} = (b_1, b_2, \cdots, b_n)$, not necessarily of the same length, define $D(\mathbf{a}, \mathbf{b})$ by induction on m and n, as follows.

$$D(\mathbf{a}, \mathbf{b}) = 0 \quad \text{if } m = n = 0,$$

$$D(\mathbf{a}, \mathbf{b}) = \sum_{k=1}^{n} g(b_k) \quad \text{if } m = 0 \text{ and } n > 0,$$

$$D(\mathbf{a}, \mathbf{b}) = \sum_{j=1}^{m} g(a_j) \quad \text{if } m > 0 \text{ and } n = 0,$$

$$D(\mathbf{a}, \mathbf{b}) = \min\left(D(\mathbf{a}', \mathbf{b}) + g(a_m),\ D(\mathbf{a}', \mathbf{b}') + d(a_m, b_n),\ D(\mathbf{a}, \mathbf{b}') + g(b_n)\right)$$
$$\text{if } m > 0 \text{ and } n > 0,$$

where $\mathbf{a}' = (a_1, a_2, \cdots, a_{m-1})$ and $\mathbf{b}' = (b_1, b_2, \cdots, b_{n-1})$. Verify that $D(\cdot, \cdot)$ is a metric on the space of all finite sequences of letters of the alphabet $\mathcal{A}$.

Problem 13. (#7 on p.22 of Rudin's book) Fix $b > 1$, $y > 0$, and prove that there is a unique real x such that $b^x = y$, by completing the following outline. (This x is called the *logarithm of y to the base b*.)

(a) For any positive integer n, $b^n - 1 \geq n(b - 1)$.

(b) Hence $b - 1 \geq n\left(b^{\frac{1}{n}} - 1\right)$.

(c) If $t > 1$ and $n > \frac{b-1}{t-1}$, then $b^{\frac{1}{n}} < t$.

(d) If w is such that $b^w < y$, then $b^{w+\frac{1}{n}} < y$ for sufficiently large n; to see this, apply part (c) with $t = y \cdot b^{-w}$.

(e) If $b^w > y$, then $b^{w-\frac{1}{n}} > y$ for sufficiently large n.

(f) Let A be the set of all w such that $b^w < y$, and show that $x = \sup A$ satisfies $b^x = y$.

(g) Prove that this x is unique.

Problem 14. Let $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$ be complex numbers. Verify the following identity.

$$\left|\sum_{k=1}^{n} a_k \overline{b_k}\right|^2 + \sum_{1 \le j < k \le n} |a_j b_k - a_k b_j|^2 = \left(\sum_{j=1}^{n} |a_j|^2\right)\left(\sum_{k=1}^{n} |b_j|^2\right).$$

Use it to prove Schwarz's inequality

$$\left|\sum_{k=1}^{n} a_k \overline{b_k}\right|^2 \le \left(\sum_{j=1}^{n} |a_j|^2\right)\left(\sum_{k=1}^{n} |b_j|^2\right)$$

and show that Schwarz's inequality becomes an identity precisely when there exist two complex numbers λ and μ not both zero such that $\lambda a_j + \mu b_j = 0$ for $1 \le j \le n$.

For the special case where $n = 2$ or 3 and all a_j, b_j $(1 \le j \le n)$ are real, interpret the identity $(*)$ above in terms of the trigonometric identity

$$\cos^2\theta + \sin^2\theta \equiv 1.$$

Problem 15. Suppose z_1, z_2, z_3 are complex numbers such that

$$|z_1| = |z_2| = |z_3|$$

and

$$z_1 + z_2 + z_3 = 0.$$

Prove that

$$|z_1 - z_2| = |z_2 - z_3| = |z_3 - z_1|.$$

Problem 16. The set $\mathbb{R}$ of real numbers is given the usual Euclidean distance as its metric. Show that a nonempty subset G of $\mathbb{R}$ is open if and only if it is a disjoint (at most countable) union of open intervals. In other words, G is open if and only if there exist $n \in \mathbb{N} \cup \{\infty\}$ and $-\infty \le a_k < b_k \le \infty$ for $0 \le k < n$ such that $G = \cup_{0 \le k < n} (a_k, b_k)$ with (a_k, b_k) and (a_ℓ, b_ℓ) disjoint for $k \ne \ell$.