n. quotient (of two non-zero integers)

n. remainder (of two non-zero integers)

definition. a divides b means that a is a factor of b, so $b = ak$ for some integer k.

v. divides (one non-zero integer of another)

definition. The greatest common divisor $\gcd(a,b)$ of two non-zero integers a, b is a positive integer d such that

(i) d divides a and d divides b

(ii) If d' divides a and d' divides b, then d' divides d

n. greatest common divisor (of two non-zero integers)

n. least common multiple (of two integers)

elementary number theory

(1) theorem (division). If a and b are integers with $a>0$, then there are integers q (the quotient of b/a) and r (the remainder) with $0 \le r < a$ and

$$b = aq + r$$

Also, q and r are unique (only one choice works; the quotient and remainder are well-defined).

(2) theorem (gcd). If a and b are non-zero integers, their greatest common divisor $d = \gcd(a,b)$ exists. That is, there is a unique positive integer d such that

(i) d divides a and d divides b ($d|a$ and $d|b$)

(ii) any other common divisor d' of a and b divides d (that is, $d'|a$ and $d'|b \Rightarrow d'|d$).

(3) corollary. $\gcd(a,b)$ is in fact the largest common divisor of a and of b

(4) theorem. If a and b are non-zero integers, the set of all linear combinations of a and b with integer coefficients,

$$\{sa+tb \mid s,t \text{ are integers}\}$$

has a smallest positive element, and this number is $\gcd(a,b)$.

(5) corollary. There exist integers s,t such that $sa+tb = \gcd(a,b)$.

definition. The m-congruence class of an integer x is the set of all additions and subtractions of m from x:

$$[x]_m = \{x, x+m, x+2m, \ldots, x-m, x-2m, \ldots\}$$

n. m-congruence class (of an integer)

adj. congruent mod m, congruent with modulus m, (of a pair of integers)

definition. Two integers a and b are called congruent mod m if $[a]_m$ is equal to $[b]_m$, or equivalently if $[a-b]_m = [0]_m$.

n. greatest common divisor (of a positive integer m and an m-congruence class)

⑥ lemma. If q is the quotient and r is the remainder of b over a, then $\gcd(b,a) = \gcd(a,r)$.

⑦ lemma. If $x \pm y = aq$ (so a divides $x \pm y$), then $\gcd(x,a) = \gcd(y,a)$

⑧ lemma. If $x \equiv y \bmod a$, then $\gcd(x,a) = \gcd(y,a)$. That is, the greatest common divisor of a and an a-congruence class $[x]$ is well-defined.

⑨ theorem (Euclidean algorithm). Suppose a and b are positive integers.

(1) The sequence of remainders $r_0 = b, r_1 = a, r_2, r_3, \ldots,$ with r_i obtained from r_{i-2} and r_{i-1} by division (except r_0 and r_1, which are given), eventually stops, when $r_{n+1} = 0$, since division by 0 is not allowed.

By construction, the division theorem says that

$$b = aq_1 + r_2 \qquad (0 < r_2 < a)$$
$$a = r_2 q_2 + r_3 \qquad (0 < r_3 < r_2)$$
$$r_2 = r_3 q_3 + r_4 \qquad (0 < r_4 < r_3)$$
$$\vdots$$
$$r_{n-1} = r_n q_n$$

(2) $\gcd(a,b) = r_n$.

n. greatest common divisor
(of several non-zero integers)

(10) theorem (expressing gcd as linear combination). The equations obtained by the Euclidean algorithm can be expressed as a matrix equation:

$$\begin{bmatrix} 1 & -q_1 & -1 & & & \\ & 1 & -q_2 & -1 & & \\ & & \ddots & \ddots & & \\ & & & 1 & -q_{n-1} & -1 \\ & & & & 1 & -q_n \end{bmatrix} \begin{bmatrix} b \\ a \\ r_2 \\ \vdots \\ r_{n-1} \\ \gcd(a,b) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Row operations, in which multiples of other rows are added or subtracted from the last row, can be performed to acheive the following sequence of forms for the last row:

$0\ 0\ 0 \ldots * * -1$,

$0\ 0\ 0 \ldots * * 0 -1$,

$\vdots$

$0\ *\ *\ 0 \cdots\ 0 -1$,

$*\ *\ 0 \cdots\ 0 -1$.

Then the last equation reads $sa + tb = \gcd(a,b)$.

(11) theorem. If $a_1, a_2, \ldots, a_n$ are non-zero integers, their greatest common divisor exists. That is, there is a unique positive integer $d = \gcd(a_1, a_2, \ldots)$ such that

(i) d divides each a_i (d is a common divisor)

(ii) any other common divisor divides d.

Also, it can be computed inductively by $\gcd(a_1, \ldots, a_n) = \gcd[a_1, \gcd(a_2, \ldots, a_n)]$

In particular, $\gcd(a,b,c) = \gcd(\gcd(a,b), c)$.

adj. relatively prime, coprime
(of a pair of integers)

<u>definition</u>. An integer is called prime if it is greater than 1 and its only positive divisors are 1 and itself.

adj. prime (of an integer)

n. p-part
p-primary part
(of an integer)

(12) theorem. Suppose a, b, and c are non-zero integers, and a and b are relatively prime ($\gcd(a,b)=1$).

Then "no part of a can divide b" in the sense that

(1) If $a \mid bc$, then $a \mid c$.

Also, "a and b can only divide c in different places" in the sense that

(2) If $a \mid c$ and $b \mid c$, then $ab \mid c$.

(13) theorem. If p is a prime (its only divisors are 1 and p) and p divides ab, then p divides a or p divides b. Also, if p has this property, then p is prime.

(14) theorem. If p is prime and p divides $a_1 a_2 \cdots a_r$, then p divides at least one of the $a_1, a_2, \ldots$.

(15) theorem. Every positive integer n is a product of powers of distinct primes, $n = (p_1)^{k_1} (p_2)^{k_2} \cdots (p_r)^{k_r}$. The set $\{p_1, p_2, \ldots, p_r\}$ of prime factors is unique, and the multiplicity or exponent k of a prime p is also unique. (unique factorization)

(16) theorem. No finite set of primes contains all primes; the set of primes is infinite.

(17) theorem. The prime factorization of $\gcd(a,b)$ has one factor p^k for each prime factor p of both a and b, where k is the smaller of the two exponents with which p appears in a and in b.

definition. A relation $R \subset X \times X$ is called
reflexive if $(x,x) \in R$ for all $x \in X$,
symmetric if $(x,y) \in R \Leftrightarrow (y,x) \in R$ for
all $x, y \in X$, and
transitive if $(x,y) \in R$ and $(y,z) \in R$
$\Rightarrow (x,z) \in R$.

definition. An equivalence relation is
a relation $R \subset X \times X$ that is
reflexive, symmetric, and transitive.

n. relation
adj. reflexive (of a relation)
adj. symmetric (of a relation)
adj. transitive (of a relation)
n. equivalence relation
n. equivalence class
adj. equivalent (of a pair)

n. function
map
mapping
(from one set to another)
n. domain (of a function)
n. image, codomain
(of a function)
adj. one-to-one, injective (of a function)
adj. onto, surjective (of a function)
adj. bijective (of a function)
n. composition (of two functions)

(18) **theorem** (inclusion-exclusion). If X and Y are finite sets,

$$|X| + |Y| = |X \cup Y| + |X \cap Y|$$

(19) **proposition** (equivalence relations). A relation $R \subset X \times X$ that is an equivalence relation (i.e., that is symmetric, reflexive, and transitive) is the same as

(1) A function $f: X \times X \to \{0,1\}$ such that

$$f(a,b) = f(b,a), \quad f(a,a) = 1, \quad f(a,b) = f(b,c) = 1 \Rightarrow f(a,c) = 1$$

(for the statement $f(a,b) = 1$ we will write $a \sim b$ or "a is equivalent to b").

(2) A partition of X.

(20) **proposition**. For a given positive integer m, the relation

$a \sim b$ if and only if $a - b = mq$ for some integer q

is an equivalence relation. In this case the statement $a \sim b$ will be written as

$$a \equiv b \bmod m, \text{ or}$$

$$a \equiv_m b.$$

There are m equivalence classes, $[0], [1], \ldots, [m-1]$. (The class represented by an integer a is written $[a]$ or $[a]_m$.) The set of equivalence classes is denoted $\mathbb{Z}_m$.

n. congruence class mod m

adj. congruent mod m (of a pair of integers)

n. sum (of two congruence classes)

n. product (of two congruence classes)

adj. invertible (of a congruence class)

n. inverse (of a congruence class)

adj. closed (of a set with respect to an operation)

definition. A congruence class $[a]_m$ is called invertible if there is a congruence class $[b]_m$ such that

$$[ab]_m = [1]_m.$$

$[b]_m$ is then called the inverse of $[a]_m$.

definition. An operation $\cdot : X \times X \to X$ is called closed on a subset $A \subset X$ if all of the $(a \cdot b)$ belong to A, for $a, b \in A$.

(21) proposition. The addition and multiplication of the integers $\mathbb{Z}$ induces well-defined operations, also called addition and multiplication, on the classes $\mathbb{Z}_m$. That is, if $[a]=[b]$ and $[c]=[d]$, then

(1) $[a+c]=[b+d]$

(2) $[ac]=[bd]$

The class appearing in (1) is written $[a]+[c]$, or just $x+y$ where $x=[a]=[b]$ and $y=[c]=[d]$.
The class appearing in (2) is written $[a]\cdot[c]$, or just $x\cdot y$.

(22) theorem (inverses of congruence classes). A class $x=[a]_m$ has a multiplicative inverse (that is, there is some $y\in\mathbb{Z}_m$ such that $x\cdot y=[1]_m$) if and only if $\gcd(m,x)=\gcd(m,a)=1$.
Actually, if $sm+ta=1$, the inverse x^{-1} is $[t]_m$.

(23) corollary (cancellation law). If $ac\equiv bc \bmod m$ and $\gcd(c,m)=1$ (that is, $[c]_m$ is invertible), then $a\equiv b \bmod m$.

(24) corollary All non-zero classes belonging to $\mathbb{Z}_p$, where p is prime, are invertible. This set is denoted $\mathbb{Z}_p^*$.

(25) proposition The set $\mathbb{Z}_m^*$ of invertible elements of $\mathbb{Z}_m$ is closed under multiplication.

n. linear congruence

definition. Two integers m, n are called relatively prime if $\gcd(m,n) = 1$.

(26) theorem (solutions of linear congruences). The equation

$$aX \equiv b \mod m$$

$$[a]_m \cdot x = [b]_m$$

has solutions if and only if $\gcd(a,m) \mid b$. In this case there are $\gcd(a,m)$ solutions, all congruent modulo $m/\gcd(a,m)$. This solution (as a class mod $m/\gcd(a,m)$) is $[a/d]^{-1}_{m/d} \cdot [b/d]_{m/d}$ (where $d = \gcd(a,m)$)

(27) theorem (Chinese remainder theorem). If m and n are relatively prime ($\gcd(m,n) = 1$), then every system

$$x \equiv a \mod m$$

$$x \equiv b \mod n$$

has a unique solution mod mn. It is given by

$$x = bsm + atn$$

where s and t are integers such that $sm + tn = 1$.

(28) theorem. If $m_1, m_2, \ldots, m_r$ are pairwise relatively prime (each $\gcd(m_i, m_j) = 1$), every system of r congruences

$$x \equiv a_1 \mod m_1$$

$$\vdots$$

$$x \equiv a_r \mod m_r$$

can be reduced to a system of $r-1$ congruences by the Chinese remainder theorem, applied to any pair of equations.

n. group

n. identity, neutral element (of a group)

n. ring

adj. commutative

adj. cyclic

n. order (of an element of a group or ring)

<u>definition</u> If k is the smallest positive integer such that

$$\underbrace{[a]_m \cdot [a]_m \cdot \cdots \cdot [a]_m}_{k \text{ times}} = [1]_m,$$

then $[a]_m$ is said to have order k.

(29) proposition. $\mathbb{Z}_m$ forms a group under addition (in fact, a commutative group generated by one element, $[1]_m$ (which is not the identity element), also called cyclic.)

$\mathbb{Z}_m$ forms a ring under addition and multiplication. The set $\mathbb{Z}_m^*$ of invertible elements forms a group under multiplication

(30) theorem. There exists a positive integer k such that $[a^k]_m = [1]_m$ (i.e., $[a]_m$ has finite multiplicative order) if and only if $\gcd(a,m) = 1$.

(31) theorem If $[a]_m$ has order k, then

$$[a]_m^r = [a]_m^s \text{ if and only if } r \equiv s \bmod k$$

(32) theorem (Fermat). If $[a]_p \in \mathbb{Z}_p^*$, so a is not divisible by p, (p is prime), then $[a]_p^{p-1} = [1]_p$. This implies $a^p \equiv a \bmod p$.

(33) corollary. If p is prime, the order of any non-zero $[a]_p$ divides $p-1$

(34) theorem. Let $\varphi(m) = |\mathbb{Z}_m^*|$, the number of invertible m-congruence classes, the number of integers from 0 to $m-1$ relatively prime to m. Then

(1) If p is prime, $\varphi(p^n) = p^n - p^{n-1}$ (for any positive integer n)

(2) If $\gcd(a,b) = 1$, $\varphi(ab) = \varphi(a)\varphi(b)$

(3) (Euler) If $[a]_m \in \mathbb{Z}_m^*$, so $\gcd(a,m) = 1$,

$$[a]_m^{\varphi(m)} = [1]_m$$

That is, the order of any $x \in \mathbb{Z}_m^*$ is at most $\varphi(m)$. In fact, it divides $\varphi(m)$.

definition. A transformation of a set X is a bijection $X \to X$ (a one-to-one and onto function, an invertible function, a correspondence)

n. transformation

definition. The symmetric group on n elements, S_n, is the set of all bijections from the set $\{1, 2, \ldots, n\}$ to itself.

n. transformation group

definition. The automorphism group of the cube, $\mathrm{Aut}(\square)$, is the set of all rigid motions of Euclidean 3-space that send the points of a fixed cube to itself.

n. group

definition. The Euclidean isometry group, $\mathrm{Isom}(E^2)$, is the set of all rigid motions of the plane.

definition. The Möbius group, $PSL_2\mathbb{C}$, is the set of all holomorphic (conformal) bijections of the Riemann sphere to itself $\mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$.

definition. The general linear group, $GL_n\mathbb{R}$, is the set of all invertible linear maps $\mathbb{R}^n \to \mathbb{R}^n$.

groups and symmetry

(35) **proposition.** Let X be a set.

(1) The identity function $id: X \to X$ is a transformation.

(2) The composition $f \circ g$ of two transformations $f, g: X \to X$ is a transformation.

(3) The inverse f^{-1} of a transformation f is a transformation.

(36) **proposition.** S_n, $Aut(\square)$, $Isom(E^2)$, $PSL_2\mathbb{C}$, $GL_n\mathbb{R}$, and $Diff(M)$ are transformation groups. That is, each is a set G of transformations of a fixed set X such that:

(i) G contains the identity transformation

(ii) For every pair $f, g \in G$, G contains $f \circ g$.

(iii) For every $f \in G$, G contains f^{-1}.

(37) **proposition** Every transformation group is a group. That is, a set G with an operation $G \times G \to G$ (called the group multiplication or addition, denoted $\cdot$ or $+$) and an element $e \in G$ (called the neutral element, the identity, 1, or 0) such that:

(i) $e \cdot g = g$ and $g \cdot e = g$ for all $g \in G$

(ii) For each $g \in G$ there is a $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$

(iii) $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ for all $g, h, k \in G$

definition. A subgroup of a group G is a subset $H \subset G$ which is also a group with respect to the multiplication and inversion in G. That is, a subset $H \subset G$ such that:

(i) $h \cdot k \in H$ for all $h, k \in H$

(ii) $h^{-1} \in H$ for all $h \in H$

definition. Two groups G and H are called isomorphic if there is a correspondence $G \to H$ (one-to-one and onto) compatible with the multiplication. That is,

if $g_1 \mapsto h_1$ and $g_2 \mapsto h_2$, then $g_1 \cdot g_2 \mapsto h_1 \cdot h_2$.

Such a correspondence is called an isomorphism.

(38) proposition. The set of all subsets of $\{1,2,\dots,n\}$,
the set of all subsets of the Euclidean plane E^2,
the set of positive definite quadratic forms on $\mathbb{R}^3$,
the set of complex structures on a surface Σ,
the set of vector space structures on an affine space,
the set of all functions $X \to Y$, and
the set of all operations $X \times X \to X$

are all sets of structures built on a set X. That is, each is a set $P(X)$ ("all structures of type P"), together with a rule $f_*: P(X) \to P(X)$ for each (allowable) transformation $f: X \to X$, such that:

(i) $id_*(S) = S$ for all $S \in P(X)$

(ii) $(f \circ g)_*(S) = f_*(g_*(S))$ for all $S \in P(X)$ and (allowable) f, g

(f_*S is called the induced structure. Sometimes all transformations are allowable; sometimes only linear maps, continuous maps, etc.)

(39) proposition. The set of all transformations preserving a structure $S \in P(X)$ (i.e., automorphisms, those $f: X \to X$ with $f_*S = S$) is a transformation group, denoted $Aut(S, X)$, or $Aut(X)$ if S is implicit.

(40) proposition. Every finite group is isomorphic to a subgroup of a permutation group S_n.

the Euclidean plane E^2

(41) proposition (classification of isometries). Every rigid motion of the plane E^2 is either:
(1) The identity $id: E^2 \to E^2$,
(2) A rotation R about some fixed point $p \in E^2$,
(3) A reflection r across some line ℓ, or
(4) A pure translation T.

(42) proposition. Let $f \in Isom(E^2)$ be a rigid motion.
(1) If R is a rotation about p, fRf^{-1} is a rotation about $f(p)$ through the same angle.
(2) If r is a reflection across ℓ, frf^{-1} is a reflection across $f(\ell)$.
(3) If T is a translation sending p to q, fTf^{-1} is a translation sending $f(p)$ to $f(q)$.

(43) proposition. If ℓ and ℓ' meet at p with angle θ and r and r' are the reflections across ℓ and ℓ', then rr' is a rotation through angle 2θ about p.

(44) theorem (crystallographic groups). There are exactly 17 finitely-generated (but not finite) groups arising as symmetry groups $Aut(S)$ of ornaments $S \subset E^2$.

definition. The order $|\sigma|$ of a permutation $\sigma \in S_n$ is the smallest positive integer k such that $\sigma^k = 1$.

the symmetric groups

(45) proposition. Each ordered r-tuple $(a_1, a_2, \ldots, a_r)$ of numbers belonging to $\{1, 2, \ldots, n\}$ corresponds to a unique permutation $\sigma \in S_n$ such that:

$$\sigma(a_i) = a_{i+1} \quad \text{if } i < r$$

$$\sigma(a_r) = a_1$$

$$\sigma(a) = a \quad \text{if } a \neq \text{any } a_i$$

This permutation is called an r-cycle, and it is denoted $(a_1 a_2 \cdots a_r)$.

(46) proposition. Every permutation $\sigma \in S_n$ is a product of disjoint r-cycles (each number $1, 2, \ldots, n$ belongs to exactly one cycle), and the set $\{r\}$ of lengths, with multiplicities, is unique. The set $\{\sigma_i\}$ of cycles is also unique, and their product in any order equals σ.

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \sigma_k$$

(47) proposition. The order $|\sigma|$ of a permutation σ is the least common multiple of the lengths of its cycles:

$$|\sigma| = \text{lcm}(r_i)$$

(48) proposition. If $\sigma \in S_n$ has order k, then

$$\sigma^r = \sigma^s \text{ if and only if } r \equiv s \bmod k$$

(49) theorem. Every $\sigma \in S_n$ is product of (usually not disjoint) transpositions, cycles of length 2.

definition. Conjugacy in a group G is the relation

$a \sim b$ if and only if for some g, $a = gbg^{-1}$

$(a, b, g \in G)$. It is an equivalence relation on G.
Its classes are called conjugacy classes.

(50) theorem. For every $\sigma, \tau \in S_n$, the cycle decomposition of $\sigma\tau\sigma^{-1}$ is exactly the same as that of τ except that each entry a_i of a cycle is replaced with $\tau(a_i)$.

(51) corollary. There is one conjugacy class in S_n for each cycle type (that is, for each additive partition of n).

Cosets, orbits, actions

(52) proposition If $H \subset G$ is a subgroup, the relation on G

$$a \sim b \text{ if and only if } a = b \cdot h \text{ for some } h \in H$$

is an equivalence relation. The classes are called cosets. The class represented by a is denoted aH, and it is also equal to $a \cdot H = \{a \cdot h \mid h \in H\}$.
(Note that in additive notation this looks different; the class of a is $a + H$.)

(53) proposition. Let $m \cdot \mathbb{Z}$ be the additive subgroup of $\mathbb{Z}$ consisting of all multiples of m. Then the cosets of $m\mathbb{Z}$ are the congruence classes mod m:

$$a + m\mathbb{Z} = [a]_m$$

The function $\varphi: \mathbb{Z} \to \mathbb{Z}_m$, $\varphi(a) = a + m\mathbb{Z}$, is a surjective homomorphism of groups. (When viewed as a set of cosets, $\mathbb{Z}_m$ is usually denoted $\mathbb{Z}/m\mathbb{Z}$.)

(54) theorem (Lagrange). If $H \subset G$ is a subgroup of a finite group, each coset of H has size $|H|$, and

(the number of H-cosets) $\cdot\, |H| = |G|$

(55) corollary. The order of an element divides the order of the group. If $g \in G$, $|g|$ divides $|G|$.

(56) proposition. (1) The permutations of the variables x, y, z induces an action of the group S_3 on the vector space of polynomials in three variables.

(2) The effect of the symmetries of the cube  on the vertices is an action of the group $\mathrm{Aut}(\square)$ on the set of 8 vertices.

(3) The effect of applying an isomorphism $K \to K$ of the field generated by the roots of a polynomial $p \in \mathbb{C}[x]$ induces an action of $\mathrm{Aut}(K)$ on the set of roots of p.

(4) The defining action of $\mathrm{Isom}(E^2)$ on E^2 induces an action of $\mathrm{Isom}(E^2)$ on the set of lines $\ell \subset E^2$.

(5) The conjugation of elements of G by various $g \in G$ (so $a \mapsto gag^{-1}$) is an action of $G = \{g\}$ on the set of its elements.

(57) theorem. (1) The orbits of an action of a group G on a set X form a partition of X. (Each $x \in X$ belongs to exactly one orbit.)

(2) If x and y belong to the same orbit of an action of G, their stabilizers are isomorphic and have the same size:

$$|G_x| = |G_y|$$

(3) If $O(x)$ is the orbit of $x \in X$ under the action of G, and G_x is the stabilizer of x (those $g \in G$ such that $g(x) = x$), then

$$|O(x)| \cdot |G_x| = |G|$$

(58) theorem (Burnside). If G acts on X and X^g denotes the fixed set of $g \in G$, those $x \in X$ with $g(x) = x$, then

$$(\text{the number of orbits}) = \frac{1}{|G|} \cdot \sum_{g \in G} |X^g|$$

applications

RSA public key encryption

(59) **theorem.** Suppose you hold a "private key" consisting of:

- two large primes p and q
- a large number a, invertible mod $(p-1)(q-1)$, and its inverse b

The "public key" is just the data:

- the product $n = pq$
- the number a

If a number m is a message encoded using the public key, so

$$m \equiv c^a \bmod n$$

for some secret number c (much less than p or q), then anyone in possession of the private key (or even just the primes p, q or just b) can decode the message; can recover c:

$$c \equiv m^b \bmod n$$

binary error-detecting and error-correcting codes

(60) theorem. Let $f: B^m \to B^n$ be any binary coding function (a one-to-one map, a way of encoding m-bit numbers as n-bit numbers, $n>m$). Let $W = \text{Image}(f)$ be the set of codewords. Let d be the minimum distance (in number of bits) between 2 codewords. (different)

(1) If $u \in W$ is a codeword and $e \in B^n$ has weight $d-1$ or less (the number of 1s is $d-1$ or less), then

$$u+e \notin W,$$

$u+e$ is not a codeword.

That is, fewer than d errors in the bits of a transmitted codeword can always be detected.

(2) If $u, v \in W$ and if $e, e' \in B^n$ have weights less than or equal to k, then

$$u+e = v+e' \Rightarrow d \leq 2k \quad \text{(provided } u \neq v\text{)}$$

The contrapositive holds: if k is such that $d \geq 2k+1$, then two different codewords altered each with k or fewer errors will always be different transmitted codes; k or fewer errors can be corrected.

(61) theorem. If $f: B^m \to B^n$ is a linear code (that is, a linear map of vector spaces, a homomorphism of groups, so it is given by a matrix), then the minimum distance d between different codewords is the smallest non-zero weight of a codeword $u \in W$.

(62) **proposition.** Given any linear code $f: B^m \to B^n$, you can choose m of the entries, to get an isomorphism $B^n \cong B^m \times B^{n-m}$, in such a way that the image subspace of codewords is the graph of a linear map $L: B^m \to B^{n-m}$:

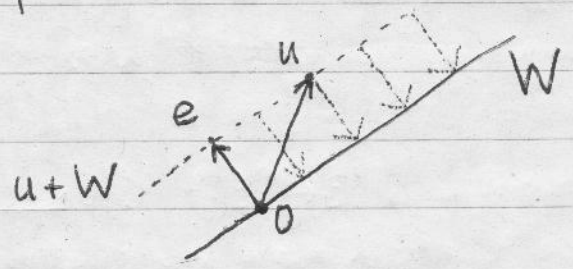
$$Im(f) = W = \{(x, L(x)) \in B^n\}$$

That is, without changing much, any linear code can be replaced with one with matrix

$$\begin{pmatrix} I_{m \times m} \\ L \end{pmatrix}$$

(63) **proposition.** Suppose $W \subset B^n$ is the set of codewords for a linear code, and suppose $e \in B^n$ is the shortest (or one of the shortest) ways to get from a non-codeword $u \in B^n$ to a codeword. That is, suppose e has smallest weight among all e such that $u + e \in W$.

Then e is also the shortest way to get from any of the $u+W$ to a codeword in W.



That is, all words belonging to the coset $u+W$ can be corrected by adding (subtracting) e.

(64) theorem (error-correction). Suppose $f: B^m \to B^n$ is a linear code with matrix $\begin{pmatrix} I_{m\times m} \\ L \end{pmatrix}$,

and suppose $H: B^n \to B^{n-m}$ is the parity check map with matrix $\begin{pmatrix} L & I_{(n-m)\times(n-m)} \end{pmatrix}$

(note that this is not the transpose, and that $L = -L$ since $1+1 \equiv 0 \bmod 2$)

(1) $H(u) = 0$ if and only if $u \in W = \mathrm{Im}(f)$.

(2) H sets up a one-to-one correspondence between the set of cosets $\{u+W\}$ (also denoted B^n/W) and B^{n-m}.

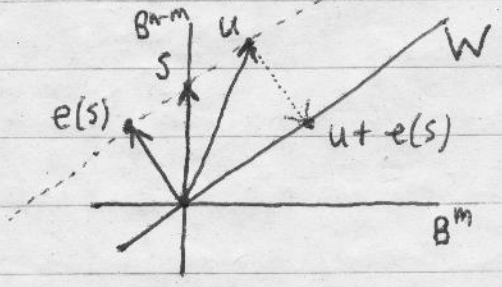
(when viewed as values of H, the elements of B^{n-m} are called, for some reason, syndromes.)

(3) If $e \in (u+W)$ is an element of smallest weight among all elements of $u+W$, and this weight k satisfies

$$(\text{minimal weight of } W) \geq 2k+1,$$

then e is in fact the only element of smallest weight k in $u+W$.

(4) If $e: B^{n-m} \to B^n$ is a choice, for each syndrome s, of element $e(s)$ in the associated coset $u+W$ of minimal weight, then e determines an error-correction scheme by the rule: $u \in B^n$ is corrected to $u + e(H(u))$.



$s = H(u)$

(65) theorem (classification of 3-dimensional Euclidean isometries)
Every rigid motion of E^3 is exactly one of the following:

(1) The identity
(2) A translation
(3) A rotation about an axis
(4) A rotation about an axis followed or preceded by a translation in the direction of that axis
(5) A reflection in a plane
(6) A reflection in a plane followed or preceded by a translation in that plane
(7) A rotation (not by 180°) about an axis followed or preceded by a reflection in a plane perpendicular to that axis
(8) An inversion in a point

(66) corollary. If the set of symmetries of a molecule (or other finite object) is non-trivial but finite, there is a unique point called the center which is fixed by all symmetries. In this case every symmetry is exactly one of the following:

(1) The identity 1
(2) A rotation R about an axis ℓ passing through the center
(3) A reflection σ across a plane π passing through the center
(4) A product $S = \sigma \cdot R$ of a rotation R about an axis ℓ passing through the center followed by the reflection in the plane π passing through the center and perpendicular to ℓ.

definition. The (linear) symmetry group $G(S)$ of a set $S \subset \mathbb{R}^3$ is the subgroup of the group $O(3)$ of orthogonal transformations of $\mathbb{R}^3$ such that $S \mapsto S$. That is, a matrix $F = \begin{pmatrix} F_{11} & F_{12} & F_{13} \\ \cdots & & \end{pmatrix} \in O(3)$ belongs to $G(S)$ if for every $\begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \in S$, $F \cdot \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \in S$.

definition. A representation of a group G on a vector space V is a homomorphism $f: G \to GL(V)$. (Sometimes just denoted V)

If V is $\mathbb{R}^n$, this is the same as a choice of $n \times n$ matrix for each $g \in G$ so that the group multiplication is compatible with matrix multiplication (the matrices are said to "represent" the group elements).

definition. Two representations $f: G \to GL(V)$ and $f': G \to GL(W)$ are called isomorphic if there is a vector space isomorphism $\varphi: V \to W$ compatible with the actions of G:

$$(f'(g))(\varphi(v)) = \varphi(f(g)(v)) \text{ for all } g \in G, v \in V \quad (!)$$

(5) The inversion in the center

(67) proposition. The following are equivalent conditions on two molecules $M, N \subset \mathbb{R}^3$ (centered at 0) and their symmetry groups $G(M), G(N) \subset O(3)$:

(1) There exists a rigid motion $\sigma: \mathbb{R}^3 \to \mathbb{R}^3$ (an orthogonal matrix) such that $G(M) = G(\sigma(N))$

(2) $G(M)$ and $G(N)$ are conjugate subgroups of $O(3)$, meaning:

(3) There exists $\sigma \in O(3)$ such that $G(M) = \sigma \cdot G(N) \cdot \sigma^{-1}$

(4) $G(M)$ is isomorphic to $G(N)$ (they are the same abstract group), and $\mathbb{R}^3$ with the action of $G(M)$ and $\mathbb{R}^3$ with the action of $G(N)$ are isomorphic representations of the group G (in fact, the isomorphism $\mathbb{R}^3 \to \mathbb{R}^3$ must be an isometry)

If these conditions hold, M and N are said to have the same symmetry

(68) fact. Two representations $f: G \to GL(V)$ and $f': G \to GL(W)$ are isomorphic if and only if the two "character" functions

$$\chi_f : G \to \mathbb{R}, \quad g \mapsto \text{trace}(f(g))$$
$$\chi_{f'} : G \to \mathbb{R}; \quad g \mapsto \text{trace}(f'(g))$$

are equal; $\chi_f(g) = \chi_{f'}(g)$ for all $g \in G$.

(69) fact. Every representation V of a finite group G is a direct sum $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ of irreducible subrepresentations (representations having no further subrepresentations).

That is, if G acts on $\mathbb{R}^3$, either $\mathbb{R}^3$ is already irreducible as a representation of G, or $\mathbb{R}^3 = V \oplus W$, where V and W are 1- and 2-dimensional irreducible representations of G, or $\mathbb{R}^3 = V \oplus W \oplus U$, where V, W, and U are irreducible 1-dimensional representations of G.

(70) fact. For a given group G, there are a finite number of irreducible representations V of G. In fact,

$$\sum_{\text{irreducible } V} (\dim V)^2 = |G|$$

Every representation is a sum of these!

(Technically we must allow the representing matrices to be complex.)

(71) **fact.** For a given group G, there are exactly as many irreducible representations V $(f: G \to GL(V))$ as conjugacy classes in G.

(72) **fact.** (orthogonality) If $(V, f: G \to GL(V))$ and $(W, f': G \to GL(W))$ are different irreducible representations, the "inner product" $\chi_f \cdot \chi_{f'}$ is 0:

$$\sum_{g \in G} \chi_f(g) \cdot \overline{\chi_{f'}(g)} = 0$$

Also, the "inner product" of χ_f with itself is $|G|$:

$$\sum_{g \in G} |\chi_f(g)|^2 = |G|$$

(73) **fact.** If $g \in G$ is not the identity,

$$\sum_{\substack{\text{irreducible } V, \\ f: G \to GL(V)}} \dim V \cdot \chi_f(g) = 0$$

(74) **fact.** For any $g \in G$,

$$\left(\begin{array}{c}\text{the number of elements in the} \\ \text{conjugacy class of } g\end{array}\right) \cdot \sum_{\substack{\text{irreducible } V, \\ f}} |\chi_f(g)|^2 = |G|$$

(75) **Theorem.** (classification of 3 dimensional point symmetries)

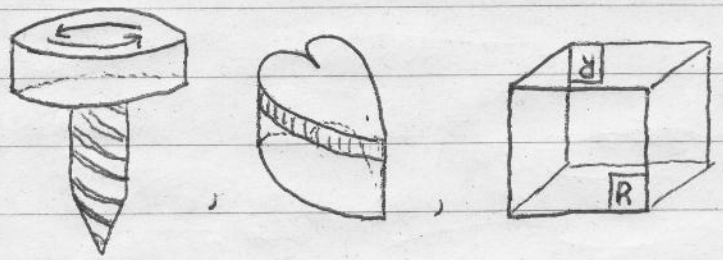
Suppose the abstract symmetry group G of an object or molecule $M \subset \mathbb{R}^3$ is a finite group. Then either:

(1) G has only elements of order 1 and 2

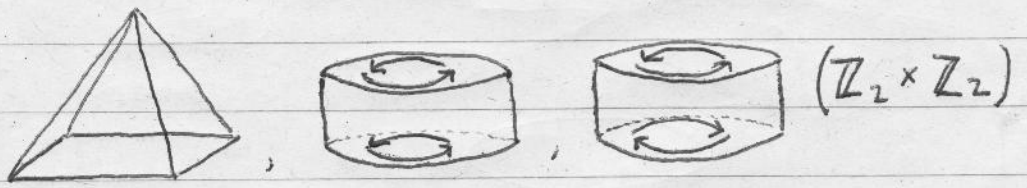
(2) G has exactly 1 element of order higher than 2

(3) G has more than 1 element of order higher than 2

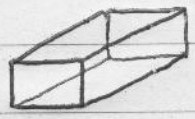
In case 1, G is isomorphic to either $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. M has the same symmetry as one of the following objects, corresponding to the 7 distinct non-trivial three-dimensional representations of these groups:



$(\mathbb{Z}_2)$



$(\mathbb{Z}_2 \times \mathbb{Z}_2)$



$(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$

In case 2, G is isomorphic to either:

- the cyclic group of order k, $\mathbb{Z}_k$ $(k>2)$
- the dihedral group of order $2k$, D_{2k} $(k>2)$
  (the symmetry group of a regular k-gon)
- $\mathbb{Z}_k \times \mathbb{Z}_2$ (k even and $k>2$)

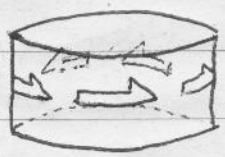
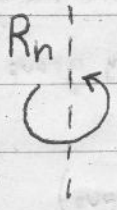
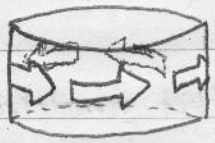
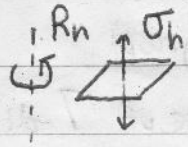
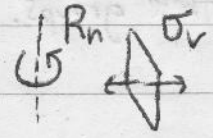
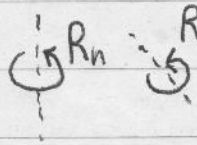
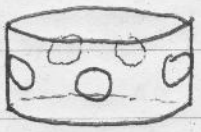
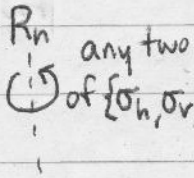
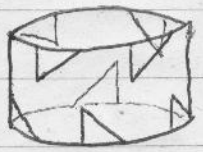
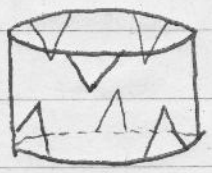
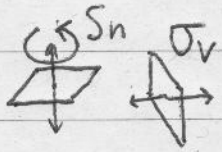
(note that the groups $\mathbb{Z}_k \times \mathbb{Z}_2$ for odd k also appear, as $\mathbb{Z}_{2k}$, by the Chinese Remainder Theorem.)

If the distinguished element has order $n>2$, G can be either

$$\mathbb{Z}_n,\ \mathbb{Z}_{2n},\ D_{2n},\ D_{4n},\ \text{or (if } n \text{ is even) } \mathbb{Z}_n \times \mathbb{Z}_2.$$

M has the same symmetry as one of the following objects, corresponding to the 7 infinite families of non-trivial three-dimensional representations of these groups:

(1 axis of order $n > 2$)

shape	generators	group	representation	chemical notation
		$\mathbb{Z}_n$	$V_{\mathbb{Z}_n} \oplus \mathbb{R}$	"C_n"
		$\mathbb{Z}_n \times \mathbb{Z}_2$	$V_{\mathbb{Z}_n} \oplus \text{sign}_{\mathbb{Z}_2}(\mathbb{R})$	"C_{nh}"
		D_{2n}	$V_{D_{2n}} \oplus \mathbb{R}$	"C_{nv}"
		D_{2n}	$V_{D_{2n}} \oplus \text{sign}_{D_{2n}}(\mathbb{R})$	"D_n"
		D_{4n}	$V_{D_{4n}}^{\text{"}D_{2n}\text{"}} \oplus \text{sgn}_{D_{4n}}^{\text{"}D_{2n}, \mathbb{Z}_2\text{"}}(\mathbb{R})$	"D_{nh}"
(n even) 		$\mathbb{Z}_n$	$V_{\mathbb{Z}_n} \oplus \text{sign}_{\mathbb{Z}_n}(\mathbb{R})$	"S_n"
(n even) 		D_{4n}	$V_{D_{4n}}^{\text{"}D_{2n}\text{"}} \oplus \text{sign}_{D_{4n}}^{\text{"}D_{2n}, \mathbb{Z}_2\text{"}}(\mathbb{R})$	"D_{nv}"

In case 3, G is isomorphic to either:

- S_4 (octahedral group, "full" tetrahedral group, symmetric group)
- A_4 (tetrahedral group, alternating group), $A_4 \times \mathbb{Z}_2$
- A_5 (icosahedral group)
- $S_4 \times \mathbb{Z}_2$ ("full" octahedral group)
- $A_5 \times \mathbb{Z}_2$ ("full" icosahedral group)

M has the same symmetry as one of 7 distinct non-trivial three-dimensional representations of these groups.