(Def) Two sets, or topological spaces, are structurally same if there is a one-to-one function mapping one onto the other such that both this function and its inverse are continuous. Two spaces that are structurally same in this sense are homeomorphic.

(Def) oriented 0-simplex is a point P. Oriented 1-simplex is a directed line segment P\_{1} P\_{2} joining the points P\_{1} and P\_{2} and viewed as traveled in the direction from P\_{1} to P\_{2}. Oriented 2-simplex is a triangular region P\_{1} P\_{2} P\_{3}.

P\_{i} P\_{j} P\_{k} is equal to P\_{1} P\_{2} P\_{3} if \begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix} is an even permutation. opposite to P\_{1} P\_{2} P\_{3} if it is an odd permutation.

(Def) Oriented 3-simplex is given by an ordered sequence P\_{1} P\_{2} P\_{3} P\_{4} of four vertices of a solid tetrahedron. Simplexes are oriented, or have an orientation, meaning that we are concerned with the order of the vertices as well as actual points where vertices are located.

(Def) Boundary of a 0-sumplex P is an empty simplex. notation is “ \partial\_{0} (P) = 0”

Boundary of a 1-simplex P\_{1} P\_{2} is defined by \partial\_{1} (P\_{1} P\_{2}) = P\_{2} – P\_{1}.

Boundary of a 2-simplex is defined by \partial\_{2} (P\_{1} P\_{2} P\_{3}) = P\_{2} P\_{3} – P\_{1} P\_{3} + P\_{1} P\_{2}

Boundary of a 3-simplex is \partial\_{3} (P\_{1} P\_{2} P\_{3} P\_{4}) = P\_{2} P\_{3} P\_{4} – P\_{1} P\_{3} P\_{4} + P\_{1} P\_{2} P\_{4} – P\_{1} P\_{2} P\_{3} . Similar definition holds for \partial\_{n} for n > 3.

Each individual summand of the boundary of a simplex is a face of the simplex.

(Def) A space divided up into simplexes according to following requirements is a simplical complex.

Each point of the space belongs to at least one simplex.

Each point of the space belongs to only a finite number of simplexes.

Two different (up to orientation) simplexes either have no points in common or one is (except possibly for orientation) a face of the other or a face of a face of the other, etc. or the set of points in common is a face, or a face of a face, etc.,, of each complex.

(Def) For a simplical complex X, The group C\_{n} (X) of (oriented) n-chains of X is the free abelian group generated by the (oriented) n-simplexes of X.

Every element of C\_{n} (X) is a finite sum of the form \sum\_{i} m\_{i} \sigma\_{i}, where the \sigma\_{i} are n-simplexes of X and m\_{i} \in \mathbf{Z}. We accomplish addition of chains by taking the algrbraic sum of the coefficients of each occurrence in the chains of a fixed simplex.

(Def) if \sigma is an n-simplex, \partial\_{n} ( \sigma ) \in C\_{n-1} (X) for n = 1,2,3. define C\_{-1} (X) = {0} , then we will also have \partial\_{0} (\sigma ) \in C\_{-1} (X). Since C\_{n} (X) is free abelian, \partial\_{n} gives a unique boundary homomorphism \partial\_{n} mapping C\_{n} (X) into C\_{n-1} (X) for n = 0,1,2,3.

(Def) Kernel of \partial\_{n} consists of those n-chains with boundary 0. The elements of the kernel are n-cycles. The usual notation for the kernel of \partial\_{n} , group of n-cycles, is ‘Z\_{n} (X) ‘.

Image under \partial\_{n} , the group of (n-1)-boundaries, consists of those (n-1)-chains that are boundaries of n-chains. This groups is denoted by ‘B\_{n-1} (X) ’.

(Thm 41.9) Let X be a simplical complex, and let C\_{n} (X) be the n-chains of X for n = 0,1,2,3. Then the composite homomorphism \partial\_{n-1} \partial\_{n} mapping C\_{n} (X) into C\_{n-2} (X) maps everything into 0 for n = 1,2,3. That is, for each c \in C\_{n} (X) we have \partial\_{n-1} (\partial\_{n} (c)) = 0. We use the notation \partial\_{n-1} \partial\_{n} = 0, or \partial^{2} = 0.

(Cor 41.10) For n = 0,1,2 and 3, B\_{n} (X) is a subgroup of Z\_{n} (X).

(Def 41.11) The factor group H\_{n} (X) = Z\_{n} (X) / B\_{n} (X) is the n-dimensional homology group of X.

(Section 42) Computations of Homology Groups

(Def) If a space is divided up into pieces in such a way that near each point the space can be deformed to look like a part of some Euclidean space \mathbb{R}^{n} and the pieces into which the space was divided appear after this deformation as part of a simplical complex, then the original division of the space is a triangulation of the space.

homology groups of the space are defined formally as in the last section.

(Prop) invariance properties of homology groups.

The homology groups of a space are defined in terms of a triangulation, but is the same (isomorphic) groups no matter how the space is trangulated.

If one triangulated space is homeomorphic to another, the homology groups of the two spaces are the same (isomorphic) in each dimension n.

(Def) n-sphere S^{n} is the set of all points a distance of 1 unit from the origin in (n+1)-dimensional Euclidean space \mathbb{R}^{n+1}. The n-cell or n-ball E^{n} is the set of all points in \mathbb{R}^{n} a dinstance \le 1 from the origin.

(subsection) Connected and Contractable Spaces

(Def) A space is connected if any two points in it can be joined by a path lying totally in the space. If a space is not connected, it is split up into a number of pieces, each of which is connected buy no two of which can be joined by a path in space. These pieces are the connected components of the space.

(Thm 42.4) If a space X is trangulated into a finite number of simplexes, then H\_{0} (X) is isomorphic to \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}, and the Betti number m of factors \mathbb{Z} is the number of connected componenets of X.

(Def) a space is contractible if it can be compressed to a point without being torn or cut, but always kept within the space it originally occupied.

(Thm 42.6) If X is a contractible space triangulated into a finite number of simplexes, then H\_{n} (X) = 0 for n \ge 1.

E^{n} is contractable for n \ge 1, so H\_{1} (E^{n}) = 0 for i > 0.

(prop) For n > 0, H\_{n} (S^{n}) and H\_{0}(S^{n}) are isomorphic to \mathbb{Z}, while H\_{i} (S^{n}) = 0 for 0 < i < n.

(Def) an element of H\_{n} (X), that is, a coset of B\_{n} (X) in Z\_{n} (X), a homology class. Cycles in the same homology class are homologous.

(Section 43) More Homology computations and applications

(Def) one-sided closed surface, the Klein bottle. the 1-dimensional homology group will have a nontrivial torsion subgroup reflecting the twist in the surface.

(subsection) Euler Characteristic

(Def) Let X be a finite simplical complex consisting of simplexes of dimension 3 and less, Let n\_{0} be the total number of vertices in the triangulation, n\_{1} the number of edges, n\_{2} the number of 2-simplexes, and n\_{3} the number of 3-simplexes. The number n\_{0} – n\_{1} + n\_{2} – n\_{3} = \sum\_{i = 0}^{3} (-1)^{i} n\_{i} is same no matter how the space X is triangulated. This number is the Euler characteristic \chi (X) of the space.

(Thm 43.7) Let X be a finite simplical complex (or triangulated space) of dimension \le 3. Let \chi (X) be the Euler characteristic of the space X, and let \beta\_{j} be the Betti number of H\_{j} (X). Then \chi (X) = \sum\_{j = 0}^{3} (-1)^{j} \beta\_{j} . This theorem holds also for X of dimension greater than 3, with the extension of the definition of the Euler characteristic to dimension greater than 3.

(subsection) Mapping of Spaces

(prop) a continuous function f mapping a space X into a space Y gives rise to a homomorphism f\_{\*n} mapping H\_{n} (X) into H\_{n} (Y) for n >0.

(prop) If z \in \mathbb{Z}\_{n} (X), and if f(z), regarded as the result of picking up z and setting it down in Y in the naively obvious way, should be an n-cycle in Y, then f\_{\*n} (z + B\_{n} (X)) = f(z) + B\_{n} (Y). That is, if z represents a homology class in H\_{n} (X) and f(z) is an n-cycle in Y, then f(z) represents the image homology class under f\_{\*n} of the homology class containing z.

(Def) a fixed point is some x \in E^{n} s.t. f(x) = x.

(Brower Fixed-point Theorem) (Thm 43.12) A continuous map f of E^{n} into itself has a fixed point for n \ge 1.

(Section 44) Homological Algebra

(subsection) Chain complexes and Mappings

(Def) For a simplical complex X, we get chain groups C\_{k} (X) and maps \partian\_{k} , as indicated in the diagram.

with \partial\_{k-1} \partial\_{k} = 0. Abstract purely algrbraic portion of this situation and consider any sequence of abelian groups A\_{k} and homomorphisms \partial\_{k} : A\_{k} \to A\_{k-1} such that \partial\_{k-1} \partial\_{k} = 0 for k \ge 1. Often A\_{k} = 0 for k < 0 and k > n in applications.

(Def 44.1) Chain complex \langel A, \partial \rangle is a doubly infinite sequence A = { \cdots , A\_{2} , A\_{1}, A\_{0}, A\_{-1} , A\_{-2}, \cdots } of abelian groups A\_{k}, together with a collection \partial = {\partial\_{k} | k \in \mathbb{Z} } of homomorphisms s.t. \partial\_{k} : A\_{k} \to A\_{k-1} and \partial\_{k-1} \partial\_{k} = 0.

(Thm 44.2) If A is a chain complex, then the image under \partial\_{k} is a subgroup of the kernel of \partial\_{k-1}.

(Def 44.3) If A is a chain complex, then the kernel Z\_{k} (A) of \partial\_{k} is the group of k-cycles, and the image B\_{k} (A) = \partial\_{k+1} [A\_{k+1}] is the group of k-boundaries. The factor group H\_{k} (A) = Z\_{k} (A) / B\_{k} (A) is the kth homology group of A.

(Fundamental lemma) (Thm 44.4) Let A and A’ with collections \partial and \partial ‘ of homomorphisms be chain complexes, and suppose that there is a collection f of hoomorphisms f\_{k} : A\_{k} \to A’\_{k} as indicated in the diagram .

Suppose, furthermore, that every square is commutative, that is, f\_{k-1} \partial\_{k} = \partial’\_{k} f\_{k} for all k, Then f\_{k} induces a natural homomorphism f\_{\*k} : H\_{k} (A) \to H\_{k} (A’).

(Def) If the collections of maps f, \partial, and \partial’ have the property f\_{k-1} \partial\_{k} = \partial’\_{k}, that the squares are commutative, then f commutes with \partial.

(Def 44.5) A chain complex \langle A’ , \partial’ \rangle is a subcomplex of a chain complex \langle A , \partial \rangle , if for all k, A\_{k}’ is a subgroup of A\_{k{ and \partial’\_{k} (C) = \partial\_{k} (c) for every c \in A’\_{k} , that is \partial’\_{k} and \partial\_{k} have the same effect on elements of the subgroup A’\_{k} of A\_{k}.

(subsection) Relative Homology

(Def) Suppose that A’ is a subcomplex of the chain complex A. simplical subcomplex Y of a simplical complex X. We can then naturally consider C\_{k} (Y) a subgroup of C\_{k}(X). \partial\_{k} [C\_{k} (Y) ] \le C\_{k-1} (Y)

If A’ is a subcomplex of the chain complex A, we can form the collection A/A’ of factor groups A\_{k}/A’\_{k} . a collection \bar{\partial} of homomorphisms \bar{\partial\_{k} } : ( A\_{k} / A’\_{k} ) \to (A\_{k-1} / A’\_{k-1}) : \bar{\partial\_{k}} (c + A’\_{k}) = \partial\_{k} (c) + A’\_{k-1} for c \in A\_{k}. then \bar{\partial}\_{k-1} \bar{\partial}\_{k} = 0

(Thm 44.7) If A’ is a subcomplex of the chain complex A, then the collection A/A’ of factor groups A\_{k} / A’\_{k} together with collection \bar{\partial} of homomorphisms \bar{\partial}\_{k} defined by \bar{\partial\_{k}} (c + A’\_{k}) = \partial\_{k} (c) + A’\_{k-1} for c \in A\_{k} is a chain complex.

(Def) The homology group H\_{k} (A/A’) is the kth relative homology group of A modulo A’.

(subsection) Exact Homology Sequence of a Pair

(Lem 44.14) Let A’ be a subcomplex of a chain complex A. Let j be the collection of natural homomorphisms j\_{k} : A\_{k} \to (A\_{k}/A’\_{k}). Then j\_{k-1} \parital\_{k} = \bar{\partial}\_{k} j\_{k}, that is, j commutes with \partial.

(Thm 44.15) the map j\_{k} of (Lem 44.14) induces a natural homomorphism j\_{\*k} : H\_{k} (A) \to H\_{k} (A/A’) .

(Lem 44.16) The map \partial\_{\*k} : H\_{k} (A/A’) \to H\_{k-1} (A’) : \partial\_{\*k}(h) = \partial\_{k} (c) + B\_{k-1} (A’) is well defined and is a homomorphism of H\_{k} (A/A’) into H\_{k-1} (A’).

(Lem 44.17) Let i\_{\*k} be the map i\_{\*k} : H\_{k}(A’) \to H\_{k}(A) induced from collection i of injection mappings i\_{k} : A’\_{k} \to A\_{k} : i\_{k}(c) = c for c \in A’\_{k}. We can construct a following diagram.

The groups in diagram, together with given maps, form a chain complex.

(Def 44.18) A sequence of groups A\_{k} and homomorphisms \parital\_{k} forming a chain complex is an exact sequence if all the homology groups of the chain complex are 0, that is, if for all k we have that the image under \partial\_{k} is equal to the kernel of \partial\_{k-1}.

(Thm 44.19) The groups and maps of the chain complex in diagram (Lme 44.17) form an exact sequence.

(Def 44.20) The exact sequence in diagram (Lem 44.17) is the exact homology sequence of the pair (A,A’).

(Section IX) Factorization

(Section 45) Unique Factorization Domains

(Def 45.1) Let R be a commutative ring with unity and let a, b \in R. If there exists c \in R s.t. b = ac, then a divides b (or a is a factor of b), denoted by a|b .

We read a \nmid b as “a does not divide b.”

(Def 45.2) an element u of a commutative ring with unity R is a unit of R if u divides 1, that is, if u has a multiplicative inverse in R. Two elements a, b \in R are associated in R if a = bu, where u is a unit in R.

(Def 45.4) A nonzero element p that is not a unit of an integral domain D is an irreducible of D if in every factorization p = ab in D has the property that either a or b is a unit.

(Def 45.5) An integral domain D is a unique factorization domain (UFD) if the following conditions are satisfied.

Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.

If p\_{1} \cdots p\_{r} and q\_{1} \cdots q\_{s} are two factorizations of the same element of D into irreducibles, then r = s and the q\_{j} can be renumbered so that p\_{i} and q\_{i} are associates.

(Def 45.7) An integral domain D is a principal ideal domain (PID) if every ideal in D is a principal ideal.

(subsection) Every PID is a UFD

(Def 45.8) If {A\_{i} | i \in I} is a collection of sets, then the union \bigcup\_{i \in I} A\_{i} of the sets A\_{i} is the set of all x s.t. x \in A\_{i} for at least one i \in I.

(Lem 45.9) Let R be a commutative ring and let N\_{1} \subseteq N\_{2} \subseteq \cdots be an ascending chain of ideals N\_{i} in R. Then N = \bigcup\_{i} N\_{i} is an ideal of R.

(Ascending Chain condition for a PID) (Lem 45.10) Let D be a PID. If N\_{1} \subseteq N\_{2} \subseteq \cdots is an ascending chain of ideals N\_{i}, then there exists a positive integer r s.t. N\_{r} = N\_{s} for all s \ge r. Equivalently, every strictly ascending chain of ideals (all inclusions proper) in a PID is of finite length.

We express this by saying that the ascending chain condition (ACC) holds for ideals in a PID.

(Thm 45.11) Let D be a PID. Every element that is neither 0 nor a unit in D is a product of irreducibles.

(Lem 45.12) An ideal \langle p \rangle in a PID is maxial iff p is an irreducible.

(Lem 45.13) In a PID, if an irreducible p divides ab, then either p | a or p | b.

(Cor 45.14) If p is an irreducible in a PID and p divides the product a\_{1}a\_{2} \cdots a\_{n} for a\_{i} \in D , then p | a\_{i} for at least one i.

(Def 45.15) A nonzero nonunit element p of an integral domain D is a prime if, for all a, b \in D, p | ab implies either p | a or p | b.

(Thm 45.17) Every PID is a UFD.

(Fundamental Theorem of Arithmetic) (Cor 45.18) The integral domain \mathbb{Z} is a UFD.

(subsection) If D is a UFD, then D[x] is a UFD

(Def 45.19) Let D be a UFD and let a\_{1}, a\_{2}, \cdots , a\_{n} be nonzero elements of D. An element d of D is a greatest common divisor (gcd) of all of the a\_{i} if d | a\_{i} for i = 1, \cdots ,n and any other d’ \in D that divides all the a\_{i} also divides d.

(Def 45.21) Let D be a UFD. a nonconstant polynomial f(x) = a\_{0} + a\_{1} x + \cdots + a\_{n} x^{n} in D[x] is primitive if 1 is a gcd of the a\_{i} for i = 0,1, …, n.

(Lem 45.23) If D is a UFD, then for every nonconstant f(x) \in D[x] we have f(x) = (c)g(x), where c \in D, g(x) \in D[x], and g(x) is primitive. The element c is unique up to a unit factor in D and is the content of f(x). Also g(x) is unique up to a unit factor in D.

(Gauss’s Lemma) (Lem 45.25) If D is a UFD, then a product of two primitive polynomials in D[x] is again primitive.

(Cor 45.26) If D is a UFD, then a finite product of primitive polynomials in D[x] is again primitive.

(Lem 45.27) Let D be a UFD and let F be a field of quotients of D. Let f(x) \in D[x], where (degree f(x)) > 0. If f(x) is an irreducible in D[x], then f(x) is also an irreducible in F[x]. Also, if f(x) is primitive in D[x] and irreducible in F[x], then f(x) is irreducible in D[x].

(Cor 45.28) If D is a UFD and F is a field of quotients of D, then a nonconstant f(x) \in D[x] factors into a product of two polynomials of lower degrees r and s in F[x] iff it has a factorization into polynomials of the same degrees r and s in D[x].

(Thm 45.29) If D is a UFD, then D[x] is a UFD.

(Cor 45.30) If F is a field and x\_{1} , \cdots x\_{n} are indeterminates, then F[x\_{1}, \cdots x\_{n} ] is a UFD.

(Section 46) Euclidean Domains

(Def 46.1) Euclidean norm on an integral domain D is a function \nu mapping the nonzero elements of D into the nonnegative integers s.t. the following conditions are satisfied.

For all a,b \in D with b \neq 0, there exist q and r in D s.t. a = bq + r, where either r = 0 or \nu (r) < \nu (b).

For all a, b \in D, where neither a nor b is 0, \nu (a) \le \nu (ab).

An integral domain D is a Euclidean domain if there exists a Euclidean norm on D.

(Thm 46.4) Every Euclidean domain is a PID.

(Cor 46.5) A Euclidean domain is a UFD.

(subsection) Arithmetic in Euclidean Domains

(Thm 46.6) For a Euclidean domain with a Euclidean norm \nu, \nu(1) is minimal among all \nu (a) for nonzero a \in D, and u \in D is a unit iff \nu (u) = \nu (1).

(Euclidean Algorithm) (Thm 46.9) Let D be a Euclidean domain with a Euclidean norm \nu, and let a and b be nonzero elements of D. Let r\_{1} be as in first condition for a Euclidean norm, that is a = bq\_{1} + r\_{1} where either r\_{1} = 0 or \nu (r\_{1}) < \nu (b) . If r\_{1} \neq 0, let r\_{2} be s.t. b = r\_{1} q\_{2} + r\_{2} where either r\_{2} = 0 or \nu (r\_{2}) < \nu (r\_{1}) . In general, let r\_{i+1} be s.t. r\_{i-1} = r\_{i} q\_{i+1} + r\_{i+1} where either r\_{i+1} = 0 or \nu (r\_{i+1}) < \nu (r\_{i}) . Then the sequence r\_{i}, r\_{2}, \cdots must terminate with some r\_{s} = 0. If r\_{1} = 0, then b is a gcd of a and b. If r\_{1} \neq 0 and r\_{s} is the first r\_{i} = 0, then a gcd of a and b is r\_{s-1}. Furthemore, if d is a gcd of a and b, then there exist \lambda and \mu in D s.t. d = \lambda a + \mu b.

(Section 47) Gaussian integers and multiplicative Norms

(subsection) Gaussian Integers

(Def 47.1) A Gaussian integer is a complex number a + bi, where a, b \in \mathbb{Z}. For a Gaussian integer \alpha = a + bi, the norm N(\alpha) of \alpha is a^{2} + b^{2}.

(Lem 47.2) In \mathbb{Z} [i], the following properties of the norm function N hold for all \alpha , \beta \in \mathbb{Z} [i].

N(\alpha ) \ge 0.

N(\alpha ) = 0 iff \alpha = 0.

N(\alpha \beta ) = N(\alpha ) N(\beta )

(Lem 47.3) \mathbb{Z} [i] is an integral domain.

(Lem 47.4) The function \nu is given by \nu (\alpha ) = N( \alpha ) for nonzero \alpha \in \mathbb{Z} [i] is a Euclidean norm on \mathbb{Z} [i] . Thus \mathbb{Z} [i] is a Euclidean domain.

(subsection) Multiplicative Norms

(Def 47.6) Let D be an integral domain. A multiplicative norm N on D is a function mapping D into the integers \mathbb{Z} s.t. the following conditions are satisfied.

N(\alpha ) = 0 iff \alpha = 0

N( \alpha \beta ) = N( \alpha ) N( \beta ) for all \alpha , \beta \in D.

(Thm 47.7) If D is an integral domain with a multiplicative norm N, then N(1) = 1 and | N(u) | = 1 for every unit u in D. If, furthermore, every \alpha s.t. | N(\alpha ) | = 1 is a unit in D, then an element \pi in D, with | N(\pi) | = p for a prime p \in \mathbb{Z} , is an irreducible of D.

(Fermat’s p = a^{2} + b^{2} Theorem) (Thm 47.10) Let p be an odd prime in \mathbb{Z}. Then p = a^{2} + b^{2} for integers a and b in \mathbb{Z} iff p \equiv 1 \pmod{4} .

(Section X) Automorphisms and Galois Theory

(Section 48) Automorphisms of Fields.

(subsection) The conjugation isomorphisms of Algebraic Field Theory

(Def) all algebraic extensions and all elements algebraic over a field F under consideration are contained in one fixed algebraic closure \bar{F} of F.

(Def 48.1) Let E be an algebraic extension of a field F. Two elements \alpha , \beta \in E are conjugate over F if irr( \alpha , F ) = irr ( \beta , F ) , that is, if \alpha and \beta are zeros of the same irreducible polynomial over F.

(The Conjugation Isomorphisms) (Thm 48.3) Let F be a field, and let \alpha and \beta be algebraic over F with deg ( \alpha , ) = n. The map \psi\_{\alpha , \beta } : F( \alpha ) \to F( \beta ) defined by \psi\_{\alpha , \beta } (c\_{0} + c\_{i} \alpha + \cdots + c\_{n-1} \alpha^{n-1} ) = c\_{0} + c\_{1} \beta + \cdots + c\_{n-1} \beta^{n-1} for c\_{i} \in F is an isomorphism of F( \alpha ) onto F( \beta ) iff \alpha and \beta are conjugate over F.

(Cor 48.5) Let \alpha be algebraic over a field F. Every isomorphism \psi mapping F( \alpha ) onto a subfield of \bar{F} s.t. \psi (a) = a for a \in F maps \alpha onto a conjugate \beta of \alpha over F. Conversely, for each conjugate \beta of \alpha over F, there exists exactly one isomorphism \psi\_{\alpha , \beta } of F( \alpha ) onto a subfield of \bar{F} mapping \alpha onto \beta and mapping each a \in F onto itself.

(Cor 48.6) Let f(x) \in \mathbb{R} [x] . If f(a + bi) = 0 for (a + bi) \in \mathbb{C}, where a, b \in \mathbb{R}, then f(a – bi) = 0 also. Loosely, complex zeros of polynomials with real coefficient occur in conjugate pairs.

(subsection) Automorphisms and Fixed Fields

(Def 48.8) An isomorphism of a field into itself is an automorphism of the field.

(Def 48.9) If \sigma is an isomorphism of a field E onto some field, then an element a of E is left fixed by \sigma if \sigma (a) = a. A collection S of isomorphisms of E leaves a subfield F of E fixed if each a \in F is left fixed by every \sigma \in S. If { \sigma } leaves F fixed, then \sigma leaves F fixed.

(Thm 48.11) Let {\sigma\_{i} | i \in I} be a collection of automorphisms of a field E. Then the set E\_{{ \sigma\_{i} }} of all a \in E left fixed by every \sigma\_{i} for i \in I forms a subfield of E.

(Def 48.12) The field E\_{{ \sigma\_{i} }} of (Thm 48.11) is the fixed field of {\sigma\_{i} | i \in I } . For a single automorphism \sigma, we shall refer to E\_{ {\sigma } } as the fixed field of \sigma.

(Thm 48.14) The set of all automorphisms of a field E is a group under function composition.

(Thm 48.15) Let E be a field, and let F be a subfield of E, Then the set G( E/F) of all automorphisms of E leaving F fixed forms a subgroup of the group of all automorphisms of E. Furthermore, F \le E\_{ G(E/F) } .

(Def 48.16) The group G(E/F) of the preceding theorem is the group of automorphisms of E leaving F fixed, or more briefly, the group of E over F.

(subsection) The Frobenius Automorphism

(Thm 48.19) Let F be a finite field of characteristic p. Then the map \sigma\_{p} : F \to F defined by \sigma\_{p} (a) = a^{p} for a \in F is an automorphism, the Frobenius automorphism, of F. Also, F\_{ \sigma\_{p} } \simeq \mathbb{Z}\_{p} .

(Section 49) The Isomorphism Extension Theorem

(subsection) Extension theorem

(Isomorphism Extension Theorem) (Thm 49.3) Let E be an algrbraic extension of a field F. Let \sigma be an isomorphism of F onto a field F’. Let \bar{F’} be an algebraic closure of F’. Then \sigma can be extended to an isomorphism \tau of E onto a subfield of \bar{F’} s.t. \tau(a) = \sigma(a) for all a \in F.

(Cor 49.4) If E \le \bar{F} is an algebraic extension of F and \alpha , \beta \in E are conjugate over F, then the conjugation isomorphism \psi\_{\alpha , \beta } : F(\alpha ) \to F(\beta ) , given by (Thm 48.3) , can be extended to an isomorphism of E onto a subfield of \bar{F}.

(Cor 49.5) Let \bar{F} and \bar{F’} be two algebraic closures of F. Then \bar{F} is isomorphic to \bar{F’} under an isomorphism leaving each element of F fixed.

(subsection) Index of a Field Extension

(Thm 49.7) Let E be a finite extension of a field F. let \sigma be an isomorphism of F onto a field F’ , and let \bar{F’} be an algebraic closure of F’. Then the number of extensions of \sigma to an isomorphism \tau of E onto a subfield of \bar{F’} is finite, and independent of F’, \bar{F’}, and \sigma. That is, the number of extensions is completely determined by the two fields E and F; it is intrinsic to them.

(Def 49.9) Let E be a finite extension of a field F. The number of isomorphisms of E onto a subfield of \bar{F} leaving F fixed is the index [E : F] of E over F.

(Cor 49.10) If F \le E \le K, where K is a finite extension field of the field F, then [K : F] = [K : E] [E : F] .

(section 50) Splitting Fields

(Def 50.1) Let F be a field with algebraic closure \bar{F} . Let {f\_{i} (x) | i \in I } be a collection of polynomials in F[x] . A field E \le \bar{F} is the splitting field of {f\_{i} (X) |i \in I} over F if E is the smallest subfield of \bar{F} containing F and all the zeros in \bar{F} of each of the f\_{i} (x) for i \in I . A field K \le \bar{F} is a splitting field over F if it is the splitting field of some set of polynomials in F[x].

(Thm 50.3) A field E, where F \le E \le \bar{F}, is a splitting field over F iff every automorphism of \bar{F} leaving F fixed maps E onto itself and thus induces an automorphism of E leaving F fixed.

(Def 50.4) Let E be an extension field of a field F. A polynomial f(x) \in F[x] splits in E if it factors into a product of linear factors in E[x].

(Cor 50.6) If E \le \bar{F} is a splitting field over F ,then every irreducible polynomial in F[x] having a zero in E splits in E.

(Cor 50.7) If E \le \bar{F} is a splitting field over F, then every isomorphic mapping of E onto a subfield of \bar{F} and leaving F fixed is actually an automorphism of E. In particular, if E is a splitting field of finite degree over F, then {E : F} = |G(E/F)|.

(Section 51) Separable Extensions

(subsection) Multiplicity of Zeros of a Polynomial

(Def 51.1) Let f(x) \in F[x]. An element \alpha of \bar{F} s.t. f( \alpha ) = 0 is a zero of f(x) of multiplicity \nu if \nu is the greatest integer s.t. (x- \alpha )^{\nu} is a factor of f(x) in \bar{F} [x].

(Thm 51.2) Let f(x) be irreducible in F[x]. Then all zeros of f(x) in \bar{F} have the same multiplicity.

(Cor 51.3) If f(x) is irreducible in F[x], then f(x) has a factorization in F[x] of the form a \prod\_{i} (x- \alpha\_{i} )^{\nu} , where the \alpha\_{i} are the distinct zeros of f(x) in \bar{F} and a \in F.

(prop) {F(\alpha ) : F } is the number of distinct zeros of irr( \alpha , F).

(Thm 51.6) If E is a finite extension of F, then {E : F} divides [E : F].

(subsection) Separable Extensions

(Def 51.7) A finite Extension E of F is a separable extension of F if {E : F} = [E : F] . An element \alpha of \bar{F} is separable over F if F( \alpha ) is a separable extension of F. An irreducible polynomial f(x) \in F[x] is separable over F if every zero of f(x) in \bar{F} is separable over F.

(Thm 51.9) If K is a finite extension of E and E is a finite extension of F , that is F \le E \le K, then K is separable over F iff K is separable over E and E is separable over F.

(Cor 51.10) If E is a finite extension of F, then E is separable over F iff each \alpha in E is separable over F.

(subsection) Perfect Fields

(Lem 51.11) Let \bar{F} be an algebraic closure of F, and let f(x) = x^{n} + a\_{n-1} x^{n-1} + \cdots + a\_{1} x + a\_{0} be any monic polynomial in \bar{F} [x] . If (f(x))^{m} \in F[x] and m \cdot 1 \neq 0 in F, then f(x) \in F[x] , that is, all a\_{i} \in F.

(Def 51.12) A field is perfect if every finite extension is a separable extension.

(Thm 51.13) Every field of characteristic zero is perfect.

(Thm 51.14) Every finite field is perfect.

(subsection) Primitive element theorem

(Primitive element theorem) (Thm 51.15) Let E be a finite separable extension of a field F. Then there exists \alpha \in E s.t. F = F(\alpha) . (Such an element \alpha is a primitive element.)

That is, a finite separable extension of a field is a simple extension.

(Cor 51.16) A finite extension of a field of characteristic zero is a simple extension.

(Section 52) Totally Inseparable Extensions

(Def 52.1) A finite extension E of a field F is a totally inseparable extension of F if {E : F} = 1 < [E : F] . an element \alpha of \bar{F} is totally inseparable over F if F(\alpha) is totally inseparable over F.

(Thm 52.3) If K is a finite extension of E, E is a finite extension of F, and F < E < K, then K is totally inseparable over F iff K is totally inseparable over E and E is totally inseparable over F.

(Cor 52.4) If E is a finite extension of F, then E is totally inseparable over F iff each \alpha in E, \alpha \neq F, is totally inseparable over F.

(subsection) Separable Closures

(Thm 52.5) Let F have characteristic p \neq 0, and let E be a finite extension of F. Then \alpha \in E, \alpha \notin F, is totally inseparable over F iff there is sime integer t \ge 1 s.t. \alpha^{p^{i}} \in F.

Furthermore, there is a unique extension K of F, with F \le K \le E, s.t. K is separable over F, and either E = K or E is totally inseparable over K.

(Def 52.6) The unique field K of (Thm 52.5) is the separable closure of F in E.

(Section 53) Galois Theory

(Recall)

Let F \le E \le \bar{F}, \alpha \in E , and let \beta be a conjugate of \alpha over F, irr(\alpha F) has \beta as a zero also. Then there is an isomorphism \psi\_{\alpha , \beta } mapping F(\alpha ) onto F(\beta ) that leaves F fixed and maps \alpha onto \beta.

If F \le E \le \bar{F} and \alpha \in E, then an automorphism \sigma of \bar{F} that leaves F fixed must map \alpha onto some conjugate of \alpha over F.

If F \le E, the collection of all automotphisms of E leaving F fixed forms a group G(E/F) . For any subset S of G(E/F) , the set of all elements of E left fixed by all elements of S is a field E\_{s} . Also, F \le E\_{G(E/F)} .

A field E , F \le E \le \bar{F}, is a splitting field over F iff every isomorphism of E onto a subfield of \bar{F} leaving F fixed is an automorphism of E. If E is a finite extension and a splitting field over F, then |G(E/F)| = {E : F} .

If E is a finite extension of F, then {E : F} divides [E : F] . If E is also separable over F, then {E : F} = [E : F]. Also, E is separable over F iff irr( \alpha , F ) has all zeros of multiplicity 1 for every \alpha \in E.

If E is a finite extension of F and is separable splitting field over F, then |G(E/F)| = {E:F} = [E : F].

(subsection) Normal Extensions

(Def 53.1) A finite extension K of F is a finite normal extension of F if K is a separable splitting field over F.

(Thm 53.2) Let K be a finite normal extension of F, and let E be an extension of F, where F \le E \le K \le \bar{F}. Then K is a finite normal extension of E< and G(K/E) is precisely the subgroup of G(K/F) consisting of all those automorphisms that leave E fixed.

Moreover, two automorphisms \sigma and \tau in G(K/F) induce the same isomorphisms of E onto a subfield of \bar{F} iff they are in the same left coset of G(K/E) in G(K/F).

(subsection) Main Theorem

(Def 53.5) If K is a finite normal extension of a field F, then G(K/F) is the Galois group of K over F.

(Main theorem of Galois Theory) (Thm 53.6) Let K be a finite normal extension of a field F, with Galois group G(K/F) . For a field E< where F \le E \le K, let \lambda(E) be the subgroup of G(K/F) leaving E fixed. Then \lambda is a one-to-one map of the set of all such immediate fields E onto the set of all subgroups of G(K/F). The following properties hold for \lambda.

\lambda (E) = G(K/E)

E = K\_{G(K/E)} = K\_{\lambda (E)}

For H \le G(K/F) , \lambda(E\_{H}) = H

[K : E] = |\lambda (E)} and [E : F] = (G(K/F) : \lambda(E) ), the number of left cosets of \lambda(E) in G(K/F).

E is a normal extension of F iff \lambda(E) is a normal subgroup of G(K/F). When \lambda(E) is a normal subgroup of G(K/F), then G(E/F) \simeq G(K/F) / G(K/E).

The diagram of subgroups of G(K/F) is the inverted diagram of intermediate field of K over F.

(prop) The Galois group G(K/F) is the group of polynomial f(x) over F.

(subsection) Galois Groups over Finite fields

(Thm 53.6) Let K be a finite extension of degree n of a finite field F of p^{r} elements. Then G(K/F) is cyclic of order n, and is generated by \sigam\_{p^{r}} , where for \alpha \in K, \sigma\_{p^{r}} (\alpha) = \alpha^{p^{r}}.

(Section 54) Illustrations of Galois Theory

(subsection) Symmetric Functions

(Def) Let F be a field, and let y\_{1}, \cdots , y\_{n} be indeterminates. There are some natural automorphisms of F(y\_{1}, \cdots , y\_{n}) leaving F fixed, those defined by permutations of {y\_{1}, \cdots , y\_{n} . Let \sigma be a permutation of {1, \cdots , n}, that is, \sigma \in S\_{n}. Then \sigma gives rise to a natural map \bar{\sigma} : F(y\_{1}, \cdots , y\_{n}) \to F(y\_{1}, \cdots , y\_{n} ) given by \bar{\sigma} \biggl( \frac{f(y\_{1} , \cdots, y\_{n} ) }{ g(y\_{1}, \cdots, y\_{n}) } \biggr) = \frac{f(y\_{\sigma (1)} , \cdots, y\_{\sigma (n)} ) }{ g(y\_{\sigma (1)}, \cdots, y\_{\sigma (n)})} for f(y\_{1}, \cdots, y\_{n}) , g(y\_{1}, \cdots, y\_{n}) \in F[y\_{1}, \cdots , y\_{n} ] , with g(y\_{1}, \cdots, y\_{n}) \neq 0. \bar{sigma} is an automorphism of F(y\_{1}, \cdots, y\_{n}) leaving F fixed.

The elements F(y\_{1}, \cdots, y\_{n}) left fixed by all \bar{\sigma} , for all \sigma \in S\_{n}, are those rational functions that are symmetric in the indeterminates y\_{1}, \cdots , y\_{n} .

(Def 54.1) An element of the field F(y\_{1}, \cdots , y\_{n}) is a symmetric function in y\_{1}, \cdots , y\_{n} over F, if it is left fixed by all permutations of y\_{1}, \cdots , y\_{n}, in the sense as explained above.

(Thm 54.2) Let s\_{1}, \cdots , s\_{n} be the elementary symmetric functions in the indeteminates y\_{1}, \cdots , y\_{n} . Then every symmetric function of y\_{1}, \cdots, y\_{n} over F is a rational function of the elementary symmetric funcitons,

Also, F(y\_{1}, \cdots, y\_{n} ) is a finite normal extension of degree n! of F(s\_{1}, \cdots , s\_{n}) , and the Galois group of this extension is naturally isomorphic to S\_{n}.

(Section 55) Cyclotomic Extensions

(subsection) Galois group of a Cyclotomic Extension

(Def 55.1) The splitting field of x^{n} -1 over F is the nth cyclotomic extension of F.

(Def 55.2) The polynomial \Phi\_{n} (x) = \prod\_{i = 1}^{\phi (n)} (x- \alpha\_{i} ) where the \alpha\_{i} are the primitive nth roots of unity in \bar{F}, is the nth cyclotomic polynomial over F.

(prop) Over \mathbb{Q}, \Phi\_{n}(x) is irreducible.

(Thm 55.4) The Galois group of the nth cyclotomic extension of \mathbb{Q} has \phi (n) elements and is isomorphic to the group consisting of the positive integers less than n and relatively prime to n under multiplication modulo n.

(Cor 55.6) The Galois group of the pth cyclotomic extension of \mathbb{Q} for a prime p is cyclic of order p-1.

(subsection) Constructible Polygons

(Def) Fermat prime p = 2^{2^{k}} + 1 for k \in \mathbb{N} which is prime.

(Thm 55.8) The regular n-gon is constructible with a compass and a straightedge iff all the odd primes dividing n are Fermat primes whose squares do not divide n.

(Section 56) Insolvability of the Quintic

(subsection) Extensions by Radicals

(Def 56.1) An extension K of a field F is an extension of F by radicals if there are elements \alpha\_{1} , \cdots, \alpha\_{r} \in K and positive integers n\_{1}, \cdots, n\_{r} s.t. K = F(\alpha\_{1}, \cdots, \alpha\_{r}) , \alpha\_{1}^{n\_{1}} \in F and \alpha\_{i}^{n\_{i}} \in F(\alpha\_{1}, \cdots, \alpha\_{i-1}) for 1 < i \le r. A polynomial f(x) \in F[x] is solvable by radicals over F if the splitting field E of f(x) over F is contained in an extension of F by radicals.

(Lem 56.3) Let F be a field of characteristic 0, and let a \in F . If K is the splitting field of x^{n} -a over F, then G(K/F) is a solvable group.

(Thm 56.4) Let F be a field of characteristic zero, and let F \le E \le K \le \bar{F}, where E is a normal extension of F and K is an extension of F by radicals. Then G(E/F) is a solvable group.

(subsection) Insolvability of the Quintic

(Def) Let y\_{1} \in \mathbb{R} be transcendental over \mathbb{Q}, y\_{1} \in \mathbb{R} be transcendental over \mathbb{Q}(y\_{1}) , and so on, until we ger y\_{5} \in \mathbb{R} transcendental over \mathbb{Q} (y\_{1}, \cdots , y\_{4} ). It can be shown by a counting argument that such transcendental real numbers exist. Transcendentals found in this fashion are independent transcendental elements over \mathbb{Q}.

(Def) Elementary symmetry functions in the y\_{i}, namely

s\_{1} = y\_{1} + y\_{2} + \cdots + y\_{5}

s\_{2} = y\_{1}y\_{2} + y\_{1}y\_{3} + y\_{1}y\_{4} + y\_{1}y\_{5} + y\_{2}y\_{3} + \cdots + y\_{3}y\_{5} + y\_{4}y\_{5} ,

\vdots

s\_{5} = y\_{1}y\_{2}y\_{3}y\_{4}y\_{5}

(Thm 56.6) Let y\_{1}, \cdots, y\_{5} be independent transcendental real numbers over \mathbb{Q}. The polynomial f(x) = \prod\_{i = 1}^{5} (x-y\_{i}) is not solvable by radicals over F = \mathbb{Q} (s\_{1}, \cdots, s\_{5}) , where s\_{i} is the ith elementary symmetric function in y\_{1}, \cdots , y\_{5}.