347H Notes

Alexander Roe

Elementary Set Theory

Theorem. Every function can be written as the sum of one even function and one odd function.

Proof. Consider some function $f : A \to B$. Let $g : A \to B$ be defined as $g(x) = \frac{f(x)+f(-x)}{2}$ and $h : A \to B$ be defined as $h(x) = \frac{f(x)-f(-x)}{2}$. Clearly, $g(x) = g(-x)$, $h(x) = -h(-x)$, and $g(x) + h(x) = \frac{f(x)+f(-x)}{2} + \frac{f(x)-f(-x)}{2} = f(x)$.

Theorem. *Triangle inequality.* For every $x, y \in \mathbb{R}, |x+y| \leq |x| + |y|$.

Proof:

Theorem. *Generalized triangle inequality.*

For $x_1, x_2, ..., x_n \in \mathbb{R}$, $|\sum_{k=1}^{n} x_k| \leq \sum_{k=1}^{n} |x_k|$.

Proof: Induction on n. For the base step, the $n = 1$ case holds trivially, since $x_1 \leq x_1$. Next, assume that $|\sum_{k=1}^{n} x_k| \leq \sum_{k=1}^{n} |x_k|$ holds for some $n > 1$. Then

$$|\sum_{k=1}^{n+1} x_k| = |x_1 + x_2 + ... + x_n + x_{n+1}|$$

By the inductive hypothesis:

$$|x_1 + x_2 + ... + x_n + x_{n+1}| = |x_1 + x_2 + ... + (x_n + x_{n+1})| = |x_1| + |x_2| + ... + |x_n + x_{n+1}|$$

Theorem. *AM-GM inequality.* For every $x, y \in \mathbb{R}$ with $x \geq 0$ amd $y \geq 0$, $\frac{x+y}{2} \geq \sqrt{xy}$.

Proof: Let x and y be two nonnegative real numbers. Then, $0 \leq (x-y)^2 = x^2 - 2xy + y^2$. Adding $4xy$ to both sides gives $4xy \leq x^2 + 2xy + y^2 = (x+y)^2$. Since x and y are both nonnegative, we can take the positive square root of both sides to obtain $2\sqrt{xy} \leq x + y$. This is equivalent to $\frac{x+y}{2} \geq \sqrt{xy}$.

Theorem. *Binomial theorem.* If $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$, then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Theorem. *Multinomial theorem.*

Definition. *Big-O Notation.* Consider a set A, and functions $f : A \to \mathbb{R}$ and $g : A \to (0, \infty)$. We say that $f(x) = O(g(x))$ if there exists some $C > 0$ so that for sufficiently large values of x, $|f(x)| \leq Cg(x)$.

Definition. *Cardinality of finite sets.* The cardinality of a finite set S is the number of elements in S, denoted $|S|$, $card(S)$, or $\#S$.

Definition. *Cardinality of infinite sets.* Consider two infinite sets A and B.

(i) If there exists a bijection between A and B, then $|A| = |B|$.

(ii) If there exists an injection from A to B, then $|A| \leq |B|$.

(iii) If there exists no surjection from A to B, then $|A| < |B|$.

Theorem. *Schröder-Bernstein Theorem.* If there are injective functions $f : A \to B$ and $g : B \to A$ between sets A and B, then there exists a bijection between the sets. Furthermore, this is equivalent to saying if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Proof.

Theorem. *Cantor's Theorem.* For any set S, there exists no surjection $f : S \to \mathcal{P}(S)$. Equivalently, $|S| < \mathcal{P}(S)$.

Proof.

Elementary Number Theory

Theorem. *Bézout's Identity.* Let $a, b \in \mathbb{Z}$ and $gcd(a, b) = g$. Then there exist $x, y \in \mathbb{Z}$ so that $ax + by = g$.

Proof.

Theorem. *Euclid's Lemma.* If $a, b \in \mathbb{Z}$, p is prime, and $p|ab$, then $p|a$ or $p|b$.

Theorem. Every integer $n \geq 2$ can be written as the product of at least one prime.

Proof. Induction on n. Base case: true for $n = 2$. Assume that $n \geq 3$ and every integer from 2 to $n - 1$ can be written as the product of primes. There are two cases:

(i) n is prime. Then n can be written as the product of one prime.

(ii) n is composite. Then $\exists d$ such that $d|n$, and $2 \leq d \leq n - 1$. Define e by $n = de$. Then $e = \frac{n}{d} \geq \frac{n}{n-1} > 1$, so $e \geq 2$. Also, $e = \frac{n}{d} \leq \frac{n}{2} \leq n - 1$. By the inductive hypothesis, both d and e can be written as the product of primes. Therefore, n can be written as the product of primes.

Theorem. *Fundamental Theorem of Arithmetic.* Every integer $n \geq 2$ has a unique prime factorization.

Proof.

Theorem. There are infinitely many primes.

Proof. Suppose there are only finitely many primes, enumerated $p_1, p_2, ..., p_n$. Consider $a = p_1 p_2 ... p_n + 1$. By the Fundamental Theorem of Arithmetic, there exists a prime q that divides a. Since $q|a$ and $q|p_1 p_2 ... p_n$, this implies $q|(a - p_1 p_2 ... p_n)$, or $q|1$. This is a contradiction; hence, there are infinitely many primes.

Theorem. Every composite number $n \geq 4$ has a prime factor $p \leq \sqrt{n}$.

Proof. Let n be composite. Then $\exists a, b \in \mathbb{Z}$ such that $a \geq 2$, $b \geq 2$, and $n = ab$. By the Fundamental Theorem of Arithmetic, a and b are the product of primes. But $min(r, s) \leq \sqrt{n}$, so one of a and b has a prime factor less than $\sqrt{n}$. Therefore, n must have at least one prime factor less than $\sqrt{n}$.

Corollary. For every $n \in \mathbb{N}$, if n has no prime factor $p \leq \sqrt{n}$, then n is prime.

Theorem. *Rational Root Theorem.* Let $f(x) = \sum_{i=0}^{n} c_i x^i$, where $c_i \in \mathbb{Z} \forall i$, $c_o \neq 0$, $c_n \neq 0$. Suppose $f(r) = 0$ where $r = \frac{p}{q}$ with $gcd(p, q) = 1$. Then $p|c_0$ and $q|c_n$.

Proof.

Elementary Abstract Algebra

Definition. *Monoids and groups.* A monoid is a set S together with a binary operation $\cdot$ such that the following hold:

- *Associativity.* $\forall x, y, z \in S$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- *Identity element.* $\exists e \in S$ so that $\forall x \in S$, $e \cdot x = x \cdot e = x$.

In addition, if the following hold:

- *Closure.* $\forall x, y \in S$, $x \cdot y \in S$.
- *Inverse element.* $\forall x \in S$, $\exists x^{-1}$ so that $x \cdot x^{-1} = e$.

Then $(S, \cdot)$ is a group.

In addition, if the following holds:

- *Commutativity.* $\forall x, y \in S$, $x \cdot y = y \cdot x$.

Then $(S, \cdot)$ is an abelian group.

Definition. *Rings and fields.* A ring is a set S together with binary operations $+$ and $\cdot$ such that the following hold:

- *Additive associativity.* $\forall x, y, z \in S$, $(x + y) + z = x + (y + z)$.
- *Additive commutativity.* $\forall x, y \in S$, $x + y = y + x$.
- *Additive identity element.* There exists an element 0 in S such that $\forall x \in S$, $x + 0 = 0 + x = x$.
- *Additive inverse element.* $\forall x \in S$, $\exists - x \in S$ such that $x + -x = 0$, where 0 is the additive identity element.
- *Multiplicative associativity.* $\forall x, y, z \in S$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- *Multiplicative identity element.* There exists an element 1 in S such that $\forall x \in S$, $x \cdot 1 = 1 \cdot x = x$.
- *Distributivity.* $\forall x, y, z \in S$, $x \cdot (y + z) = x \cdot y + x \cdot z$, and $(y + z) \cdot x = y \cdot x + z \cdot x$.

That is, $(S, +, \cdot)$ is an abelian group under addition and a monoid under multiplication.

In addition, if the following holds:

- *Multiplicative commutativity.* $\forall x, y \in S$, $x \cdot y = y \cdot x$.

Then $(S, +, \cdot)$ is a commutative ring.

In addition, if the following holds:

- *Multiplicative inverse element.* $\forall x \in S$ with $x \neq 0$, $\exists x^{-1} \in S$ such that $x \cdot x^{-1} = 1$, where 1 is the multiplicative identity element.

Then $(S, +, \cdot)$ is a field.

Theorem. *Lagrange's Theorem.*

Theorem. *Lagrange's Theorem.* Let S be a finite set, and let $(S, +, \cdot)$ be a commutative ring. Let $T =$. Then, for every $x \in T$, $x^{|T|} = 1$.

Proof. Let $T = t_1, t_2, ..., t_k$. For any $x \in T$, let $U = xt_1, xt_2, ..., xt_n$.

Theorem. *Cancellation law of modular arithmetic.* If $ax \equiv ay \pmod{n}$ and $gcd(a, n) = 1$, then $x \equiv y \pmod{n}$.

Proof. Suppose $ax \equiv ay \pmod{n}$ and $gcd(a, n) = 1$. It follows that $n|(ax - ay) \Leftrightarrow n|(a(x - y))$. Since a and n are relatively prime, n must divide $x - y$. Thus, $x \equiv y \pmod{n}$.

Theorem. *Euler's Theorem.* If a and n are relatively prime integers, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Let $gcd(a, n) = 1$, and $S = s_1, s_2, ..., s_{\phi(n)}$, where all the elements of S make up a reduced residue system modulo n (i.e. $gcd(s_i, n) = 1 \; \forall i$). Consider $a \cdot S = as_1, as_2, ..., as_{\phi(n)}$. We claim that $a \cdot S$ is a permutation of S. Suppose $as_i \equiv as_j \pmod{n}$ for some i, j with $i \neq j$. Then, by the cancellation law, $s_i \equiv s_j \pmod{n}$. Hence, multiplication by any integer relatively prime to n permutes the set S. It follows that

$$\prod_{i=1}^{\phi(n)} as_i \equiv \prod_{i=1}^{\phi(n)} s_i \pmod{n}$$

which is equivalent to

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} s_i \equiv \prod_{i=1}^{\phi(n)} s_i \pmod{n}.$$

Since $gcd(s_i, n) = 1 \; \forall i$, by the cancellation law, we have

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

This concludes the proof.

Theorem. *Fermat's Little Theorem.* If $a \in \mathbb{Z}$ and p is prime, then $a^p \equiv a \pmod{p}$. Equivalently, if p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Let p be prime and $S = 1, ..., p - 1$ (one element from each congruence class modulo p). Consider some integer a such that $p \nmid a$. Consider the following set:

$$a \cdot S = a, 2a, ..., (p - 1)a \pmod{p}$$

If $xa \equiv ya \pmod{p}$, then $x \equiv y \pmod{p}$ by the cancellation law. Thus, multiplying by a permutes the set S. It follows that

$$a \cdot 2a \cdots (p - 1)a \equiv 1 \cdot 2 \cdots (p - 1) \pmod{p}$$

By the cancellation law, we have

$$a^{p-1} \equiv 1 \pmod{p}$$

This concludes the proof.

Theorem. *Wilson's Theorem.* If p is prime, then $(p - 1)! \equiv -1 \pmod{p}$.

Proof. Let p be prime. Since $\mathbb{Z}_p$ is a field, every element $\in 1, 2, ..., p - 1$ has a multiplicative inverse. Suppose some element $a \in 1, 2, ..., p - 1$ is its own inverse. Then, $a^2 \equiv 1 \pmod{p}$. It follows that p must divide $(a + 1)$ or $(a - 1)$. The only possible solutions for a are $a = 1$ or $a = p - 1$. Therefore, the rest of the elements $2, 3, ..., p - 2$ can be grouped into inverse pairs. So we have

$(p-1)! \equiv 1 \cdot (2 \cdots (p-2)) \cdot (p-1) \pmod{p} \;\Leftrightarrow (p-1)! \equiv 1 \cdot (1 \cdots 1) \cdot -1 \pmod{p}$ $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$.

This concludes the proof.

Theorem. If $\mathbb{Z}_n$ is a field, then n is prime.

Proof. Suppose $\mathbb{Z}_n$ is a field and n is composite. Then we can write $n = pq$, where p and q are integers that are at least 2. Since $\mathbb{Z}_n$ is a field, there exists some $a \in \mathbb{Z}_n$ so that $ap \equiv 1 \pmod{n}$. Then

$q \equiv 1 \cdot q \equiv (ap) \cdot q \equiv a(pq) \equiv an \equiv 0 \pmod{n}$.

This is a contradiction, since $q \not\equiv 0 \pmod{n}$. Hence, n is prime.

Theorem. Let m and n be relatively prime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.

Proof.

Theorem. *Chinese Remainder Theorem.*

Proof.

Corollary. If $n = {p_1}^{e_1} ... {p_k}^{e_k}$ then $\phi(n) = p_1 - 1^{e_1 - 1} ... p_k - 1^{e_k - 1}$.

Proof.

Definition. *Carmichael Numbers.*

Theorem. *Korselt's Criterion.*

Proof.

Elementary Real Analysis

Axiom. *The completeness axiom for* $\mathbb{R}$. Every subset of $\mathbb{R}$ that has an upper bound has a supremum. Equivalently, every subset of $\mathbb{R}$ that has a lower bound has an infimum.

Definition. *Sequences.* A sequence is any function $f : \mathbb{N} \to \mathbb{R}$.

Definition. *Limit.* A sequence (a_n) has a limit L if for every $\epsilon > 0$, there exists some $N \in \mathbb{N}$ so that for every $n \geq N$, $|a_n - L| < \epsilon$.

Theorem. A sequence cannot have more than one limit.

Proof. Suppose $\lim\limits_{n \to \infty} a_n = L$ and $\lim\limits_{n \to \infty} a_n = M$, with $L \neq M$. By definition of limit, for every $\epsilon > 0$, there exists some $N \in \mathbb{N}$ so that for every $n \geq N$, $L - \epsilon < a_n < L + \epsilon$, and there exists some $K \in \mathbb{N}$ so that for every $n \geq K$, $M - \epsilon < a_n < M + \epsilon$. Without loss of generality, suppose $L < M$, and take $\epsilon = \frac{L-M}{3}$. Then $a_n < L + \epsilon < M - \epsilon < a_n$, which is a contradiction. Hence, a sequence cannot have more than one limit.

Theorem. Given any set S such that sup$S$ exists, there exists a sequence (a_n) with $a_n \in S \forall n \in \mathbb{N}$ and $\lim\limits_{n \to \infty} a_n =supS$.

Proof.

Theorem. $\mathbb{Q}$ is dense in $\mathbb{R}$.

Proof.

Theorem. *Monotone Convergence Theorem.* Every bounded, eventually monotone sequence converges.

Proof.

Theorem. e is irrational.

Proof. Recall the Taylor series $e^x = \sum\limits_{n=0}^{\infty} \dfrac{x^n}{n!}$. Then $e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + ...$ Suppose e is rational. Then, $\exists a, b \in \mathbb{Z}$ with $b \neq 0$. Then $b!e = a(b-1)! \in \mathbb{Z}$. It follows that

$$b!e = b!\left(\tfrac{1}{0!} + \tfrac{1}{1!} + ... + \tfrac{1}{b!}\right) + b!\left(\tfrac{1}{(b+1)!} + \tfrac{1}{(b+2)!} + ...\right) = (b! + b! + ... + 1) + b!\left(\tfrac{1}{(b+1)!} + \tfrac{1}{(b+2)!} + ...\right)$$

Since $b!e \in \mathbb{Z}$, and the integers are closed under addition, we must have $b!(\frac{1}{(b+1)!} + \frac{1}{(b+2)!} + ...) \in \mathbb{Z}$. But

$$b!\left(\tfrac{1}{(b+1)!} + \tfrac{1}{(b+2)!} + ...\right) = \tfrac{1}{b+1} + \tfrac{1}{(b+1)(b+2)} + ... < \tfrac{1}{(b+1)^1} + \tfrac{1}{(b+1)^2} ... = \tfrac{1}{b} < 1.$$

This is a contradiction; hence, e is irrational.

Computability Theory

Definition. *Computable sets.* A set $S \in \mathbb{N}$ is computable if there exists a finite-length algorithm that represents the following function:

$$f(x) = \begin{cases} 0 & \text{if } x \notin S \\ 1 & \text{if } x \in S \end{cases}$$

Cauchy Sequences.

Definition. A sequence (a_n) is Cauchy if $\forall \epsilon > 0$, $\exists N \in \mathbb{N}$ so that $\forall n \geq m \geq N$, $|a_n - a_m| < \epsilon$.

Theorem. Every convergent sequence is Cauchy.

Proof. Suppose $\lim a_n = L$. Then $\forall \epsilon > 0, \exists N \in \mathbb{N}$ so that $\forall n \geq N$, $|a_n - L| < \frac{\epsilon}{2}$. Then for all $n \geq m \geq N$, $|a_n - a_m| < \epsilon$. So (a_n) is Cauchy.