Math 250A Lecture Notes
Groups, Rings, and Fields

Professor: Richard Borcherds
Scribe: Daniel Raban

Contents

1 Groups

1.1 Groups and Actions

Definition 1.1. A *group* is the set of symmetries of something.

Example 1.1. Consider the symmetries of a rectangle. You can:
1: Do nothing
a: Reflect horizontally
b: reflect vertically
c: rotate by π.

Definition 1.2. A *group* is a set G with a binary operation $G \times G \to G$ (usually written $(a, b) \to a + b, a \times b, ab,$ or $a \cdot b$) such that
(1) There is an identity (called e, 1, or 0) such that $ea = a = ae$
(2) Each element has inverse a^{-1} such that $a^{-1}a = aa^{-1} = e$
(3) The operation is associative $(ab)c = a(bc)$.

We must reconcile the two definitions. The first, "concrete" definition can be thought of in the second, "abstract" way by making the operation composition of symmetries. Is the reverse true? Cayley proved that the answer is yes. To show this, we must construct some S with G as the set of its symmetries. G has to act on S. This means we have an action of G on S.

Definition 1.3. An *action* of G on S is a map $G \times S \to S$ such that
(1) $g(h \cdot s) = (gh) \cdot s$ for $s \in S$ and $g, h \in G$
(2) $e \cdot s = s$ for $s \in S$.

Then what is S that satisfies this properties? Well, we can set $S = G$ and make the action on S multiplication by G. This represents G as a subgroup of the symmetries of S; this is not necessarily the group of symmetries of S. But we have shown that G is isomorphic to the set of permutations of a set. Recall:

Definition 1.4. A *subgroup* H of G is a subset of G closed under $\times$ and inverses, containing the identity, e.

Definition 1.5. A *homomorphism* from G to H is a function from G to H preserving $\times$, inverses, and the identity; i.e. $f(ab) = f(a)f(b)$.

Definition 1.6. An *isomorphism* is a homomorphism that is a bijection.

If there is an isomorphism from G to H, then they are essentially the same, up to a relabeling of the elements.

Example 1.2. Let $G = (\mathbb{R}, +)$, and let $H = (\mathbb{R}^*, \times)$ (the nonzero reals). The isomorphism $G \to H$ is the exponential map.

So our new problem is to put some "structure" on $S(= G)$ so that G is the set of all symmetries preserving the structure. The structure is a right action of G on S.

Definition 1.7. A *left* action $G \times S \to S$ is given by $g \cdot s$. A *right* action $S \times G \to S$ is given by $s \cdot g$.

Remark 1.1. The left and right actions of G on S are different, unless the operation is commutative.

A symmetry $f : S \to S$ preserves a right action of G if $f(s \cdot g) = f(s) \cdot g$. Elements of G acting on left preserve right actions as $(g \cdot s) \cdot h = g \cdot (s \cdot h)$ (which follows from the associative law). The right action commutes with the left action. Moreover, anything commuting with the right action is of the form $s \mapsto g \cdot s$ from some $g \in G$. Suppose $f : S \to S$ commutes with a right action. Then $f(e) = g$ for some g. Then $f(s) = f(es) = f(e) \cdot s = g \cdot s$. So f is "the same" as g. So G is exactly the symmetries of G preserving the right action of G.

Picture G as a graph, where edges between elements are labeled by their right actions. Then the left action of G is the symmetries of the graph.

1.1.1 The 8 actions of a group on itself

Suppose we have left action of G on S $(g, s) \mapsto g \cdot s$. We can get a right action by putting $s \cdot g = g^{-1}s$. Indeed, we have $s(gh) = (gh)^{-1}s = h^{-1}(g^{-1}s) = (sg)h$.

4 left actions of G on G:

1. $g \cdot s = s$, the "trivial" action
2. $g \cdot s = gs$, the standard left action
3. $g \cdot s = sg^{-1}$, a right action "made into" a left action
4. $g \cdot s = gsg^{-1}$, the adjoint action, or conjugation [1]

1.2 Lagrange's theorem and consequences

The way we will approach group theory is to list all groups and to prove theorems when we need to study groups of a particular order (different from the treatment in the Lang textbook).

- Order 1: the "trivial" group
- Order 2, 3 (prime order): There is just one group of any prime order p.

To prove the latter fact, we need Lagrange's theorem.

Theorem 1.1 (Lagrange)**.** *If H is a subgroup of G, and the order (or number of elements) of G, H is finite. Then the order of H divides the order of G.*

[1] Some people write conjugation as $g^{-1}sg$.

Definition 1.8. The left cosets of H in G are sets of the form $gH := \{gh : h \in H\}$. The right cosets of H in G are sets of the form $Hg := \{hg : h \in H\}$.

Proof. Look at coests of H in G. Any two left cosets have H elements. Also, any two left cosets are either the same or disjoint. If $g_1h_1 = g_2h_2$, then for $h \in H$, $g_1h = g_2(h_2h_1^{-1}h)$, which is in g_2H. So $|G| = |H| \times$ number of left cosets. □

A special case: if $g \in G$, look at the subgroup H of all powers of g; i.e. $H = \{g^n : n \in \mathbb{Z}\}$. The order of g is the smallest $n > 0$ such that $g^n = e$ (if n exists). The order of subgroup H is the order of g. If $|G|$ is finite, $g \in G$, then order of g divides order of G. Suppose G has order p (prime). Pick $g \in G$. Then g has order 1 or p; the first case is $g = e$, and the second is for every other element. So $G = H$.

1.2.1 Applications of Lagrange's theorem

Theorem 1.2 (Fermat)**.** *If $g \in \mathbb{Z}$ and p (prime) does not divide g, then $g^{p-1} = 1 \pmod p$.*

Proof. Look at group $(\mathbb{Z}/p\mathbb{Z})^*$. This is a group of order $p - 1$, so every element has order dividing $p - 1$. □

Theorem 1.3 (Euler)**.** *Suppose $g, m \in \mathbb{Z}$ are coprime. Then $g^{\phi(n)} = 1 \pmod m$, where $\phi(m)$ is the number of irreducible elements of $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Same as the proof of Theorem 1.2. □

1.2.2 Geometric meaning of Lagrange's theorem

Suppose G acts on a set S transitively. If s, t are in S, then $s = g \cdot t$ for some g. Fix some $s \in S$. Put $H = \{h \in G : h \cdot s = s \, \forall s \in S\}$, the elements of G fixing S. Then the points of S are in bijection with the cosets of H, sending $t \mapsto \{g \in G : \text{ s.t. } g \cdot s = t\}$. These are left cosets since if $g \cdot s = t$, then $(gh) \cdot s = t$, as $h \cdot s = s$.

Interpret $|G| = |H| \times$ number of left cosets in terms of the action. Then we have that $|G| =$ number of elements fixing $s \times$ number of elements of set S. For example, if G is the group of rotations of an icosahedron, then

$$|G| = \text{number of elements fixing center of a face} \times \text{number of faces.}$$

So in this case, $|G| = 3 \times 20 = 60$.

1.3 Groups of order 4 and product groups

- Groups of order 4: 2 Examples.
  - $(\mathbb{Z}/4\mathbb{Z}, +)$ with elements $\{0, 1, 2, 3\}$

- Symmetries of a rectangle $\{1, a, b, c\}$

To show that these two are not isomorphic, look a the orders of elements. The orders of elements in the former are 1, 4, 2, and 4; the orders of elements in the latter are 1, 2, 2, and 2. Order does not change under isomorphism, so these groups are not isomorphic.

Are these all the groups of order 4? Well, by Lagrange's theorem, all elements have order 1, 2, or 4. If a group has an element g of order 4, then the elements are $1, g, g^2, g^3$ with the product being $g^a g^b = g^{a+b \pmod 4}$. Then this is isomorphic to $(\mathbb{Z}/4\mathbb{Z}, +)$. If all elements have order 2, G is abelian (commutative). $1 = g^2h^2 = ghgh$, so $hg = h^{-1}g^{-1} = gh$, making G abelian. Writing G additively, G is a vector space over the field $\mathbb{F}_2$ with 2 elements. So G is isomorphic to the unique 2-dimensional vector space over $\mathbb{F}_2$. So, indeed, there are just 2 groups of order 4.

Definition 1.9. The *product* of 2 groups G and H is $G \times H$, where the operation is $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1, h_2)$.

The group $\{1, a, b, c\}$ is isomorphic to a product of 2 subgroups. $\{1, a, b, c\} \cong \{1, a\} \times \{1, b\}$, where $1 \mapsto (1, 1)$, $a \mapsto (a, 1)$, $b \mapsto (1, b)$, and $c \mapsto (a, b)$.

Example 1.3. $\mathbb{R}^* \cong \{1, -1\} \times \mathbb{R}^+$.

Example 1.4. The polar decomposition gives us $\mathbb{C}^* = S^1 \times \mathbb{R}^+$.

Example 1.5. If $\mathbb{F}$ is a field, the vector space $\mathbb{F}^n$ is a product of n copies of $\mathbb{F}$, under addition.

Example 1.6. Let G be the group of all roots of 1 in $\mathbb{C}$ (contains square roots, cube roots, fourth roots, etc). Then $G = \left\{z \in \mathbb{C} : z = e^{2\pi i(m/n)}, m, n \in \mathbb{Z}\right\}$. Define the subgroups $H_1 = \left\{z \in G : \exists n \in \mathbb{Z} \text{ s.t. } z^{2n} = 1\right\}$ and $H_2 = \left\{z \in G : \exists n \in \mathbb{Z} \text{ s.t. } z^{2n+1} = 1\right\}$. Then $G \cong H_1 \times H_2$. In fact, we can separate in this way by any prime, not just by 2.

2 Groups of orders 6 and 8

2.1 Two groups of order 6

- Groups of order 6
  - the cyclic group $\mathbb{Z}/6\mathbb{Z}$
  - the symmetric group S_3

The former is actually a product[2], $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It has nontrivial proper subgroups $A = \{0, 3\}$ and $B = \{0, 2, 4\}$. $G = AB$, $A \cap B = \{0\}$, and A, B commute, so $G \cong A \times B$.

Definition 2.1. The *symmetric group* is $S_n = \{\text{permutations of } n \text{ points } 1, 2, \ldots, n\}$

Notation for permutations: $(a\ b\ c\ d)$ is the function taking $a \mapsto b \mapsto c \mapsto d \mapsto a$. The 6 elements are $\{e, (1\,2), (2\,3), (1\,3), (1\,2\,3), (1\,3\,2)\}$. The proper subgroups are $\{e, (1\,2\,3), (1\,3\,2)\}, \{e, (1\,2)\}, \{e, (2\,3)\}, \{e, (1\,3)\}$, and $\{e\}$.

2.2 Quotient groups

Fundamental problem: Suppose H is a subgroup of G. We have a set of left cosets aH, the set of such denoted by G/H. Is G/H a group? The most natural attempt is to define the operation as $(aH)(bH) = (ab)H$. The operation we have defined implies that cosets are equivalence classes for the relation $a \equiv b$ iff $aH = bH$ (meaning $a^{-1}b \in H$). Is this well-defined?

Suppose $b_1 \equiv b_2$, so $b_1 = b_2 h$ for some $h \in H$. Then $ab_1 = ab_2 h$, so $ab_1 \equiv ab_2$. Suppose $a_1 \equiv a_2$. We want $a_1 b \equiv a_2 b$. We have $a_2 hb = a_2 b$, so we would be done if the group is commutative. In fact, the condition we need here is $hb = bh'$ for some $h' \in H$; so this operation is well defined if $b^{-1}Hb = H$.

Definition 2.2. A subgroup H is *normal* in G if $gH = Hg$ for all $g \in G$.

Example 2.1. Let $G = S_3$ and $H = \{e, (1\,2\,3), (1\,3\,2)\}$. Then H is normal.

Remark 2.1. In fact, any subgroup of index 2 is always normal. H is normal $\iff$ left cosets are the same as right cosets. If H has index 2, left cosets are H and $G \setminus H$; these are also right cosets, so H is normal. So G/H is a group of order 2.

Example 2.2. Let $G = S_3$ and $H = \{e, (1\,2)\}$. H is not normal because $(23)H(23)^{-1} \neq H$; we have $(2\,3)(1\,2)(2\,3)^{-1} = (1\,3)$, which is not in H. In this case, the right cosets are not equal to the left cosets.

[2] Cayley once made the mistake of thinking these two were different groups, claiming that there were 3 groups of order 6.

2.3 Other groups of order 6

We want to classify the groups of order 6. The first step is to pick an element of order 3. Why does this exist?

Theorem 2.1. *Suppose p is prime and p divides $|G|$. The G has an element of order p.*

Proof. Use induction on the order of the group. Assume this is true for all smaller groups.

First case: G is abelian. Pick some element g of some prime order q; this exists because any element has order dividing G and if g has order mn, g^m has order n. If $q = p$, we are done. If $q \neq p$, then look at group $G/\langle g\rangle$; this has order less than G, so our inductive hypothesis gives us that $G/\langle g\rangle$ has ana elements h or order p. Now lift h to some $a \in G$. $a^p \in \langle g\rangle$, so a has order p or pq. So a or a^q has order p.

Second case: G is not abelian. Look at the adjoint action of G on itself; i.e. $g \cdot s = gsg^{-1}$. Decompose G into orbits under this action. The meaning of a, b being in the same orbit is that $a = gbg^{-1}$ for some $g \in G$. The orbits partition G into equivalence classes. So $|G| = \sum |\text{Orbit}|$. Lagrange's theorem says that $|\text{Orbit}| = |G| / |H|$, where H is the stabilizer of one point of the orbit. So $|G| = \sum_{\text{orbits}} |G| / |H|$. We now have 2 cases:

Case 1: Some H with $|H| < |G|$ has order divisible by p. Then by induction, H has an element of order p, so G does, as well.

Case 2: If $|H| < |G|$ and $|H|$ is not divisible by p, then $|G| / |H|$ is divisible by p. So

$$\underbrace{|G|}_{\text{divisible by } p} = \underbrace{\sum_{\substack{\text{orbits} \\ H \subsetneq G}} \frac{|G|}{|H|}}_{\text{divisible by } p} + \sum_{\substack{\text{orbits} \\ H = G}} \frac{|G|}{|H|} = \underbrace{\sum_{\substack{\text{orbits} \\ H \subsetneq G}} \frac{|G|}{|H|}}_{\text{divisible by } p} + \sum_{\substack{\text{orbits} \\ H = G}} 1.$$

Elements that commute with everything in G, the set of which is called the center of G, is abelian and has order divisible by p because the term on the right is precisely the order of the center of G. By the previous cases, the center of G has an element of order p, so we are done. □

Remark 2.2. This does not need to hold if p is not prime. $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has no element of order 4, but 4 divides $|G|$.

Suppose G has order 6. Pick element g of order 3. Then $\left\{e, g, g^3\right\}$ is a subgroup of order 3. It is normal since it has index 2. Pick an element h of order 2. This gives a subgroup $\{e, h\}$, which is not necessarily normal. Then G is a semidirect product of these subgroups of orders 2 and 3.

Definition 2.3. A *direct product* of groups A and B is $A \times B$ where the operation is $(a_1, b_1)(a_2, b_2) := (a_1a_2, b_1b_2)$.

Here, A and B are both normal and commute. In the following definition, A and B will not necessarily commute.

Definition 2.4. Suppose A is normal and B may not be normal. For each element $b \in B$, $a \mapsto bab^{-1}$ is an automorphism of A. Suppose we have a automorphism φ_b of A for each element of B where $\varphi_{b_1 b_2} = \varphi_{b_1}\varphi_{b_2}$ (this means we have a homomorphism from B into $\mathrm{Aut}(A)$). Then a *semidirect product* of groups A and B is $A \rtimes B$ where the operation is $(a_1, b_1)(a_2, b_2) := (a_1\varphi_{b_2}(a_2), b_1 b_2)$.

So if we have a action of the group B on A, we can define the semidirect product $A \rtimes B$.

Example 2.3. Let $A = \mathbb{Z}/3\mathbb{Z}$, and let $B = \mathbb{Z}/2\mathbb{Z}$. The automorphisms of A are the identity and $a \mapsto -a$. There are 2 ways for B to act on A, the trivial action $\varphi_b(a) = a$, and the nontrivial action $\varphi_b(a) = -a$ if $b \neq e$. These produce the two groups of order 6: $\mathbb{Z}/6\mathbb{Z}$ and S_3, respectively.

There are no other groups of order 6.

2.4 Groups of order 8

Case 1: All elements have order 2. This implies the group is abelian (same argument as last lecture), so it is really a vector space over $\mathbb{F}_2$. So it is $G \cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$.

Case 2: Some element g has order 4. Then $H = \{1, g, g^2, g^3\}$ is a subgroup of index 2, so it is normal. We write what is called an exact sequence:

$$1 \to \underbrace{\mathbb{Z}/4\mathbb{Z}}_{\cong H} \overset{\text{injective}}{\to} G \overset{\text{surjective}}{\to} \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\cong G/H} \to 1.$$

Definition 2.5. An *exact sequence* is a sequence of groups $A \xrightarrow{f} B \xrightarrow{g} C$, where $\mathrm{im}(f) = \ker(g)$. A short exact sequence is an exact sequence of the form $1 \to A \to B \to C \to 1$.

Remark 2.3. A standard blunder is to assume that if we have an exact sequence $1 \to H \to G \to H/G \to 1$, then G is a direct or semidirect product of H and G/H. A counterexample is $G = \mathbb{Z}/4\mathbb{Z}$ and $H = \mathbb{Z}/2Z$.

Remark 2.4. Given $A, B \subseteq G$ with $1 \to A \to G \to B \to 1$ exact, a common problem is to find G. G is called the extension of B by A[3]. This is hard even when A and B are abelian.

Pick some $h \in H$ mapping to a nontrivial element of $\mathbb{Z}/2\mathbb{Z}$. So G contains g, h, $g^4 = e$, $h^2 = e, g$, or g^2, and $\{1, g, g^2, g^3\}$, so $hgh^{-1} = g$ or g^3.

So we get 6 cases. Note that $hgh^{-1} = g$ iff G is abelian. We cannot have $hgh^{-1} = g^3$ and $h^2 = g$, because then g and h commute, so the group is abelian and not abelian. If $h^2 = g$ and $hgh^{-1} = g$, then $G = \mathbb{Z}/8\mathbb{Z}$. Otherwise, if $hgh^{-1} = g$, then $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $hgh^{-1} = g^3$ and $h^2 = e$, we get the dihedral group of order 8. If $h^2 = g^2$ and $hgh^{-1} = g^3$, we have the quaternion group. This covers all the cases.

[3]This is also sometimes called the extension of A by B.

Remark 2.5. The quaternions[4] $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ form a 4 dimensional division algebra containing $\mathbb{C} = \{a + bi, \in \mathbb{R}\}$.

We then have

- Groups of order 8
  - the cyclic group $\mathbb{Z}/8\mathbb{Z}$
  - the product group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $(\cong \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2)$
  - the product group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  - the dihedral group D_8
  - the quaternion group Q_8

[4]The word quaternion actually means soldier. Quaternions (not the mathematical kind) are referenced in the New Testament of Christianity.

3 Non abelian groups of order 8

3.1 The dihedral group

Last time we found two nonabelian groups of order 8, the dihedral group D_8 (the symmetries of a square) and the quaternion group Q_8.

Problem: How many ways are there to arrange 8 non-attacking rooks on a chessboard? Here, non-attacking means that two rooks cannot be placed in the same row or column. There are 8 choices of where to put a rook in the first row, 7 places of where to put a rook in the second row, and so on. So the number of ways is 8!.

Consider a modification to this problem: how many ways are there to do the above up to symmetry? Well, D_8 acts on the configurations by acting on the chessboard. How many orbits are there?

Theorem 3.1 (Burnside[5])**.** *Suppose a group $G \circlearrowright S$. Then the number of orbits under this action is equal to the average number of fixed points of the action. That is,*

$$|\{Orbits\}| = \frac{1}{|G|} \sum_{g \in G} f(g),$$

where $f(g)$ is the number of elements of S fixed by g.

Proof. Look at the set of pair (g, s) with$g \cdot s = s$. Count the number of pairs in two ways:

Method 1: For each g, there are $f(g)$ choices for s. So we get $\sum_{g \in G} f(g)$.

Method 2: Look at one orbit of G of S. Say the orbit contains some $s \in S$. By Lagrange's theorem, the number of points in the orbit is $|G| \,/\, |G_s|$, where G_s is the stabilizer of s. So $|G| = |\text{Orbit}| \times |\text{number of elements in } G \text{ fixing a point of the orbit}|$. This means that the number of elements of G fixing a point in the orbit is the same for each point in the orbit. Then

$$\begin{aligned} |\text{pairs } (g,s)| &= \sum_{\text{orbits}} |\{\text{pairs in orbit}\}| \\ &= \sum_{\text{orbits}} |\text{Orbit}| \times |\text{number of elements in } G \text{ fixing a point of the orbit}| \\ &= \sum_{\text{orbits}} |G| \\ &= |G| \times |\{\text{Orbits}\}| \,. \end{aligned}$$

Dividing both our results by $|G|$ gives us the desired equality. □

Definition 3.1. Two elements $s, b \in G$ are *conjugate* if there exists some $g \in G$ such that $a = gbg^{-1}$. Informally, elements are conjugate if they "sort of look the same."

[5]Many mathematicians have proved this independently of each other, so we could really put anyone's name here.

The elements of D_8 that are conjugate will have the same number of fixed points. To calculate the number of configurations fixed by each conjugacy class, it is helpful to draw pictures and eliminate rows based on the symmetries.

Conjugacy classes of G	number of configurations fixed by element
identity	$8! = 40320$
reflections parallel to sides	$2 \times 0 = 0$
switch both diagonals	$8 \times 6 \times 4 \times 2 = 384$
rotation by $\pi/2$	$2 \times (6 \times 2) = 24$
reflection along a diagonal	$2 \times 764 = 1528$

The most tricky of these is the last one; let c_n be the desired number (not yet multiplied by 2, the size of the conjugacy class), where the chessboard is $n \times n$. then we have a few possibilities: if we place a rook in the top left corner, then there are c_{n-1} ways to arrange other rooks. If we place a rook elsewhere in row 1, we have c_{n-2} ways to arrange the other rooks. So we get a recurrence relation $c_n = c_{n-1} + (n-1)c_{n-2}$, and we can solve to get $c_8 = 764$.

These sum up to be 42256, so using the above theorem, we have our final answer as $42256/8 = 5282$ configurations.

3.2 Quaternions

We can represent quaternions using complex matrices:

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \qquad K = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Any nonzero quaternion has an inverse. Conjugate $\bar{z} = a - bI - cJ - dK$, so $z\bar{z} = a^2 + b^2 + c^2 + d^2$. Then $z^{-1} = 1/z = \bar{z}/(z\bar{z}) = \bar{z}/(a^2 + b^2 + c^2 + d^2)$, where the denominator is nonzero if $z \neq 0$. So nonzero quaternions form a group under multiplication. Call $|z| = a^2 + b^2 + c^2 + d^2$. Letting H^* be the nonzero quaternions, we have a homomorphism $H^* \to \mathbb{R}^*$ that takes $z \to |z|$. This homomorphism has kernel S^3. In fact, our quaternion group is a subgroup of S^3.

Identify $\mathbb{R}^3 = \{bI + cJ + dK \in H\}$. The map $v \mapsto g^{-1}vg$ (for g a nonzero quaternion) maps $\mathbb{R}^3 \to \mathbb{R}^3$. It is a rotation of $\mathbb{R}^3$.[6] So we get a homomorphism $S^3 \to \underbrace{\mathrm{SO}_3(\mathbb{R})}_{\text{rotations of } \mathbb{R}^3}$.

This is not an isomorphism because the kernel has order 2 (exercise). We get a short exact sequence

$$1 \; to \; \{\pm 1\} \to S^3 \to \mathrm{SO}_3(\mathbb{R}) \to 1.$$

[6] In computer graphics, such as in video games, quaternions are used to compute rotations of $\mathbb{R}^3$. They are quicker to multiply than 3×3 matrices.

Pick any finite group of rotations, a subset of $\mathrm{SO}_3(\mathbb{R})$. For example, pick rotations of a rectangle in $\mathbb{R}^3$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or rotations of an icosahedron (has 60 elements). The inverse image of the previous homomorphism is a subgroup of S^3 of twice the order. In our examples, we get the quaternions and the "binary icosahedral group."

4 Groups of order 9, 10, and 12

4.1 Groups of order 9

There are two natural examples for the abelian cases:

- Groups of order 9
  - $\mathbb{Z}/9\mathbb{Z}$
  - $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

These are the only abelian groups: if we have an element of order 9, then we have $\mathbb{Z}/9\mathbb{Z}$, and if all elements are of order 3 an G is abelian, then it is a product of vector spaces over 3 elements, $\mathbb{F}_3 \times \mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

In fact, these two are the only groups of order 9 due to the following theorem:

Theorem 4.1. *Let p be prime. All groups of order p^2 are abelian.*

We require a lemma:

Lemma 4.1. *Any group of order p^n has nontrivial center.*

Proof. Sum over the conjugacy classes of G, picking some g in each C_g. Denote the center of G as Z. If g is in the center of G, then its conjugacy class has only 1 element: g itself. Then

$$|G| = \sum_g |C_g| = \sum_g \frac{|G|}{|G_g|} = \sum_{g \notin Z} \frac{|G|}{|G_g|} + |Z|$$

Since p divides the order of G and the summation term, p divides the order of the center. In particular, the center contains at least p elements and is nontrivial. □

Proof. Suppose G has order p^2. By our lemma, the center is nontrivial, so the center has order p or p^2.

However, the center cannot have order p. Suppose it does, and pick some g not in the center. If $g^2 \in Z$, then g has order p^2, so the group is cyclic and hence abelian. Then $g^2 \notin Z$, so $\langle g \rangle \cap Z = \{e\}$. Then $G = \langle g \rangle\, Z$, so every element can be written as $g^n a$ for some n and a in the center of G. Then all elements commute with each other, so the center is all of G, which is a contradiction.

So the center has order p^2 and is hence all of G. So G is abelian. □

4.2 Nilpotent groups

Suppose G_0 has order p^n. Take its center Z_0, and let $G_1 = G_0/Z_0$. Keep quotienting out by the center. One might think that the center would be trivial after quotienting out by the center, but this is actually not true. Take $G = \{\pm 1, \pm i, \pm j, \pm k\}$ and $Z = \{\pm 1\}$; then $G/\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has nontrivial center.

Definition 4.1. A group is *nilpotent* if it can be reduced to 1 element by repeatedly taking the quotient of its center at each step.

All products of groups of prime power order are nilpotent. Later, we will prove a converse: any finite nilpotent group is the product of group of order p^n.

4.3 Groups of order $2p$

For groups of order 10, and more generally order $2p$ for some prime p, we can generalize the methods we used for groups of order 6:

1. Pick subgroup H of order p
2. H has index 2 so is normal
3. Pick subgroup S of order 2

As in the case of order 6, $G \cong H \rtimes \mathbb{Z}/2\mathbb{Z}$. This is classified by the ways $\mathbb{Z}/2\mathbb{Z}$ can act on $\mathbb{Z}/p\mathbb{Z}$. Later, we will show that the automorphisms are isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$, so we get two groups:

- Groups of order $2p$
  - the abelian group $\mathbb{Z}/2p\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
  - the dihedral group D_{2p}, the symmetries of the regular $2p$-gon (nonabelian)

4.4 Groups of order 12

Our list will be:

- Groups of order 12
  - the abelian group $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
  - the abelian group $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
  - the nonabelian group D_{12}, the dihedral group of order 12 ($\cong D_6 \times \mathbb{Z}/2\mathbb{Z}$)[7]
  - A_4, the rotations of a tetrahedron (nonabelian)
  - binary dihedral group (nonabelian)

[7] D_{8n+4} splits as a product for any $n \in \mathbb{N}$.

5 Groups of Order 12,. . . ,24

5.1 Groups of order 12

Last time we introduced A_4, the symmetries of a tetrahedron, and the binary dihedral group as nonabelian groups of order 12. Recall, that if we have some homomorphism $S^3 \to \mathrm{SO}_3(\mathbb{R})$, then the inverse image has order $2 \times |G|$. If $G = S_3$, then we get A_4.

Look at the rotations of a tetrahedron; what are the conjugacy classes? We have

1. identity
2. rotation by $2\pi/3$ (4 of these)
3. rotation by $4\pi/3$ (4 of these)
4. pick opposite edges and reflect across them (3 of these).

5.1.1 Sylow theorems

Recall that if H is a subgroup of G, the $|H|$ divides $|G|$. Suppose m divides $|G|$. Does G have a subgroup of order m? In general, the answer is no. 6 divides the order of A_4, but there is no subgroup of order 6; this is the smallest counterexample. However, the Sylow theorems provide cases in which this must be true.

Theorem 5.1 (Sylow)**.** *Suppose p is prime, p^n divides $|G|$, and p^{n+1} does not divide $|G|$. Then*

1. *G has a subgroup of order p^n (called a Sylow p-subgroup or p-Sylow subgroup).*
2. *All such subgroups are conjugate.*
3. *There are $1 \pmod p$ such subgroups (and this number divides $|G|$).*
4. *Any subgroup of order p^m with $m \leq n$ is contained in some subgroup of order p^n.*

Proof. To prove part (1), we have 2 cases and proceed by induction on $|G|$. The first case is when some proper subgroup H has index prime to p. Then p^n divides H, so H has a subgroup of order p^n by induction. The second case is when all proper subgroups have index divisible by p. Look at the adjoint action of G on itself. Then any orbit of G has 1 element (stabilizer $= G$) or a multiple of p elements (stabilizer of points $\neq G$). Then, as we showed before, the order of the center is divisible by p. Pick $g \in Z$ of order p. Then $G/\langle g \rangle$ has a subgroup of order p^{n-1} by induction. The inverse image of this subgroup has order p^n.

See Lang for parts (2),(3), and (4), or do them as an exercise. □

Applying this theorem to subgroups of order 3 of groups of order 12, the number of such subgroups is 1 (mod 3) and divides 12. Then the number of is 1 or 4. If it is 1, then the subgroup is normal. Also by the Sylow theorem, G has a subgroup of order $2^2 = 4$. In this case, G is a semidirect product of a normal subgroup of order 3 and a subgroup of order 4. Look at the action of a group of order 4 on it. If $\mathbb{Z}/4\mathbb{Z}$ acts trivially, we get $\mathbb{Z}/12\mathbb{Z}$. If it acts nontrivially, we get the binary dihedral group. If we have $\mathbb{Z}/2\mathbb{Z}$, and it acts trivially, we get $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$; the nontrivial action gives us D_{12}.

If we have 4 subgroups of order 3, label them A_1, A_2, A_3, A_4, where $A_i \cap A_j = \{e\}$ if $i \neq j$. So we get $8 = 4 \times 2$ elements of order 3. This leaves 4 elements not of order 3. We know there is a subgroup of order 4 (by Sylow), so we get 3 elements of order 4, and this subgroup is normal. So G is the semidirect product of the subgroup of order 4 by subgroups $\mathbb{Z}/3\mathbb{Z}$. $\mathbb{Z}/3\mathbb{Z}$ acts nontrivially on the subgroup of order 4. The only possibility is $\mathbb{Z}/3\mathbb{Z}$ acting on $(\mathbb{Z}/3\mathbb{Z})^2$, so there is only 1 possible group. This group is A_4, since it has 4 subgroups of order 3 (fix one of the 4 vertices).

5.2 Solvability

So far we have shown that groups of order ≤ 12 can be split up into products with cyclic groups.

Definition 5.1. A finite group is called *solvable* if either

1. it is cyclic
2. it has a normal subgroup N with N and G/N solvable.

Definition 5.2. G is callled *simple* if has no normal subgroup other than $\{e\}$ and itself.

Example 5.1. The rotations of an icosahedron is a non-cyclic simple group. Look at the conjugacy classes:

1. identity (order 1)
2. rotation by $2\pi/3$ (order 3, 20 of them, each corresponding to a face)
3. rotation by $2\pi/5$ (order 5, 12 of them, each corresponding to a vertex)
4. rotation by $4\pi/5$ (order 5, 12 of them, each corresponding to a vertex)
5. rotation by π (order 2, 15 of them, (number of edges)/2).

Any normal subgroup must be a union of conjugacy classes. Suppose n is the order of a normal subgroup. Then $n = 1+$ some of $\{12, 12, 15, 20\}$, and $n = 1, 2, 3, 5, 6, 10, 12, 15, 20, 30, 60$. Then the only solutions are $n = 1$ or $n = 60$, which shows that this group is simple.

Every finite group can be split up into simple groups.

Theorem 5.2 (Jordan-Holder)**.** *The set of simple groups we get does not depend on the choice of splitting.*

Proof. See Lang.[8] □

Finite simple groups have been classified as 18 types in infinite series and 26 others (sporadic).

Example 5.2. $\mathrm{GL}_n(\mathbb{F}_p)$ gives rise to $\mathrm{SL}_n(\mathbb{F}_p)$ by quotienting out by the kernel of the determinant map, and $\mathrm{SL}_n(\mathbb{F}_p)$ gives rise to $\mathrm{PSL}_n(\mathbb{F}_p)$ by quotienting out by the center.

5.3 Groups of order 13, 14, and 15

13 is prime, and 14 is of order $2p$, so our previous results give us:

- Groups of order 13
  - $\mathbb{Z}/13\mathbb{Z}$
- Groups of order 14
  - $\mathbb{Z}/14\mathbb{Z}$
  - the dihedral group D_{14}

For groups of order 15, we prove general results for groups of order p, q for primes $p < q$.

The Sylow theorems give us that G has a subgroup of order q. The number of conjugates is 1 (mod q) and divides pq. So the only possibility is 1. So G has a normal subgroup $\mathbb{Z}/q\mathbb{Z}$. SO G is a semidirect product of $\mathbb{Z}/q\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$. How can $\mathbb{Z}/p\mathbb{Z}$ act on $\mathbb{Z}/q\mathbb{Z}$? $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) = (\mathbb{Z}/q\mathbb{Z})^*$, which has order $q-1$. This is cyclic (will prove later when we cover fields), so it has 1 subgroup of order p if p divides $q-1$. So either p does not divide $q-1$ or p divides $q-1$. In the first case, the only subgroup of order pq is cyclic, so we get 1 group of order 15. In the second case, there are 2 groups: the first is the cyclic group (comes from the trivial action), and the second is $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. We summarize this as

- Groups of order pq $(p < q)$
  - If p divides $q-1$
    - $\mathbb{Z}/pq\mathbb{Z}$
  - If p does not divide $q-1$
    - $\mathbb{Z}/pq\mathbb{Z}$

[8] Professor Borcherds couldn't really make sense of the proof in Lang, and he has never actually used the Jordan-Holder theorem, which is why proof here has been omitted.

- $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Example 5.3. Let $p = 2$. 2 divides $q - 1$, so we get the cyclic and dihedral groups.

Example 5.4. Let $p = 3$ and $q = 7$. 3 divides $7 - 1$, so we get a nonabelian group. This is the smallest non-abelian group of odd order.

5.4 Groups of order 16

Groups of order 16 are a mess (same is true for p^n, where $n \geq 4$). We just list them and not prove anything.

- Groups of order 16
  - Abelian
    - $\mathbb{Z}/16\mathbb{Z}$
    - $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
    - $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
    - $\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$
    - $(\mathbb{Z}/2\mathbb{Z})^4$
  - Nonabelian, with an element of order 8
    - Generalized quaternion: $g^8 = 1$, $aga^{-1} = g^{-1}$, $a^2 = g^4$
    - Dihedral: $g^8 = 1$, $aga^{-1} = g^{-1}$, $a^2 = 1$
    - Semidihedral: $g^8 = 1$, $aga^{-1} = g^3$, $a^2 = 1$
    - (Nameless): $g^8 = 1$, $aga^{-1} = g^5$, $a^2 = 1$
  - Products
    - $Q_8 \times \mathbb{Z}/2\mathbb{Z}$
    - $D_8 \times \mathbb{Z}/2\mathbb{Z}$
  - Semidirect products
    - $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
    - $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$
  - Miscellaneous
    - Pauli matrices, generated by the matrices

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm i & 0 \\ 0 & \pm i \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}.$$

5.5 Finitely generated abelian groups

So far, the finitely generated abelian groups we know about are finite products of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$. These are actually all the examples.

Theorem 5.3. *Let G be a finitely generated abelian group. Then G is a finite product of groups of the form $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$.*

Proof. Suppose G is abelian (written additively), generated by $g_1, \ldots, g_n$. We have the relations $m_{1,1}g_1 + m_{1,2}g_2 + \cdots + m_{1,n}g_n = 0$, etc, which give us a (possibly infinite) matrix of the coefficients. We can simplify the matrix by adding k times any column to any other; this is a change of generators $g_i \mapsto g_i + kg_j$. We can add k times any row to any other row; if rows $R = S = 0$, this is equivalent to $R = 0$ and $kR + S = 0$. We can apply these operations to make $m_{1,1}$ as small as possible. Subtract multiples of column 1 from other columns to make row 1 have only 1 nonzero entry ($m_{1,1}$). This is possible because $m_{1,1}$ divides $m_{1,2}$; otherwise $m_{1,2} = km_{1,1} + r$ for $|r| < m_1$, and we could subtract $km_{1,1}$ from $m_{1,2}$ and then subtract $r = m_{1,2}$ from $m_{1,1}$ to make $m_{1,1}$ smaller. We can kill off the first column in the same way, leaving $m_{1,1}$ as the only nonzero entry in the first column. Repeat this whole process with $m_{2,2}$ and so on to get a matrix where only $m_{i,i}$ is nonzero for $1 \leq i \leq n$. So our group is now generated by $g_1, \ldots, g_n$ with the relations $m_{1,1}g_1 = 0$, $m_{2,2}g_2 = 0, \ldots$. So $G \cong \mathbb{Z}/m_{1,1}\mathbb{Z} \times \mathbb{Z}/m_{2,2}\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{n,n}\mathbb{Z}$, where if $m_{i,i} = 0$, we just have $\mathbb{Z}$ in the product. □

Remark 5.1. This decomposition is unique if we insist that $m_{i,i}$ divides $m_{j,j}$ for $i < j$ or if we insist that all $m_{i,i}$ are prime powers or 0, and order does not matter.

5.6 Groups of order 17,. . . ,24

17 is prime, so we have

- Groups of order 17
  - $\mathbb{Z}/17\mathbb{Z}$

Groups of order 18 have a normal subgroup of order 3^2. We can then classify the groups by semidirect products to get 5 groups.

- Groups of order 18
  - 5 semidirect product groups
- Groups of order 19
  - $\mathbb{Z}/19\mathbb{Z}$

Groups of order 20 have a normal subgroup of order 5. We can then classify the groups by semidirect products to get 5 groups, as in the case of order 18.

- Groups of order 20
  - 5 semidirect product groups

$21 = pq$ for $p = 3$ and $7 = q$ (and 3 divides $7 - 1$), so we have

- Groups of order 21
  - $\mathbb{Z}/pq\mathbb{Z}$

$22 = 2p$, so we have

- Groups of order 22
  - $\mathbb{Z}/22\mathbb{Z}$

23 is prime, so we have

- Groups of order 23
  - $\mathbb{Z}/23\mathbb{Z}$
- Groups of order 24
  - the symmetric group S_4
  - Binary dihedral group (inverse image of A_4 under $S^3 \to \mathrm{SO}_3$)
  - a dozen or so others...

6 Symmetric Groups

6.1 Basic definitions

Definition 6.1. The *symmetric group* S_n is the group of all permutations of the n points $\{1, \dots, n\}$.

$|S_n| = n!$ because there are n choices for the image of 1, then $n-1$ choices for the image of 2, etc. We denote elements using cycle notation: $(a\, b\, c\, d)$ is the function taking $a \mapsto b \mapsto c \mapsto d$.

Definition 6.2. A transposition is a permutation that exchanges 2 elements and fixes all others.

Proposition 6.1. *S_n is generated by the transpositions $(1\,2), (2\,3), (3\,4), \dots, (n-1\,n)$.*

Proof. This is "bubblesort," the "2nd worst" sorting algorithm.[9] In the worst case, bubblesort takes $n(n-1)/2$ exchanges to sort a list of n elements. □

6.2 The alternating group

Look at S_n acting on variables $x_1, \dots, x_n$. It also acts on $\mathbb{C}[x_1, \dots, x_n]$, polynomials in n variables. Look at the discriminant,

$$\Delta = (x_1 - x_2)(x_2 - x_3) \cdots (x_1 - x_3) \cdots (x_{n-1-x_n}) = \prod_{i<j} (x_i - x_j).$$

Any $\sigma \in S_n$ maps Δ to Δ or $-\Delta$, so there exists some homomorphism $\varepsilon : S_n \to \{\pm 1\}$.

Definition 6.3. The *alternating group* A_n is the subgroup of elements $\sigma \in S_n$ such that $\sigma(\Delta) = \Delta$); this is the kernel of ε.

So A_n is normall in S_n, of order $n!/2$.

6.3 S_n, A_n, and platonic solids

Symmetries of platonic solids are very closely related to the groups S_n and A_n.

The rotations and reflections of a tetrahedron is S_4, acting on the vertices; the rotations are then A_4. The rotations of a cube or an octahedron are given by S_4 acting on the permutations of the diagonals; then the rotations and reflections are given by $S_4 \times \mathbb{Z}/2\mathbb{Z}$. The number of rotations of a dodecahedron or an icosahedron is given by permutations of the five inscribed "inner cubes," which gives a homomorphism of rotations to S_5, and this group is A_5; then the rotations and reflections are given by $A_5 \times \mathbb{Z}/2\mathbb{Z}$.

[9] The "worst" algorithm is called bogosort.

We summarize the results in this table:

platonic solid	number of rotations	number of rotations and reflections
tetrahedron	12 (A_4)	24 (S_4)
cube/octahedron	24 (S_4)	48 ($S_4 \times \mathbb{Z}/2\mathbb{Z}$)
dodecahedron/icosahedron	60 (A_5)	120 ($A_5 \times \mathbb{Z}/2\mathbb{Z} \ncong S_5$)

These groups are "spherical reflection groups."

6.4 Conjugacy classes of S_n

We can write any element of S_n as a product of disjoint cycles.

Definition 6.4. The cycle shape is the sizes of the cycles with multiplicities.

Example 6.1. The permutation $(1\,2\,4)(5\,7\,8)(6\,9)(10)(3)$ has cycle shape $3^2, 2, 1^2$.

Two elements are conjugate if they have the same cycle shape. Given a, b, with the same cycle shape, how can we find g with $a = gbg^{-1}$? Write out the two permutations in cycle notation and pair off elements:

$$(1\,2\,4)(5\,7\,8)(6\,9)(10)(3)$$
$$\uparrow\uparrow\uparrow\ \uparrow\uparrow\uparrow\ \ \uparrow\uparrow\ \ \uparrow\ \ \uparrow$$
$$(2\,4\,5)(6\,7\,8)(1\,3)(9)(10)$$

This gives us $g = (1\,6\,5\,4\,2\,1)(3\,9\,10)(7)(8)$.

Example 6.2. How many conjugacy classes are the of S_4? This is the number of cycle shapes, which is also the number of partitions of 4. Denoting C_σ as the conjugacy class (viewing S_4 as the rotations of a cube) and G_σ as the stabilizer under the action of conjugation (also is the centralizer).

partition	cycle shape	C_σ	$\lvert G_\sigma\rvert$	$\lvert C_\sigma\rvert = \lvert G\rvert \,/\, \lvert G_\sigma\rvert$
1+1+1+1	1^4	identity	24	1
2+1+1	$2, 1^2$	rotation by π	4	6
3+1	$3, 1$	rotation by $2\pi/3$	3	8
2+2	2^2	rotation by π	8	3
4	4	rotation by $\pi/2$	4	6

If σ has cycle shape $1^{n_1}2^{n_2}3^{n_3}\cdots$, then the number of elements in the centralizer is $1^{n_1}n_1! \cdot 2^{n_2}n_2! \cdots$.

6.5 Normal subgroups of S_n

What are the normal subgroups of S_n? We already know of $\{e\}$, A_n, and S_n. Viewing S_4 as the rotations of a cube, we have that S_4 acts on 3 lines by permuting them; so we have a homomorphism $S_4 \to S_3$, where the kernel is a normal subgroup of order 4 (the identity + 3 rotations by π). Following this pattern, we have homomorphisms S_2 onto S_1, S_3 onto S_2, and S_4 onto S_3. However, the pattern breaks because there is no homomorphism from S_5 onto S_4; S_5 has a simple subgroup A_5, the rotations of an icosahedron. If N is any normal subgroup of S_5, $N \cap A_5$ is normal in A_5, so it is 1 or 5. So the only normal subgroups of S_5 are $\{e\}$, A_5, and S_5.

Theorem 6.1. *A_n is simple for $n \geq 5$.*

Proof. We sketch a proof using induction on n. Suppose N is normal in S_n. Pick an element $g \in N$ with $g \neq e$. Find h so that $ghg^{-1}h^{-1}$ fixes the point 1 (exercise). So $ghg^{-1}h^{-1} = g(hg^{-1}h^{-1})$ is also in N, which makes N have nontrivial intersection with S_{n-1} (things fixing 1). So $N \cap S_{n-1} = A_{n-1}$ or S_{n-1}. So N contains all elements of A_n fixing 1. Similarly, it contains all elements fixing i for any i. These generate A_n (also an exercise). □

Example 6.3. There are three groups of order 120 containing A_5 and $\mathbb{Z}/2\mathbb{Z}$ as composition factors.

1. $A_5 \times \mathbb{Z}/2\mathbb{Z}$
2. S_5, which has a subgroup A_5 and the quotient group $\mathbb{Z}/2\mathbb{Z}$
3. Binary icosahedral group[10], which has a quotient group A_5 and a subgroup $\mathbb{Z}/2\mathbb{Z}$

6.6 Outer automorphisms of S_n

Conjugation is an automorphism of a group G, and we get an exact sequence

$$1 \to Z(G) \to \text{conjugations} \to \text{Aut}(G) \to \text{outer automorphisms} \to 1.$$

For $n \geq 3$ with $n \neq 6$, $\text{Aut}(S_n) \cong S_n$, and all these automorphisms are inner automorphisms.

Let's find a non-inner automorphism of S_6. Start with S_5. This has a subgroup of order 20. S_5 acts on $0, 1, 2, 3, 4 \in \mathbb{F}_5$, and has the following subgroup: all permutations of the form $x \mapsto ax + b$ for $a, b \in \mathbb{F}_5$. So S_5 has a subgroup of index 6, so it acts transitively on 6 points, giving us a homomorphism from $S_5 \to S_6$ which is different from the usual such

[10] Let G be this group. Then S^3/G, the cosets of G in S^3 (not a group), has the same homology as S^3 but is not homeomorphic to S_3.

homomorphisms that fix some element (which are not transitive). S_6 has 12 subgroups $\cong S_5$, not 6, as we might expect.

Any subgroup of index n in G products a homomorphism from $G \to S_n$, where G acts transitively on n points, so any subgroup of index 6 in S_6 gives a homomorphism from $S_6 \to S_6$. Pick one of the "funny" homomorphisms $S_5 \to S_6$ to get a homomorphism from $S_6 \to S_6$. Check that this is not an inner automorphism (exercise).

7 Category Theory

7.1 Categories

The purpose of category theory is to generalize common properties of existing structures so we do not need to refer to the internal structure of our objects at all.

Definition 7.1. A *category* is a collection of *objects* and a set of *morphisms* such that

1. Each morphism has a domain and a range, both of which are objects
2. For each object a, there is an identity morphism 1_a
3. For morphisms $X : a \to b$ and $Y : b \to c$, there is a composite morphism $Y \circ X$
4. $(X \circ Y) \circ Z = X \circ (Y \circ Z)$ if both are defined
5. $1_b \circ X = X \circ 1_a = X$ if $X : a \to b$

Example 7.1. In the category of sets, the objects are sets, and the morphisms/arrows are functions.

Example 7.2. In the category of groups, the objects are groups, and the morphisms/arrows are group homomorphisms.

Example 7.3. In the category of topological spaces, the objects are topological spaces, and the morphisms/arrows are continuous functions.

Example 7.4. Take a category with a single object, and let the morphisms be the elements of a group G, where composition of the morphisms is the group operation. This is a group.

Example 7.5. Let S be a partially ordered set with $\leq$. We can make a category with objects equal to the elements of S and morphisms from $a \to b$ such that there is 1 morphism if $a \leq b$ and 0 otherwise.

7.2 Functors

Definition 7.2. A *(covariant) functor* F from a category $\mathscr{C}$ to a category $\mathscr{D}$ is defined by the properties

1. F is a function from objects of $\mathscr{C}$ to objects of $\mathscr{D}$
2. F is a function[11] from morphisms of $\mathscr{C}$ to morphisms of $\mathscr{D}$
3. $F(1_A) = 1_{F(A)}$

[11] Really, these are two separate functions, but we refer to them together as one function, the functor F.

4. $F(f \circ g) = F(f) \circ F(g)$.

Let $f : A \to B$ be a morphism. The fourth condition makes it so $F(f)$ is a morphism from $F(A) \to F(B)$; this is because we can set $g = 1_A$.

Example 7.6. We can define a functor F from the category of groups to the category of sets by $F(G) =$ the underlying set of G. F sends group homomorphisms to themselves as functions.

Example 7.7. The reason why functors were introduced was to study homology groups H_i. H_i is a functor from topological spaces to abelian groups.

Example 7.8 (Abelianization of a group)**.** Suppose G is a group. We can make G abelian by quotienting out $G/\left\langle \left\{ ghg^{-1}h^{-1} : g, h \in G \right\} \right\rangle$ to get an Abelian group G^{ab}. This is a functor from Groups to Abelian groups. If $f : G \to H$, we get a map $G^{\text{ab}} \to H^{\text{ab}}$ (exercise).

Example 7.9. We have a functor from sets to abelian groups given by $F(S) = F_{\text{ab}}(S)$, the free abelian group on S. This is the set of elements $n_1 s_1 + n_2 s_2 + \cdots$ such that all but finitely many $n_i = 0$. If $f : S \to S'$ is a function, $F(f') : S \to S'$ sends $\sum_\alpha n_\alpha s_\alpha \mapsto \sum_\alpha n_\alpha s'_\alpha$.

Example 7.10. Take a group G, viewed as a category with 1 object. A functor from the group to sets will send the 1 object to some set and each $g \in G$ to some function $S \to S$. So we get the action of G on a set S, the permutations of S.

Definition 7.3. A *contravariant functor* is a functor where $F(f \circ g) = F(g) \circ F(f)$.

Similarly to the note we made above, this property implies that if $f : A \to B$ is a morphism, $F(f)$ is a morphism from $F(B) \to F(A)$.

Example 7.11. Let both categories be vector spaces over the same field K. We can define a functor $F(V) = \text{Hom}(V, K)$; this is V^*, the dual of V. Suppose $f : V \to W$ is a morphism; we must map it to some morphism $F(f) : W^* \to V^*$. We get the morphism $\lambda \mapsto \lambda \circ f$.

Example 7.12. Suppose $\mathscr{C}$ is the category of a abelian groups. Look at $\text{Hom}(A, B)$ for abelian groups A, B. This is a *bifunctor* in 2 variables form $C \times C \to C$. It is covariant in B and contravariant in A. If $f : B_1 \to B_2$, we get a map $F(f) : \text{Hom}(A, B_1) \to \text{Hom}(A, B_2)$. If $g : A_1 \to A_2$, we get a map $F(g) : \text{Hom}(A_2, B) \to \text{Hom}(A_1, B)$.

Example 7.13. We can have the category of categories, where the objects are categories and the morphisms are functors.

Remark 7.1. This does not actually exist because there is no set of all sets. Let $R = \{x : x \notin x\}$; then $R \in R \iff R \notin R$. Similarly, the category of all groups does not exist, either. We have a few possible solutions:

1. Only work with groups whose elements are in some fixed large set
2. Work in set theory with "classes"
3. Grothendieck universes
4. Ignore it

We will adopt the 4th solution.

7.3 Natural transformations

What does natural mean? Look at finite dimensional vector spaces. We know that $V \cong V^*$, but there is no *natural* isomorphism. However, $V \cong V^{**}$ with a "natural isomorphism"

$$v \mapsto f_v, \text{ where for each } w \in V^*, \ f_v(w) = w(v).$$

Definition 7.4. Suppose we have 2 categories C, D with functors $F : C \to D$ and $G : C \to D$. A *natural transformation* $\varphi : F \to G$ is a function φ such that

1. $\varphi(a)$ is a morphism from $F(a) \to G(a)$
2. if $f : a \to b$, $\varphi(b) \circ F(f) = G(f) \circ \varphi(a)$. That is, the following diagram commutes:

$$\begin{array}{ccc} F(a) & \xrightarrow{\varphi(a)} & G(a) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(b) & \xrightarrow{\varphi(b)} & G(b) \end{array}$$

Example 7.14. Look at $C = D =$ vector spaces over a field K. Let F be the identity from C to D, and let G be the double dual, $G(V) = V^{**}$. Then there is a natural transformation from $F \to G$. For each vector space V, we have a morphism (in fact an isomorphism since it has an inverse) from $F(V) \to G(V)$ that satisfies the conditions above.

7.4 Products

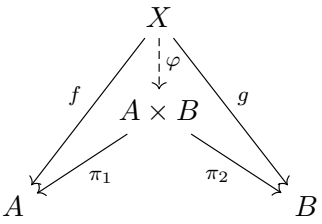
The product is a typical construction in many spaces. Familiar examples include:

Example 7.15. The product of sets A, B is $A \times B = \{(a, b) : a \in A, b \in B\}$.

Example 7.16. The product of groups A, B is $A \times B = \{(a, b) : a \in A, b \in B\}$ with a group operation given by $(a, b)(c, d) = (ac, bd)$.

Example 7.17. The product of topological spaces A, B is $A \times B = \{(a, b) : a \in A, b \in B\}$ with the product topology.

Definition 7.5. Suppose X is any object with morphisms $f : X \to A$ and $f : X \to B$. Then a *product* $A \times B$ of A and B is an object with morphisms $\pi_1 : A \times B \to A$ and $\pi_2 : A \times B \to B$ such that there exists a unique map $\varphi : X \to A \times B$ such that $\varphi \circ \pi_1 = f$ and $\varphi \circ \pi_2 = g$.



This property defines $A \times B$ up to canonical isomorphism (a morphism $f : A \to B$ such that we can find $g : B \to A$ with $f \circ g = 1_B$ and $g \circ f = 1_A$). Suppose X, Y are both products of A and B. Then the composition of the two maps φ, ψ between X and Y is the identity by the uniqueness of the map defined above.

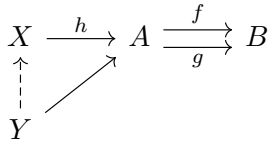
So we can define products in any category, and this definition ignores the internal structure of the objects.

7.5 Equalizers

Definition 7.6. Let A and B be objects in a category. The *equalizer* of two morphisms $f, g : A \to B$ is an object X and a morphism $h : X \to A$ such that

1. $f \circ h = g \circ h$
2. If Y is an object with $i : Y \to A$ such that $f \circ i = g \circ i$, then Y factors uniquely through X.

That is, the followng diagram commutes:



Suppose A, B are groups with $f : A \to B$. The kernel of f is the equalizer of f and $\mathbb{1}$, the trivial map from $A \to B$.

7.6 Initial and final objects

Definition 7.7. A is an *initial object* if there is a unique morphism from A to any other object in the category.

Initial objects are unique up to isomorphism (exercise).

Example 7.18. The empty set is an initial object in the category of sets.

Example 7.19. The trivial group is an initial object in the category of groups.

Definition 7.8. A is a *final object* if there is a unique morphism from any other object in the category to A.

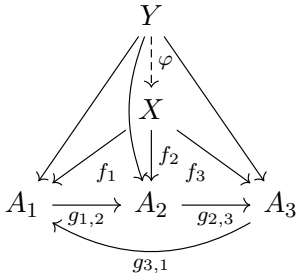
Example 7.20. A 1-element set is a final object in the category of sets.

Example 7.21. The trivial group is a final object in the category of groups.

7.7 Limits and pull-backs

Definition 7.9. A *limit* of $\{A_\alpha\}$ is an object X with morphisms $f_\alpha : X \to A_\alpha$, characterized by the following properties:

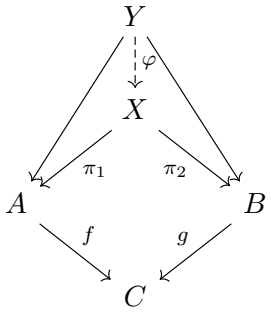
1. If $g_{\alpha,\alpha'} : A_\alpha \to A_{\alpha'}$ is a morphism, then $f_{\alpha'} = g_{\alpha,\alpha'} \circ f_\alpha$.
2. Any Y with this property factors through X.



Example 7.22. A product is a limit of A and B.

Example 7.23. The equalizer is a limit of A and B with morphisms $f, g : A \to B$.

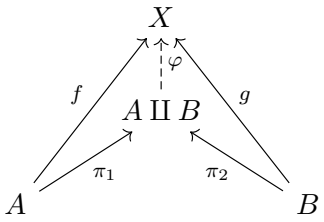
Definition 7.10. The *pull-back* X is a limit of A and B with morphisms $f : A \to C$ and $g : B \to C$.



Example 7.24. The pull-back of sets A, B is $\{(a, b) \in A \times B : f(a) = g(b)\}$.

7.8 Coproducts

If we reverse the arrows in a product, we get a coproduct.



Example 7.25. In the category of sets, the coproduct is the disjoint union.

Example 7.26. In the category of abelian groups, the coproduct equals $A \times B$, so the coproduct equals the product.

In the category of groups, what is the coproduct of A and B? It is the *free group* on two generators. We will discuss this next lecture.

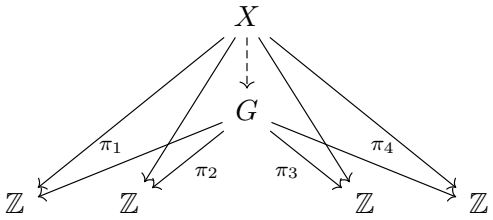
We can also take infinite products and coproducts. The infinite product of abelian groups is the usual infinite product, and the infinite coproduct of abelian groups is the subgroup of the infinite product such that all but finitely many of the coordinates vanish.

8 Free Groups

8.1 Free abelian groups

Definition 8.1. The *free abelian group* on n generators $g_1, g_2, \ldots, g_n$ is the group of elements of the form $\sum_{i=1}^{n} n_i g_i$ with $n_i \in \mathbb{Z}$.

There exists a unique isomorphism $\mathbb{Z}^n \cong G$ taking $e_i \mapsto g_i$. In categorical terms, the free abelian group is the coproduct of n copies of Z.



Call n, the exponent of $\mathbb{Z}$, the rank of the free abelian group. Is the rank determined by $G = \mathbb{Z}^n$? Yes, because the number of homomorphisms from $\mathbb{Z}^n \to \mathbb{Z}/2\mathbb{Z}$ is 2^n.

Proposition 8.1. *Any subgroup of $\mathbb{Z}^n$ is free of rank $\leq n$.*

Proof. Recall the proof that finitely generated abelian groups are products of cyclic groups. We showed that if A is a subgroup of $\mathbb{Z}^n$, we can find generators $g_1, \ldots, g_n$ of $\mathbb{Z}^n$. So A is generated by $n_1 g_1, n_2 g_2, \ldots$ for some n_i, making A free of rank $\leq n$. □

8.2 The free group on $g_1, \ldots, g_n$

8.2.1 Construction of the free group

Take all words in symbols $g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_n, g_n^{-1}$, including the empty word. For example 1, g_1, $g_1 g_2$, $g_1 g_2 g_1^{-1} g_2$, etc. These have an associative product, which is just concatenation of words. However, aa^{-1} is not the identity, so we still have some work to do. Take the smallest equivalence relation such that $g_1 g_1^{-1} \equiv 1$, $g_2 g_2^{-1} \equiv 1$,$g_3 g_3^{-1} \equiv 1$, ... and such that if $a \equiv b$, then $ac \equiv bc$ and $ca \equiv cb$. This second condition ensures that the product is well-defined.

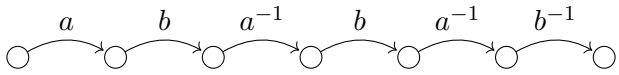
Definition 8.2. The *free group* on generators $g_1, \ldots, g_n$ is the group of equivalence classes of words in symbols $g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_n, g_n^{-1}$ under this equivalence relation, with the group operation being concatenation of words.

What does the free group look like? It can be identified with "reduced" words in $g_1, g_1^{-1}, \ldots$, where reduced means that we cancel out $g_1 g_1^{-1}$, $g_2 g_2 - 1$, etc.

If A and B are different reduced words, are they different in the free group? Yes. It is sufficient to show that AB^{-1} is empty. Then it is sufficient to show that if A is a reduced

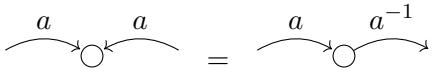
word other than 1, the empty word, then $A \not\equiv 1$. We show that if $A \neq 1$ is a reduced word, we can find a finite group G and a map from the free group to G so that the image of A under this map is nontrivial. This is the statement that free groups are residually finite (nontrivial elements can be detected by finite groups).

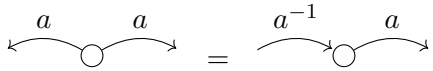
Our finite group will be S_n for $n = 1+$length of the word A. We will illustrate the argument with an example. Let $A = b^{-1}a^{-1}ba^{-1}ba$. Draw the following graph on n vertices:



Map a to an element of S_{11} that respects the arrows on the graph; here, we must send a to a permutation σ_a with $\sigma_a(1) = 2$, $\sigma_a^{-1}(3) = 4$, and $\sigma_a^{-1}(5) = 6$, and we must send b to a permutation σ_b with $\sigma_b(2) = 3$, $\sigma_b(4) = 5$, and $\sigma_b^{-1}(6) = 7$. The constraints on a^{-1} become constants on a by noting that $\sigma_a^{-1}(x) = y \iff \sigma_a(y) = x$; the same holds for b^{-1}. Then A gets mapped to the permutation $\sigma_b^{-1}\sigma_a^{-1}\sigma_b\sigma_a^{-1}\sigma_b\sigma_a$, and this permutation sends the leftmost vertex, representing the element 1, to the rightmost vertex, representing the element $n = 7$.

There are two cases we need to watch out for. The first case is when we have two arrows labeled (without loss of generality) a going into the same vertex. The second case is when we have two arrows labeled a leaving the same vertex. But these are the graphs





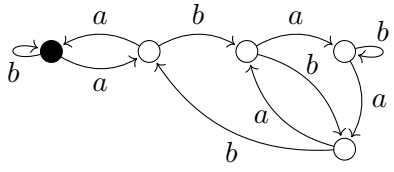
We cannot have aa^{-1} or $a^{-1}a$, lest these be reduced to the empty word. So our construction holds, and we are done.

For free abelian groups, a and b are isometries of the euclidean plane. For free groups, a and b are isometries of the hyperbolic plane.

8.2.2 Subgroups of free groups

Subgroups of free groups are free, but may have larger rank.

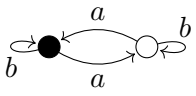
Look at the set of left cosets of G in F, and F acts on the left cosets. This gives the action of the generators $g_1, g_2, \ldots$ on the cosets. Pick one point, and call it the base point. This action determines a subgroup of index n of things fixing the base point. The number of subgroups of index n of F are in bijection with the connected graphs on n points with G-colored cycles.



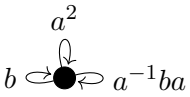
Free groups are the same as fundamental groups of connected graphs with a designated base point. The fundamental group is the set of homotopy classes of loops from the base point to itself, where loops follow the edges of the graph. Here, homotopy classes mean that two paths are equivalent if the difference between the two are just edges traversed that were immediately retraced backwards. The inverse of a path is the path traversed backwards.

The fundamental group of the graph containing 1 point with n loops to itself is the free group on n generators. Conversely, the fundamental group of any connected graph is a free group. Why? Pick an edge with distinct vertices; then we can contract the two points into one without changing the fundamental group. We can repeat this until there is only 1 point left, and we can then identify the fundamental group of the graph with a free group.

Example 8.1. Let G be a subgroup of index 2 of the free group on a, b.

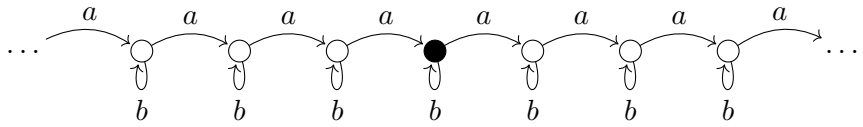


Contract the bottom edge, so we get a free group on 3 generators. What are these generators? Following the loops from the base point to itself, we get the generators b, a^2, and $a^{-1}ba$.



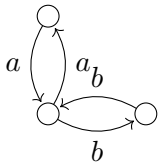
Not every subgroup of a finitely generated group is finitely generated.

Example 8.2. We will find a subgroup of the free group on 2 generators that is not finitely generated. Consider the following graph:

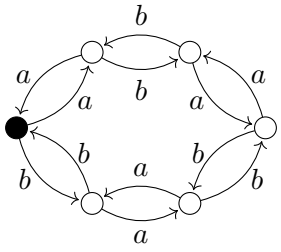


Contracting all the edges labeled a, we get 1 vertex with infinitely many loops going to itself. These loops are labeled with the generators $\left\{a^k b a^{-k} : k \in \mathbb{Z}\right\}$.

Example 8.3. Map the free group on two generators a, b to S_3 so a and b permute the vertices $\{1, 2, 3\}$ as follows:



S_3 is generated by a, b with the relations $a^2 = 1$, $b^2 = 1$, and $(ab)^3 = 1$. What is the kernel of this map? The kernel is a subgroup of index 6.



Contract along the inner edges to get the desired free group.

If G has index n in the free group on m generators, then the graph of F_m has Euler characteristic $1 - m$; the Euler characteristic of a graph is $|\text{vertices}| - |\text{edges}|$. The graph of G has n vertices and mn edges, so it has Euler characteristic $m - nm = n(1 - m)$. So the number of generators is $n(1 - m)$.

9 Rings

9.1 Definition and examples

Definition 9.1. A *ring* is a set R along with two binary operations, $+$ and $\times$, such that

1. R is an abelian group under $+$
2. $\times$ is associative
3. $a(b+c) = ab + ac$, $(a+b)c = ac + bc$.

We also have two optional axioms:

1. $\times$ has identity[12] 1 such that $1a = a1 = a$.
2. $ab = ba$ (commutative rings).

Example 9.1. The integers, $\mathbb{Z}$, are a ring.

Example 9.2. The Gaussian integers, $\mathbb{Z}[i] = \left\{m + ni : m, n \in Z, i^2 = -1\right\}$, are a ring.

Example 9.3. Polynomials over a field K, $K[x]$, are a ring.

Example 9.4. The set of $n \times n$ matrices with entries in K, $M_n(K)$, is a ring.

Example 9.5. The Burnside ring of a group $G = S_3$ is the set of all sums $\sum n_i A_i$ for $n_i \in \mathbb{Z}$ and A_i some transitive permutation representation of G (up to isomorphism). The 4 transitive permutation representations of S_3 are conjugacy classes: $\{1, (1\,2)\}$, $\{1, (1\,3)\}$, $\{1, (2\,3)\}$, $\{1, (1\,2\,3), (1\,3\,2)\}$. We get the adjoint representation on 6 points, 3 points, 2 points, and 1 point, so we get sums of the form $aA^1 + bA^2 + cA^3 + dA^6$.

Any permutation representation is the union of transitive ones. So the set of all finite permutation representations (up to isomorphism) is the elements of $aA^1 + bA^2 + cA^3 + dA^6$. This is not a ring, but we can force it to be by adding $-$.[13]

$+$ in this ring is the disjoint union of representations. $\times$ in this ring is the product of permutation representations. In particular, we have the multiplication table

$\times$	A^1	A^2	A^3	A^6
A^1	A^1	A^2	A^3	A^6
A^2	A^2	$A^2 \oplus A^2$	A^6	$A^6 \oplus A^6$
A^3	A^3	A^6	$A^3 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6$
A^6	A^6	$A^6 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6$	$A^6 \oplus A^6 \oplus A^6 \oplus A^6 \oplus A^6 \oplus A^6$

[12] It is sometimes common in analysis to consider rings that do not have an identity element.

[13] This is the same thing one does in the construction of the integers from the natural numbers. Doing this to any commutative monoid returns what is called the Grothendieck group.

9.2 Analogies between groups and rings

We can draw a parallel between groups and rings.

- A set S (in relation to groups) corresponds to the vector space with basis S (for rings).
- The symmetric group S_n (symmetries of $\{1, 2, \ldots, n\}$) corresponds to $M_n(K)$ (linear transformations of K^n).[14]
- We study G by making G act on some set. We study rings by making them act on K^n.
- Sets A, B have $A \amalg B$ and $A \times B$ with $a + b$ and ab elements, respectively. Given vector spaces V, W with respective dimensions a and b, $V \oplus W$ has dimension $a + b$; the tensor product[15] $V \otimes W$ has the property that if A is a basis for V and B is a basis for W, then $A \times B$ is a basis for $V \otimes W$, so $V \otimes W$ has dimension ab.
- $|A \cup B| = |A| + |B| - |A \cap B|$. Similarly, if V and W are vector spaces, $\dim(V \cup W) = \dim(V) + \dim(W) - \dim(V \cap W)$.

Remark 9.1. If $D = A \cup B \cup C$, then $|D| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$. This is not true for vector spaces. Let U, V, W be 2 dimensional vector spaces in $\mathbb{R}^3$ containing some fixed line.

9.3 Group rings

Definition 9.2. Let G be a group and R a commutative ring. The *group ring* $R[G]$ is the free abelian group with basis G, where $\times$ is the group operation on G extended linearly.

Example 9.6. Let G be the Klein 4 group $\{1, a, b, c\}$ with $a^2 = b^2 = c^2 = 1$, $ab = c$, ... So $\mathbb{C}[G]$ is a 4 dimensional vector space with basis a, b, c, d. It is a product of 4 copies of the ring $\mathbb{C}$.

Look at $e_1 = (1 + a + b + c)/4$, $e_2 = (1 + a - b - c)/4$, $e_3 = (1 - a + b - c)/4$, and $e_4(1 - a - b + c)/4$. Any product of two different ones of these is 0 and all have square themselves. This is $e_i e_j = 0$(if $i \neq j$) and $e_i^2 = e_i$. This latter statement says that the e_i are *idempotent*.

More generally, for a ring R, suppose $e \in R$ is idempotent. Then $R = eR \oplus (1 - e)R$, both of which are rings. Conversely, in $A \times B$, $(1, 0)$ is idempotent. So the presence of idempotents is equivalent to the ring splitting as a product.

[14] S_n is the Weyl group of $GL_n(K)$

[15] In older texts, this is sometimes referred to as the Kronecker product.

Example 9.7. Let G be the monoid $G = \mathbb{N}$. Then $\mathbb{Z}[G]$ is still a ring if we take our basis to be $x^0, x^1, x^2, \ldots$. This makes $Z[G] = \left\{n_0x^0 + n_1x^1 + n_2x^2 + \cdots\right\}$, the polynomial ring. If we take $G = \mathbb{Z}$, we get the Laurent polynomials in $\mathbb{Z}$.

9.3.1 An alternative description of $R[G]$

We can think of elements of $R[G]$ as functions from $G \to R$, where $f(g_i) = r_i$. Then the product of $R[G]$ is given by $fh(g) = \sum_{g_1g_2=g} f(g_1)h(g_2)$, which is called the convolution of f and h.

Let $G = \mathbb{R}$, which is not finite. Consider the ring of all compactly supported continuous functions f. Then $f * h(x) = \int f(y)h(x-y)\,dy$, another type of convolution. This is a ring under convolution, but it does not have an identity element for convolution.[16]

9.4 Ideals

Ideals correspond to normal subgroups (kernels of homomorphisms). We define ideals by the properties we need for the kernel of a homomorphism.

Definition 9.3. An ideal I of a ring R is a subset of R such that

1. I contains 0_R and is closed under addition and subtraction (I is a normal subgroup of R with respect to addition)
2. If $r \in I$ and $t \in R$ then $rt, tr \in I$ (stronger than saying that I is closed under $\times$).

We must check that the two conditions above are sufficient. Suppose I satisfies these. Can we form R/I? Addition is well defined since I is a normal subgroup of R with respect to addition. To see if multiplication is well defined, we first define multiplication to be $(aI)(bI) = (ab)I$. We want that if $a \equiv b$ ($a - b \in I$) and $c \equiv d$ ($c - d \in I$), then $ac \equiv bd$ ($ac - bd \in I$). Let $b = a + i_1$ and $d = c + i_2$. Then

$$ac - bd = ac - (a + i_1)(c + i_2) = ac - ac - i_1c - i_2a - i_1i_2 = -(\underbrace{i_1c}_{\in I} + \underbrace{i_2a}_{\in I} + \underbrace{i_1i_2}_{\in I}).$$

If S is any subset of a ring R, we can force S to be 0 by taking the smallest ideal $I \supseteq S$. In this case, I is the set of finite sums of the form $\sum_{s_i \in S} r_i s_i t_i$ with $r_1, t_i \in R$.

9.5 Generators and relations

We form a free ring on a set S. We have 2 choices:

[16] The Dirac δ distribution is actually an identity for convolution for a larger ring than this.

1. Free commutative ring: First form the free commutative monoid on S. If $S = \{x, y, z\}$, then this is $\{x^{n_1}y^{n_2}z^{n_3} : n_i \in \mathbb{N}\}$ The free commutative ring is the ring $\left\{n_{a,b,c}x^a y^b z^c : a, b, c \geq 0\right\}$.

   Say we have the elliptic curve $y^2 = x^3 - x$. We can form the coordinate ring $Z[x, y]/(y^2 - x^3 + x)$, where we are quotienting out by the ideal generated by $y^2 - x^3 + x$.

2. Noncommutative free ring: Take the noncommutative free monoid on $\{x, y, z\}$. This is all words in $\{x, y, z\}$. The noncommutative free ring is the group ring of the free monoid.

   Now we can construct rings such as $Z[x, y, z]/(x^2 + y^2z - zy^2)$ (some ideal generated by some elements), which is noncommutative.

Example 9.8. Suppose A and B are rings. We can construct the coproduct as follows: assume $A \cap B = \varnothing$, and form the free ring F on the set $A \cup B$. Quotient out by an ideal to force the map from $A \to F$ to be a homomorphism; we have $I = (f(a + b) - f(a) - f(b), f(ab) - f(a)f(b) \forall a, b, \in R)$ and so on (including all the relations we want). Then F/I is the coproduct of A and B.

Example 9.9. The coproduct of $Z[x]$ and $Z[y]$ in the category of rings is the free noncommutative ring on x, y. However, the coproduct of $Z[x]$ and $Z[y]$ in the category of commutative rings is the polynomial ring $Z[x, y]$.

10 Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

10.1 Euclidean Domains and Principal Ideal Domains

10.1.1 Euclidean Domains

Recall that every integer $\neq 0$ is a product of primes in an essentially unique way. $12 = 2 \times 2 \times 3 = 2 \times 3 \times 2 = (-2) \times (-3) \times 2$. So the product is unique up to order and multiplication by *units*.

This was essentially proved by Euclid. The key point he used was division with a remainder. That is, given a, b with $a \neq 0$, we can write $a = bq + r$, where r is smaller than b. Here, q is called the quotient, and r is the remainder.

What does smaller mean in this context? For integers, this means $|r| < |b|$. We can do the same thing for polynomials $a, b \in \mathbb{R}[x]$; a smaller than b means that $\deg(a) < \deg(b)$ (or $a = 0$).

Definition 10.1. A commutative ring R is a *Euclidean domain* if it has a function $|\cdot| : R \to \mathbb{N}$ such that given a, b with $b \neq 0$, we can find r, q such that $a = bq + r$ and $|r| < |b|$.[17]

Example 10.1. Let $Z[i] = \left\{a + bi : a, b \in \mathbb{Z}, i^2 = -1\right\}$ be the Gaussian integers. $Z[i]$ is a Euclidean domain. Define $|a + bi| = a^2 + b^2$. This is the usual Euclidean norm but squared to make sure we get an integer. Given a, b, we need to find r, q such that $a = bq + r$, which means $a/b = q + r/b$, where $|r/b| < 1$. Given any a/b, we can find $q \in Z[i]$ of distance < 1 from a/b. Draw an open disk of radius 1 around each elements of $Z[i]$. These cover $\mathbb{C}$, so we can find r, q.

10.1.2 Principal Ideal Domains

Definition 10.2. The *ideal generated by elements* $g_1, g_2, \dots$ is the smallest ideal containing these elements.

We denote $(a, b, c, \dots)$ as the ideal generated by $a, b, c \dots$.

Definition 10.3. A *principal ideal domain* is a commutative ring where all ideals are generated by one element.

Example 10.2. $\mathbb{Z}$ is a principal ideal domain. In $\mathbb{Z}$, we only have ideals of the form $n\mathbb{Z}$.

Example 10.3. Here is an example of a commutative ring that is not a PID. Let $R = \mathbb{C}[x, y]$, and let $I = (x, y)$ be the set of all polynomials with constant term 0. If $I = (f)$, then f divides x and f divides y. This means $f = 1$, but $1 \notin (x, y)$.

[17] We don't actually need the codomain of the norm function to be $\mathbb{N}$; we just need it to be a well-ordered set. In practice, however, the useful examples are all with sets that are basically $\mathbb{N}$.

Theorem 10.1. *Euclidean domains are principal ideal domains.*

Proof. Let I be any ideal. Choose $a \in I$ with $a \neq 0$ and $|a|$ minimal. Then we claim that $I = (a)$. Suppose $b \in I$. Then $b = aq + r$ with $|r| < |a|$. So $r = b - aq$ means that $r \in I$, and the minimality of $|a|$ forces $r = 0$. So $b = aq$ for some q, and this holds for any $b \in I$, so $I = (a)$. □

Example 10.4. $R = \mathbb{Z}[(1 + \sqrt{-19})/2]$ is a PID that is not Euclidean. R is a PID; for proof, see an algebraic number theory course. Here is a sketch that R is not Euclidean. Let $a \in R$ be nonzero and not a unit, with $|a|$ minimal. Then look at $R/(a)$. If $b \in R$, $b = aq + r$ with $|r| < |a|$. Then r is 0 or a unit. So every element of $R/(a)$ is represented by 0 or a unit. The only units of R are ± 1, so $R/(a)$ has ≤ 3 elements. If $a \neq \pm 1, 0$, then $R/(a)$ has ≥ 4 elements (actually $|a|^2$).

10.2 Unique factorization domains

10.2.1 Definitions and relationship to principal ideal domains

Definition 10.4. Let $a, b \in R$. We say a *divides* b (denoted $a|b$) if there exists some $c \in R$ such that $ac = b$.

Definition 10.5. An element a is called *irreducible* if $a \neq 0$, a is not a unit, and $a = bc$ implies that either b or c is a unit.

Definition 10.6. An element a is called *prime* if $a|bc$ implies that $a|b$ or $a|c$.

For $\mathbb{Z}$, these two definitions are equivalent, but this is not the case in all rings.

Lemma 10.1. *In a principal ideal domain, irreducible elements are prime.*

Proof. Suppose p is irreducible and $p|ab$. We want to show that $p|a$ or $p|b$. Suppose that $p \not| a$. Then $(p, a) = (c)$ since R is a principal ideal domain. Then $c|p$, so c is a unit or is a unit times p. The second case is not possible because $pu = c$ divides a, but a is not divisible by p. So (c) contains 1 (by multiplying c by c^{-1}) and is then equal to R. So $(p, a) = (1) = R$.

We now have $px + ay = 1$ for some $x, y \in R$, which makes $pbx + aby = b$. Both terms are divisible by p, so $p|b$. Hence, p is prime. □

Definition 10.7. A *unique factorization domain* is a commutative ring in which every element can be uniquely expressed as a product of irreducible elements, up to order and multiplication by units.

Theorem 10.2. *Every principal ideal domain is a unique factorization domain.*

Proof. We first show existence of factorization into irreducibles. Given $a \in R$, first find irreducible p dividing a if a is not a unit. Let $a = bc$; if b is irreducible, stop. Otherwise, let $b = de$, and repeat the process until we get an irreducible element. Can this go on forever? No. Suppose we have $a, b, c, d, e, \dots$ with $a = b'b$, $b = c'c$, etc., where $b', c', \dots$ are not units. Then the ideal $(a, b, c, d, \dots) = (x)$, since we are in a PID. But then $x \in (a, b, c, d, e)$ (some finite sequence of the variables), so the sequence must stop after finitely many steps.

Now put $a = bc$ with b irreducible, $c = de$ where d is irreducible, $e = fg$, where f is irreducible and so on. This stops after a finite number of steps by a similar argument. So every nonzero element is a product of irreducibles.[18]

To prove uniqueness, suppose $a = p_1 \cdots p_m = q_1 \cdots q_n$ with p_i, q_j irreducible. We want to show that these factorizations are unique up to order and units. p_1 is irreducible, so p_1 divides some q_i as p_1 is prime. The q_i are irreducible, so $q_i = p_1 u$ for some unit $u \in R$. By removing p_1 and this q_i from their respective sides (really we are bringing the two products to the same side, factoring out the p_1, and asserting that the rest equals 0), we can repeat this to eventually get our result. □

Example 10.5. R be the set of polynomials in x^q for rational $q > 0$; this is a set of terms of elements like $3 + 3x^{5/7} + 2x^{17/3}$. This argument goes wrong here because $x = x^{1/2}x^{1/2} = x^{1/4}x^{1/4}x^{1/4}x^{1/4} = \cdots$. The ideal $(x^{1/2}, x^{1/4}, x^{1/8}, \dots)$ is not principal.

10.2.2 Examples and Applications

Example 10.6. Suppose $a + bi \in \mathbb{Z}[i]$ is prime. Then $(a + bi)(a - bi) = a^2 + b^2 \in Z$. So we can use this to factor elements in Z into elements in $\mathbb{Z}[i]$. For example, $5 = 2^2 + 1 = (2 + i)(2 - i)$.

$$65 = 5 \times 13 = (2 + i)(2 - i)(3 + 2i)(3 - 2i) = (4 + 7i)(4 - 7i) = (8 - i)(8 + i)$$

This gives us $65 = 4^2 + 7^2 = 8^2 + 1^2$. So the different factorizations of $x \in \mathbb{Z}$ in the Gaussian integers give us the ways to write x as a sum of two squares.

Example 10.7. Let $R = \mathbb{Z}[\sqrt{-2}]$. Imagine this as a rectangular lattice in $\mathbb{C}$. The circles of radius 1 around these points cover $\mathbb{C}$, so as we argued before with $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ is a euclidean domain and hence is a unique factorization domain.

Now let $R = \mathbb{Z}[\sqrt{-3}]$. The circles of radius 1 do not cover the point $1/2 + \sqrt{-3}/2$. In fact, R is not a unique factorization domain. We have $2 \times 2 = (1 + \sqrt{3}i)(1 - \sqrt{3}i)$, and the only units are ± 1. These are all irreducible elements. If $2 = ab$, then $|a|\,|b| = |2| = 2$, which means $|a| = \pm 1$ or $|b| = \pm 1$.

Multiplying $z \in R$ by a multiplies $|z|$ by $|a|$ and rotates z by $\arg(a)$. So a principal ideal in $\mathbb{Z}[\sqrt{-3}]$ looks like a rotated and rescaled rectangular lattice. What does a non-principal

[18] This is still true if R has the following property: there is no strictly increasing sequence of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$. These are called *Noetherian rings*.

ideal look like? Look at $(2, 1+\sqrt{-3})$; we get a "diamond" lattice instead of a rectangular one.

Unique factorization domains need not be principal ideal domains.

Example 10.8. $\mathbb{Z}[x]$ is a UFD and has the non-principal ideal $(2, x)$.

Example 10.9. Let K be a field. $K[x, y]$ is a UFD and has the non-principal ideal (x, y).

We will see later that if R is a UFD, then so is $R[x]$, the ring of polynomials over R.

Theorem 10.3 (Fermat)**.** *Any prime $p \in \mathbb{Z}$ with $p > 0$ and $p \equiv 1 \pmod 4$ can be uniquely expressed as $a^2 + b^2$ (up to sign differences in a, b).*

Proof. $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p - 1 = 4n$. It has an element -1 of order 2. Let g be a generator, so $g^{4n} = 1$. So $-1 \equiv g^{2n} \pmod p$, which means that -1 is a square mod p. This gives us that $-1 = a^2 - np$ for some n, a. So $np = a^2 + 1 = (a + i)(a - i)$ in $\mathbb{Z}[i]$. $p|(a + i)(a - i)$, but does not divide either of these two factors, so p is not prime and hence is not irreducible in $\mathbb{Z}[i]$. So $p = (a + bi)(a - bi)$ for some $a, b \in \mathbb{Z}$ (we must have this decomposition because $a + bi$ times any other number would not be purely real). This makes $p = a^2 + b^2$.

For uniqueness, suppose that $p = x^2 + y^2$. Then $p = (x + iy)(x - iy)$, which means $x + iy = u(a + bi)$ for some unit u because $Z[i]$ is a unique factorization domain. Then $x = \pm 1$ and $b = \pm b$. □

11 Prime Ideals and Maximal Ideals

11.1 Fields and integral domains

Definition 11.1. A *field* is a commutative ring where all nonzero elements have multiplicative inverses.

Definition 11.2. An *integral domain* is a ring where $ab = 0$ implies that $a = 0$ or $b = 0$.

Proposition 11.1. *All fields are integral domains.*

Proof. Let R be a field. Then for $a, b \in R$,

$$ab = 0 \implies a^{-1}ab = a^{-1}0 \implies b = 0. \qquad \square$$

Definition 11.3. Let I be an ideal of R. I is called *maximal* if R/I is a field.

Definition 11.4. Let I be an ideal of R. I is called *prime* if R/I is an integral domain. Equivalently, I is prime if $ab \in I$ implies that $a \in I$ or $b \in I$.

Why are these definitions equivalent?

$$\begin{aligned} R/I \text{ is an integral domain} &\iff [(a+I)(b+I) = I \implies a \in I \text{ or } b \in I] \\ &\iff [ab + I = I \implies a \in I \text{ or } b \in I] \\ &\iff [ab \in I \implies a \in I \text{ or } b \in I]. \end{aligned}$$

We can see by the previous proposition that all maximal ideals are prime.

Definition 11.5. An ideal $I \neq R$ is *maximal* if for any ideal J, $I \subseteq J$ implies that $I = J$ or $J = R$.

Proposition 11.2. *Let I be an ideal of a ring R. Then R/I is a field iff I is maximal.*

Proof. Suppose I is maximal. Since $I \neq R$, $1 \notin I$, so R/I contains an element $1 + I \neq I$. Letting $x + I \in R/I$, note that $I + Ax = R$, so there exists some $y \in I$ and $a \in R$ such that $y + ax = 1$. Then $ax + I = 1 + I$, so $(a + I)$ is the inverse of $x + I$ in R/I. So R/I is a field.

Conversely, suppose R/I is a field. Then for $x \notin I$, there exists some $a \notin I$ such that $ax + I = 1 + I$. Then $ax + y = 1$ for some $y \in I$, so $(1) \subseteq Ax + I$, which makes $Ax + I = R$. This holds for all $x \notin I$, so I is maximal. $\square$

Example 11.1. Let $R = \mathbb{Z}$. The ideals are of the form (n) for $n = 0, 1, 2, 3, \ldots$. The maximal ideals are $(2), (3), (5), (7), \ldots$. The prime ideals are $(0), (2), (3), (5), (7), \ldots$.

Example 11.2. Let $R = \mathbb{C}[x]$; this is a PID. The ideals are (f) for a polynomial f. The maximal ideals are $(x - a)$ for $a \in \mathbb{C}$ (any polynomial f of degree > 1 factorizes as $f = gh$, so $(f) \subsetneq (g)$, making (f) not maximal). The prime ideals are $(x - a)$ for $a \in \mathbb{C}$, and (0).

Example 11.3. Let $R = \mathbb{C}[x, y]$. The ideal (x, y) is maximal because $R/(x, y) = \mathbb{C}$, which is a field. The ideals $(x - a, y - b)$ are also maximal. These are the only maximal ideals.[19] The prime ideals are $(x - a, y - b)$, (0), and (f) if f is any irreducible polynomial; this is because $\mathbb{C}[x, y]/(f)$ is an integral domain because $\mathbb{C}[x, y]$ is a UFD.

11.2 Maximal ideals and Zorn's lemma

Definition 11.6. A *partial order* is a relation $\leq$ on a set S such that for all $a, b, c \in S$

1. $a \leq a$ (reflexivity).
2. If $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry).
3. If $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity).

Example 11.4. Let S be the set of subsets of some set T. The ordering $\leq$ is inclusion.

Definition 11.7. Let S be a partially ordered set. A *totally ordered* subset T of S is a subset such that for all $a, b \in T$, $a \leq b$ or $b \leq a$.

Definition 11.8. Let S be a partially ordered set. An *upper bound* of a subset T is an element $a \in S$ such that $b \leq a$ for all $b \in T$.

Definition 11.9. Let S be a partially ordered set. An element $a \in S$ is *maximal*[20] if $a \leq b$ implies that $b = a$.

Lemma 11.1 (Zorn)**.** *Suppose S is a nonempty partially ordered set such that for any totally ordered subset of S, there is an upper bound. Then S has a maximal element.*

Proof. We will sketch a proof because a full proof requires some set theory. Suppose no maximal element exists; we will find a contradiction.

Step 1: Pick $s_0 \in S$ since S is nonempty. Then $\{s_0\}$ is totally ordered, so it has an upper bound s_1. If s_0 is not maximal, then $s_1 > s_0$.

Step 2: Repeat this with $\{s_0, s_1\}$, which is totally ordered. And repeat this.

Step 3: We do this infinitely many times[21], and find s_ω, which is an upper bound of $\{s_0, s_1, s_2, \ldots\}$.

Step 4. We find an s_α for every ordinal α. But the set of ordinals is a proper class, so it must be bigger than S since S is a set. So we have a contradiction. □

Corollary 11.1. *If I is an ideal of R with $I \neq R$, I is contained in some maximal ideal.*

[19] See Hilbert's Nullstellensatz. This word means zero position theorem.

[20] You might think that maximal should mean that $b \leq a$ for all $b \in S$, but this is a very strong condition. This implies a unique maximal element, which is not true for our definition of maximality.

[21] Picking elements in this way requires the axiom of choice. As such, Zorn's lemma was somewhat controversial in the early 20th century.

Proof. Look at the set S of ideals $\neq R$ containing I. It is partially ordered by $\subseteq$ and is nonempty because it contains I. Now suppose I_α is a totally ordered set of ideals; then $\bigcup_\alpha I_\alpha$ is an ideal and is greater than I_α for each α. Why is this an ideal? The total ordering is key. If $a, b \in \bigcup_\alpha I_\alpha$, then $a \in I_{\alpha_1}$ and $b \in I_{\alpha_2}$; without loss of generality, $I_{\alpha_1} \subseteq I_{\alpha_2}$, so $a + b \in I_{\alpha_2}$. This is the upper bound needed to satisfy the conditions of Zorn's lemma. □

Remark 11.1. You may be wondering why we need Zorn's lemma. In general, there exist nonempty ordered sets with no maximal elements. For example, take the open unit interval, $(0, 1)$.[22]

Corollary 11.2. *The intersection of all prime ideals of a ring is the set of elements x with $x^n = 0$ for some n (called nilpotent).*

Proof. Let $\mathfrak{p}$ be a prime ideal. If $x^n = 0$, then $x^{n-1}x = x^n = 0 \in \mathfrak{p}$, so since $\mathfrak{p}$ is prime, $x^{n-1} \in \mathfrak{p}$ or $x \in \mathfrak{p}$, and so on, so $x \in \mathfrak{p}$.

Suppose x is not nilpotent; we need to find a prime ideal P not containing x. Let $M = \{1, x, x^2, \ldots\}$, which doesn't contain 0 because x is not nilpotent. Let S be the set of ideals disjoint from M. S is partially ordered by inclusion. S is nonempty because $(0) \in S$. Any totally ordered subset $\{I_\alpha\}$ of S has an upper bound $\bigcup_\alpha I_\alpha$. So, by Zorn's lemma, S has a maximal element I; I is maximal in S, not a maximal ideal.

I is prime. Suppose $a, b \notin S$. Then $(I, a) > I$, so it contains an element of M $x^n = i_1 + sa$. Likewise, (I, b) contains an element of M $x^n = i_2 + tb$. So $i_1 i_2 + i_2 sa + i_1 tb + stab = x^{m+n}$ is an element of M, and the first 3 terms on the left hand side are in I. So $ab \notin I$ because otherwise the right hand side of this equation would be an element of I, which is impossible because it is in M. So I is prime, as desired. □

12 Localization

12.1 What is localization?

The integers do not have division. This is inconvenient, so we construct the rational numbers $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}, n \neq 0\}$. $\mathbb{Q}$ is a field.

More generally, suppose R is a ring and S is a subset of R. We find a new ring $R[S^{-1}]$ so that all elements of S have inverses. This is localization.

Example 12.1. If R is an integral domain and S is the set of nonzero elements of R, then $R[S^{-1}]$ is a quotient field of R.

[22] Assuming that ordered sets always have a maximal element has been the cause of numerous philosophical blunders over the years, such as some attempted proofs of the existence of a god.

12.2 Construction

We may as well assume $1 \in S$ and S is closed under multiplication. If a, b have inverses, then ab should, as well. First, Assume S has no zero divisors. We basically copy the construction of $\mathbb{Q}$ from $\mathbb{Z}$.

Take all pairs (r, s) with $r \in R$ and $s \in S$. Call this r/s. We have an equivalence relation $r_1/s_1 \equiv r_2/s_2$ means $r_1 s_2 = r_2 s_1$. The subtle point of this construction is that we need to check that this equivalence relation is transitive.

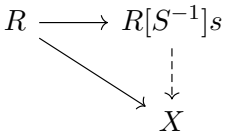
We first assume that S has no zero divisors. Suppose $r_1/s_1 \equiv r_2/s_2$ and $r_2/s_2 \equiv r_3/s_3$. We have $r_1 s_2 = r_2 s_1$ and $r_2 s_3 = r_3 s_2$. So $r_1 s_2 s_3 = r_2 s_1 s_3 = s_1 r_3 s_2$. This makes $s_2(r_1 s_3 = r_3 s_1) = 0$, and since s_2 is not a zero divisor, $r_1 s_3 = r_3 s_1$; i.e. $r_1/s_1 \equiv r_3/s_3$. The remaining step is to check that the equivalence classes form a ring. We leave this as an exercise.

In this case, we have the map $R \to R[S^{-1}]$ sending $r \mapsto r/1$. This map is injective because it has trivial kernel; $r/1 = 0/1$ means $1r = 0 \cdot 1 = 0$, which makes $r = 0$.

What if S has zero divisors? Then $r_1/s_1 \equiv r_2/s_2$ is not an equivalence relation. So let I be the ideal of all elements with $xs = 0$ for some $s \in S$. Check that this is an ideal. Now form R/I, and let $\bar{S}$ be the image of S in R/I. Then $\bar{S}$ has no zero divisors in R/I, so we can form $(R/I)[\bar{S}^{-1}]$ as before.

So we get a ring $R[S^{-1}]$ with the following properties:

1. There is a homomorphism from $R \to R[S^{-1}]$.
2. The images of all elements of S are invertible in $R[S^{-1}]$.
3. $R[S^{-1}]$ is the universal ring with these properties.



The kernel of the map $R \to R[S^{-1}]$ is I, the set of elements killed by something in S. Then $r_1/s_1 \equiv r_2/s_2$ can be defined as $\exists s_3$ such that $s_3(r_1 s_2 - r_2 s_1) = 0$.

12.3 Examples

Why is localization called localization?

Example 12.2. Let $R = \mathbb{C}[x]$, the set of polynomial functions on $\mathbb{C}$. Suppose we want to examine $0 \in \mathbb{C}$. What do the functions near 0 look like? An example is the rational functions that are nonsingular at 0; this is an approximation to all holomorphic functions in a neighborhood of 0. This is equal to $R[S^{-1}]$, where S is the set of polynomials that are nonzero at 0. The map $R \to R[S^{-1}]$ is injective but not surjective.

Example 12.3. Let R be the set of continuous functions on $\mathbb{R}$. Focus on the point $0 \in \mathbb{R}$. Look at the germs, functions that are equivalent in a neighborhood of 0. The ring of germs is $R[S^{-1}]$, where S is the set of functions that are nonzero at 0. Here, the map $R \to R[S^{-1}]$ is surjective but not injective.

You may have noticed that in these two examples, S was the complement of a prime ideal. In general, if p is any prime ideal, then the complement of p is multiplicatively closed.

Example 12.4. Let $R = \mathbb{Z}$, and suppose we are interested in (2). Let $S = \mathbb{Z} \setminus (2)$, the odd numbers. So we get a ring $\mathbb{Z}_{(2)}$, the rationals a/b with b odd. In general, let $R_p = R[S^{-1}]$, where S is the complement of a prime ideal p. The units of $\mathbb{Z}_{(2)}$ are rationals of the form a, b with a, b odd. 2 is a prime element of $Z_{(2)}$. Anly element of $Z_{(2)}$ equals $2^n u$ for some unit u and a unique $n \in \mathbb{N}$. So this is a UFD with only one prime: 2. We see that localizing at 2 "kills off" all primes other than 2.

13 Modules

13.1 Basic notions and examples

13.1.1 Modules and homomorphisms

Informally, a module M over a ring R is like a vector space but over a ring.

Definition 13.1. A *(left) module* M over a ring R is an abelian group with a map $R \times M \to M$ sending $(r, m) \mapsto r \cdot m$ such that for $r, s \in R$ and $x, y \in M$

1. $r \cdot (x + y) = r \cdot x + r \cdot y$.
2. $(r + s) \cdot x = r \cdot x + s \cdot x$
3. $(rs) \cdot x = r \cdot (s \cdot x)$
4. $1_R \cdot x = x$ (if R has 1).

A *right module* is the same thing, except the map is $M \times R \to R$, so the actions of R on M is on the right.

Definition 13.2. Let M be an R-module. A *submodule* N is a subgroup of M such that $r \cdot n \in N$ for each $r \in R$ and $n \in N$.

Definition 13.3. A homomorphism of modules M_1, M_2 is a map $f : M_1 \to M_2$ such that

1. $f(m_1 + m_2) = f(m_1) + f(m_2)$
2. $f(r \cdot m) = r \cdot f(m)$.

Better (but not standard) notation would be that homomorphisms of left modules should be written on the right (and vice versa for right modules). So we should write mf, not fm. This makes it so the second condition gives us that $(rm)f = r(mf)$, which gets rid of the needless switching of the order of r and f. We will alternate between the two notations.

Definition 13.4. Let M, N be modules over R. Then $\mathrm{Hom}_R(M, N)$ is the set of module homomorphisms from M to N.

If R is commutative, $\mathrm{Hom}_R(M, N)$ is an R-module.

Definition 13.5. An *endomorphism* of M is a homomorphism from M to itself.

Definition 13.6. A *bimodule* is a left module over one ring and a right module over another, where the left and right actions commute.

Example 13.1. R is an (R, R) bimodule.

13.1.2 Exact sequences of modules

Suppose we have the exact sequence

$$0 \to A \to B \to C \to 0.$$

Are the following two sequences exact?

$$0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C) \to 0$$

$$0 \leftarrow \mathrm{Hom}(A, N) \leftarrow \mathrm{Hom}(B, N) \leftarrow \mathrm{Hom}(C, N) \leftarrow 0$$

The answer is no.[23] Look at

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Then

$$0 \to \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})}_{=0} \xrightarrow{\times 2} \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})}_{=0} \to \underbrace{\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})}_{=\mathbb{Z}/2\mathbb{Z}} \not\to 0$$

$$\not 0 \not\leftarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \xleftarrow{\times 2} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \leftarrow \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \leftarrow 0.$$

Instead, we get exact sequences

$$0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C)$$

$$\mathrm{Hom}(A, N) \leftarrow \mathrm{Hom}(B, N) \leftarrow \mathrm{Hom}(C, N) \leftarrow 0.$$

We leave this as an exercise.

13.1.3 Examples of modules

Example 13.2. Vector spaces over fields are modules.

Example 13.3. Abelian groups are modules over $\mathbb{Z}$.

Example 13.4. Left ideals of R are the same as left submodules of a module R.

Example 13.5. Let G be a group acting on a set S. Form the vector space V over K with basis S, and form the group ring $K[G]$. G acts on V by acting on the basis elements. So V is a module over the ring $K[G]$.[24]

[23] The study of homological algebra is based on the fact that these sequences are not always exact in this way.

[24] The study of these modules is very important in representation theory.

Example 13.6. Suppose M is a left module over a ring R. Then $\mathrm{Hom}_R(M, M)$, the endomorphisms of M, is a ring, where the product is composition of endomorphisms. M is a right module over $\mathrm{Hom}_R(M, M)$. Furthermore, the right action of $\mathrm{Hom}_R(M, M)$ commutes with the left action of R on M (follows from the definition of a homomorphism). So M is a $\mathrm{Hom}_R(M, M)$ bimodule.

$\mathrm{Hom}_R(M, M)$ is analogous to the permutations of a set S. If we have a group, we can represent it as the permutations of the set S. Similarly, a ring is often studied as a subring of $\mathrm{Hom}_T(M, M)$ for some T-module M.

Example 13.7. Take an algebraic number field such as $\mathbb{Q}[i]$, where $i^2 = -1$. Think of $Q[i]$ as a vector space over $\mathbb{Q}$, and think of the ring $\mathbb{Q}[i]$ as endomorphisms of this vector space. So we can represent elements of $\mathbb{Q}[i]$ as matrices. Matrices are linear transformations of vector spaces or equivalently homomorphisms of modules.

Pick a basis of $\mathbb{Q}[i]$: $\{1, i\}$. The action of 1 is $1 \to 1$ and $i \to i$ and the action of u is $1 \to i$ and $i \to -1$. So we have the matrices

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

So $\mathbb{Q}[i]$ can be thought of as the matrices

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

with $a, b \in \mathbb{Q}$.

Look at the invariants of matrices, the trace and the determinant. Here, $\mathrm{tr}(a+bi) = 2a$, and $\det(a + bi) = |a + bi|$.

13.2 Free modules

Definition 13.7. The *direct sum* of modules M_α over R is the abelian group $\bigoplus M_\alpha$ with the action of R on each component α determined by the action of R on M_α.

Definition 13.8. A *free module* is a module that is a direct sum of copies of R.

In some sense, free modules are the simplest sort of module.

Example 13.8. Any vector space is a free module.

Example 13.9. $\mathbb{Z}$ is a free module over $\mathbb{Z}$. However, $\mathbb{Z}/2\mathbb{Z}$ is not free.

We want to define the *rank* of a free module as the number of copies of R in the sum. Is this well defined? We must check that if $R^m \cong R^n$, then $m = n$. However this is not always true. When is this true?

- This is true when R is a field.
- This is false if R is the 0 ring.
- This is true if R is commutative with $R \neq 0$.

  Pick a maximal ideal I in R and suppose $R^m \cong R^n$. Reduce mod I, so $(R/I)^m \cong (R/I)^n$ as modules over a field R/I. So $m = n$ because R/I is a field.
- This is sometimes true if R is not commutatative (see below).
- There exist rings $R \neq 0$ such that $R \cong R \oplus R$ as R modules (see below).

Example 13.10. Take $R = M_n(K)$, the $n \times n$ matrices over a field K, and suppose $R^a \cong R^b$. These are vector spaces of dimension an^2 and bn^2, respectively, so $a = b$.

Example 13.11. Here is an example of a ring $R \neq 0$ such that $R \cong R \oplus R$ as R modules. This is a possibly unsettling result. Homomorphisms from R^m to R^n can be identified with $m \times n$ matrices, as in linear algebra. If $R \cong R \oplus R$, we have a 1×2 invertible matrix!

Pick an abelian group A such that $A \cong A \oplus A$, such as $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$. Put $R = \mathrm{End}(A)$; in our example, this is the set of $\infty \times \infty$ matrices with only finitely many nonzero entries in each row. Then $R = \mathrm{Hom}(A, A) = \mathrm{Hom}(A, A \oplus A) = R \oplus R$.

So the rank of a free R-module is not necessarily well-defined.

13.3 Projective modules

Given a free module M, we can recover the underlying set S_M; this is via a forgetful functor F from the category of modules to the category of sets. Likewise, given a set S, we can form the free module M_S with basis S; this is also via a functor, F'. These functors commute with morphisms in the following way:

$$\begin{array}{ccc} M & \xrightarrow{F} & S_M \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle F(f)} \\ N & \xleftarrow[F']{} & S_N \end{array}$$

We say that the functors F and F' are *adjoint*. As a consequence, free modules are projective.

Definition 13.9. A *projective module* P is a module with the following property. If the sequence $M \to N \to 0$ is exact, then any map $P \to N$ lifts to a map $P \to M$.

$$\begin{array}{ccccc} M & \longrightarrow & N & \longrightarrow & 0 \\ & \nwarrow & \uparrow & & \\ & & P & & \end{array}$$

Proposition 13.1. *The following are equivalent:*

1. *P is projective.*
2. *$P \oplus Q$ is free for some module Q.*

Proof. (1) $\implies$ (2) : Pick a free module F so $\varphi : F \to P$ is onto. Then $F \to P \to 0$, so we can find a map $P \to F$.

$$\begin{array}{ccccc} F & \xrightarrow{\varphi} & P & \longrightarrow & 0 \\ & \nwarrow^{\cdots} & \uparrow{\scriptstyle \mathrm{id}} & & \\ & & P & & \end{array}$$

But then F splits as $P \oplus \ker(\varphi)$.

(2) $\implies$ (1): Exercise. □

Example 13.12. $R = \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, so $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3/Z$ are projective over $\mathbb{Z}/6\mathbb{Z}$ but not free.

Example 13.13. Let R be the ring of continuous functions on a circle S^1, and let $M = R$. Then we can think of M as continuous functions $S^1 \to S^1 \times \mathbb{R}$. M is sections of $S^1 \times \mathbb{R} \to S^1$, which equals the real valued functions on S^1. This is a *vector bundle*[25] over S.

Consider a Möbius band, and view it as a vector bundle over S^1, so each fiber is isomorphic to $\mathbb{R}$. Now define a module N to be the sections of this twisted vector bundle. Then N is projective but not free.

N is not free because the orientations of the fibers change as you go around S^1. It is projective because $N \oplus N = M \oplus M$. At each point of S^1, consider the normal bundle. Now take the orthogonal complement. So we get 2 Möbius bands so at each point, and their fibers intersect at every point. So we can think of $N \oplus N$ as the sum of 2 Möbius bands.

In effect, we can think of projective modules as "twisted free modules."

Example 13.14. Let $R = \mathbb{Z}[\sqrt{-5}]$; we can think of this as a rectangular lattice in $\mathbb{C}$. Let $M = (2, 1 + \sqrt{-5})$. The principal ideals here are rectangular with respect to this lattice picture. Non-principal ideals are diamond shaped. Principal ideals here are free modules, and nonprincipal ideals are not free.

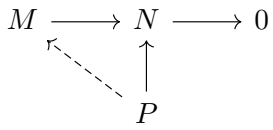
We want to show that M is projective, and we do so by showing that $M = R \oplus R$. We map $g : R \oplus R \xrightarrow{\text{onto}} M$ by sending $(1, 0) \mapsto 2$ and $(0, 1) \mapsto 1 + \sqrt{-5}$. We want to construct a section $f : M \to R \oplus R$, where $g(f(m)) = m$. So $R \oplus R = M \oplus \ker(g)$. Let $f(x) = (-x, x(1 + \sqrt{-5})/2)$, and check that $f(x) \in R \oplus R$. So M is projective.

[25] We won't be going over vector bundles in detail in this course. If you don't know what a vector bundle is, see a topology course.

14 More on Projective Modules

14.1 Projective modules as direct sums

Recall that P is a projective module if it satisfies the following commutative diagram for exact sequences of modules M and N:



We also showed that P projective iff $P \oplus Q$ is free for some Q. Are all submodules of free modules projective? The answer is no.

Example 14.1. Here is a non-projective submodule of a free module. Let $R = K[x, y]$, where K is a field, and let $I = (x, y)$, the ideal of polynomials with constant term 0. Look at $R \oplus R \xrightarrow{g} I \to 0$ where $(1, 0) \mapsto x$ and $(0, 1) \mapsto y$. If I is projective, then there exists some map $f : I \to R \oplus R$ such that $gf(a) = a$. Now suppose that $f(x) = (a, b)$ and $f(y) = (c, d)$. Then $ax + by = x$ and $cx + dy = y$. Then $y(a, b) = x(c, d))$, so $ya = xc$ and $yb = xd$. There are no polynomials satisfying this because $ax + by = x$ implies that $a = 1 + yp$ (where p is a polynomial), and $ya = xc$ implies that a cannot be $1 + yp$.

14.2 Eilenberg-Mazur swindle

This is a technique useful for proving $1 = 0$. Here is a basic example.

Example 14.2. Start with $1 + (-1) = 0$. Then

$$0 = (1 + (-1)) + (1 + (-1)) + \cdots$$

$$1 = 1 + (-1 + 1) + (-1 + 1) + \cdots,$$

so we have shown that $1 = 0$.

We assumed two things in the above example:

1. 1 has an additive inverse -1.
2. All infinite sums make sense.

The second condition is violated in $\mathbb{Z}$, but we can use this technique to show that one of these two conditions does not hold.

Example 14.3. Knots have no inverse. Suppose we have a closed loop with a knot in it. Is there another knot we can put on the loop that will cancel out the first knot? The answer is no. Apply the swindle: add infinite numbers of knots, making each successive knot smaller so the knots all fit on the loop. Then the above contradiction would occur, so a knot must not have an additive inverse.

Example 14.4. Suppose P is projective. Then $P \oplus Q = F$, where F is free. Then Q is also projective. We can take Q to be free (in fact equal to F). Think of free modules as 0 in some sense. So $P \oplus Q$ is free means that Q is a sort of additive inverse of P (again, if we ignore free modules). So infinite sums are defined, and we can use the swindle to get that $P = 0$ if we ignore free modules. What we mean here is that $P \oplus Q$ is free for some free module Q. The catch is that this free module Q is not finitely generated.

15 Tensor Products

This is covered in Chapter XVI in Lang, but we will cover it here. This is something you really should know.

15.1 Construction and universal property

Definition 15.1. A *bilinear* map $f : X \times Y \to Z$ is a map such that $f(\cdot, y)$ is linear for fixed y and $f(x, \cdot)$ is linear for fixed x.

Definition 15.2. Suppose R is a commutative[26] ring, and suppose that M and N are R-modules. The *tensor product* $M \otimes N$ is the module such that if $f : M \times N \to P$ is bilinear, then there exists a linear map $\tilde{f} : M \otimes N \to P$ such that the following diagram commutes

$$\begin{array}{ccc} M \times N & \xrightarrow{\varphi} & M \otimes N \\ & \searrow^{f} & \downarrow \tilde{f} \\ & & P \end{array}$$

To construct $M \otimes N$, take the free module on elements $m \otimes n$ with $m \in M$ and $n \in N$. We get linear maps from this to $P : m \otimes n \mapsto f(m, n)$. Take the quotient by all elements of the form

$$(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n$$
$$m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2$$
$$(rm) \otimes n - r(m \otimes n)$$
$$m \otimes (rn) - r(m \otimes n).$$

Taking the quotient by these elements enforces relations we want, such as

$$(rm) \otimes n = r(m \otimes n) = m \otimes (rn),$$

so the tensor product exists.

[26] This assumption is not necessary, but it simplifies things for now.

Now that we have constructed the tensor product, what does it look like? We have the identity

$$(M_1 \oplus M_2) \otimes N \cong (M_1 \otimes N) \oplus (M_2 \otimes N),$$

which says that a bilinear map $(M_1 \oplus M_2) \otimes N \to P$ is the same as a pair of bilinear maps from $(M_1 \otimes N) \to P$ and $(M_2 \otimes N) \to P$. Similarly, we have the identity

$$R \otimes M \cong M,$$

which says that bilinear maps $R \times M \to P$ are the same as linear maps from $M \to P$.

Example 15.1.

$$R^m \otimes R^n \cong R^{m+n}$$

If V, W are vector spaces with bases $\{v_i\}$ and $\{w_j\}$, then $V \otimes W$ has basis $v_i \otimes w_j$.

15.2 Exact sequences and the tensor product

Proposition 15.1. *Suppose $A \to B \to C \to 0$ is exact. Then so is*

$$A \otimes M \to B \otimes M \to C \otimes M \to 0.$$

Remark 15.1. This does not hold if we put a $0 \to$ before both of these sequences. We say that $\otimes M$ is *right exact*.

Proof. To prove things about the tensor product, forget the construction of the tensor product using relations and instead use the universal property.

Homomorphisms $A \otimes B \to C$ are bilinear maps $A \times B \to C$, which are linear maps $A \to \mathrm{Hom}_R(B, C)$. Think of this as an analogue of the fact that functions $R \times S \to T$ are the same as functions from R to the set of functions from S to T.

The key point of this proof is that $A \to B \to C \to 0$ is exact if and only if

$$\mathrm{Hom}(A, M) \leftarrow \mathrm{Hom}(B, M) \leftarrow \mathrm{Hom}(C, M) \leftarrow 0$$

is exact. We leave this as an exercise.[27]

We want to show that $A \otimes N \to B \otimes N \to C \otimes N \to 0$ is exact. Then this is equivalent to the following sequence being exact:

$$\mathrm{Hom}(A \otimes N, M) \leftarrow \mathrm{Hom}(B \otimes N, M) \leftarrow \mathrm{Hom}(C \otimes N, M) \leftarrow 0.$$

Then, using our identification of homomorphisms $A \otimes N \to M$ with linear maps $A \to \mathrm{Hom}_R(N, M)$, this is equivalent to the following sequence being exact:

$$\mathrm{Hom}(A, \mathrm{Hom}(N, M)) \leftarrow \mathrm{Hom}(B, \mathrm{Hom}(N, M)) \leftarrow \mathrm{Hom}(C, \mathrm{Hom}(N, M)) \leftarrow 0.$$

And this is exact by applying the key point again. □

[27] This was an exercise from last lecture, but Professor Borcherds suspects that no one actually does them.

We can now calculate $M \otimes N$. Pick $R^a \to R^b \to M \to 0$, where R^a, R^b are free. Pick relations generating $\ker(R^b \to M)$ and pick a set of b generators of M. Tensoring with N gives us that

$$R^a \otimes N \to R^b \otimes N \to M \otimes N \to 0$$

is exact. So we get

$$N^a \to N^b \to M \otimes N \to 0,$$

which makes $M \otimes N = N^b / \operatorname{im}(N^a \to N^b)$.

Example 15.2. We can find $M \otimes N$ for finitely generated abelian groups M, N. Recall that finitely generated abelian groups are direct sums of copies of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. Since $(A \oplus B) \otimes C = (A \otimes C) \oplus (B \otimes C)$, it is enough to work out a few cases:

1. $\mathbb{Z} \otimes \mathbb{Z} = \mathbb{Z}$
2. $\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}.m\mathbb{Z}$
3. $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$
4. $\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(\gcd(m,n)\mathbb{Z})$.

To obtain this last result, take the exact sequence

$$\mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0.$$

Then the sequence

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}) \to 0$$

is exact, so

$$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/m(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(\gcd(m,n)\mathbb{Z}).$$

Example 15.3.

$$\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$$

$$\mathbb{Z}/9\mathbb{Z} \otimes \mathbb{Z}/12\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$$

The tensor product is not left exact. Look at $0 \to \mathbb{Z} \xrightarrow{\times 2} Z \to \mathbb{Z}/2\mathbb{Z} \to 0$. The following sequence is not exact:

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

15.3 More examples and properties

Definition 15.3. An *algebra* S over a ring R is a commutative ring with a homomorphism $R \to S$ that makes S an R-module.

You can think of algebras as modules with multiplication.

Example 15.4. Let S, T be algebras over R. Then $S \otimes_R T$ is a push-out of S, T over R.

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ T & \longrightarrow & S \otimes_R T \end{array}$$

Check that $S \otimes_R T$ is a commutative ring. We need a bilinear map $(S \otimes T) \times (S \otimes T) \to (S \otimes T)$. This is a linear map from $S \otimes T \otimes S \otimes T \to S \otimes T$. This relies on associativity of the tensor product; $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$ because maps from each to M are trilinear maps $A \times B \times C \to M$. We have a map $S \otimes S \to S$ given by the product on S. Same for $T \otimes T \to T$. So we get a map $S \otimes T \otimes S \otimes T \to S \otimes S \otimes T \otimes T \to S \otimes T$ by sending $(s_1 \otimes t_1) \times (s_2 \otimes t_2) \to s_1 s_2 \otimes t_1 t_2$. We leave verification of the pushout property as an exercise.

Example 15.5. $S = K[x]$ and $T = K[y]$ with bases $\{x^m\}$ and $\{y^n\}$, respectively. $S \otimes_R T$ has a basis $x^m \otimes y^n$. This can be identified as as the polynomial ring $K[x, y]$ via the map $x^m \otimes y^n \to x^m y^n$.

Example 15.6. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is a ring. $\mathbb{C}$ has basis $\{1, i\}$, so $\mathbb{C} \otimes \mathbb{C}$ has basis $\{1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i\}$. Calculating a few products, we get

$$(i \otimes i)(i \otimes i) = i^2 \otimes i^2 = -1 \otimes -1 = 1 \otimes 1$$

$$(1 \otimes 1)(a \otimes b) = (a \otimes b)$$

$$(1 \otimes 1 + i \otimes i)^2 = 2(1 \otimes 1 + i \otimes i).$$

Call $e = (1 \otimes 1 + i \otimes i)/2$. Then $e^2 = e$, so e is idempotent. Then this ring splits as a product, so $\mathbb{C} \otimes \mathbb{C} = e(\mathbb{C} \otimes \mathbb{C}) \times (1 - e)\mathbb{C}(\mathbb{C} \otimes \mathbb{C}) \cong \mathbb{C} \times \mathbb{C}$.

Example 15.7. The tensor product satisfies all the axioms of a commutative *semiring* (a ring but without subtraction)

1. $(A \otimes B) \otimes C$
2. $(A \oplus B) \otimes C \cong (A \otimes C) \oplus (B \otimes C)$
3. $A \otimes B \cong B \otimes A$

4. $A \oplus B \cong B \oplus A$
5. $(A \oplus B) \oplus C \cong A \oplus (B \oplus C)$
6. $R \otimes A \cong A$.

If we want to construct a ring out of this structure, we have a few problems:

1. The set of all modules is not a set.
2. There is no subtraction.

   This can be circumvented by constructing the set of all pairs $M - N$ for M, N modules under some equivalence relation.
3. By the swindle, $M = 0$ for any M.

We circumvent problems 1 and 3 by only considering finitely generated modules.[28]

Example 15.8. Take $R = \mathbb{Z}$, the integers. The finitely generated modules are all of the form $\mathbb{Z}^n \oplus (\mathbb{Z}/2\mathbb{Z})^{n_2} \oplus (\mathbb{Z}/4\mathbb{Z})^{n_4} \oplus (\mathbb{Z}/8\mathbb{Z})^{n_8} \oplus \cdots \oplus (\mathbb{Z}/3\mathbb{Z})^{n_3} \oplus \cdots$. So we get a basis $\{n_i b_i\}$, where we allow the n_i to be positive or negative. The product is $b_0 \times b_n = b_n$ and $b_{p^a} \times b_{p^b} = b_{p^{\min(a,b)}}$.

15.4 Tensor products of noncommutative rings

When R is a noncommutative ring, $M \otimes_R N$ is only defined for M a right module and N a left module. This is because we need

$$(mr) \otimes n = m \otimes (rn).$$

Secondly, $M \otimes_R N$ is only an abelian group, not an R-module. We have that

$$mr \otimes n = m \otimes rn,$$

but multiplying by s gives us

$$mrs \otimes n = m \otimes srn,$$

even though we want $m(rs) \otimes n = m \otimes (rs)n$.

[28] This leads into K-theory, where you consider the ring of finitely generated modules over a ring R.

16 Duality

16.1 Notions of duality for algebraic objects

16.1.1 Duality of vector spaces

Definition 16.1. Let V be a vector space over a field K. Then we have the *dual vector space*, $V^* = \mathrm{Hom}(V, K)$.

Recall from linear algebra that we have a natural map $V \to V^{**}$ taking $v \mapsto (f \mapsto f(v))$ for $f \in Hom(V, k)$. Additionally, V^* is isomorphic to V if $\dim(V) < \infty$, but there is no natural isomorphism. This does not hold in the general case; if $V = \bigoplus_{n=1}^{\infty} K$, then V has countable dimension, but $\dim(V^*)$ is uncountable.

More generally, for objects in a category, we pick a "dualizing object," and let the dual be the set of homomorphisms to that object.

16.1.2 Duality of free modules

For free modules over a ring R, we take the dualizing object to be R. Then $M^* = \mathrm{Hom}(M, R)$, and $M^{**} \cong M$ if $M \cong \mathbb{R}^n$. This also holds if M is projective. We have $M \oplus N$ is free, so $M \oplus N \cong (M \oplus N)^{**}$; then it is not difficult to obtain the property for M.

16.1.3 Duality for finite abelian groups

Since abelian groups are modules over $\mathbb{Z}$, one might think that you should make $\mathbb{Z}$ the dualizing object, but the only homomorphism from $G \to \mathbb{Z}$ is the trivial one. So make the dualizing object $\mathbb{Q}/\mathbb{Z}$.

Proposition 16.1. *Let G be a finite abelian group. Then $G \cong G^*$.*

Proof. G is a direct sum of cyclic groups, so it is enough to check for when is G cyclic. Whe have $G \cong \mathbb{Z}/n\mathbb{Z}$, which means that $G^* = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \{q\mathbb{Z} \in \mathbb{Q}/\mathbb{Z} : n(q\mathbb{Z}) = \mathbb{Z}\} = \{0, 1/n, 2/n, \ldots, (n-1)/n\}$. This is cyclic of order n. □

We also get that $G \cong G^{**}$, and this isomorphism is considered natural.

16.2 Applications of duality

16.2.1 Dirichlet characters

Definition 16.2. A *Dirichlet character* is an element of the dual of $(\mathbb{Z}/N\mathbb{Z})^*$, the group of units[29] of the ring $\mathbb{Z}/N\mathbb{Z}$.

[29] We are being sloppy here by using $*$ to both mean dual and the group of units. In the case of $((\mathbb{Z}/N\mathbb{Z})^*)^*$, we mean $\mathrm{Hom}((\mathbb{Z}/N\mathbb{Z})^*, S^1)$.

Replace $\mathbb{Q}/\mathbb{Z}$ by S^1, unit circle in the complex numbers. We have the map $\mathbb{Q}/\mathbb{Z} \to S^1$ sending $x \mapsto e^{2\pi i x}$, so $\mathbb{Q}/\mathbb{Z} \cong$ elements of finite order in S^1.

Example 16.1. For $N = 8$, $(\mathbb{Z}/N\mathbb{Z})^* = \{1, 3, 5, 7\}$ with $1^2 = 5^2 = 7^2 = 1$. The characters are

	1	3	5	7
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	1	-1	-1
χ_3	1	-1	-1	1

Dirichlet was interested in this because he defined the Dirichlet L-function

$$\sum_{n \geq 1} \frac{\chi(n)}{n^s},$$

where χ is a Dirichlet character. When $N = 1$ and χ is the trivial character, we get the RIemann Zeta function.

Definition 16.3. Let χ_1, χ_2 be Dirichlet characters for the same N. Then the *inner product* of χ_1, χ_2 is

$$(\chi_1, \chi_2) := \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \chi_1(x)\overline{\chi_2(x)}.$$

Proposition 16.2. *Dirichlet characters are orthogonal.*

Proof. Let $\chi_1 \neq \chi_2$, and define the homomorphism $\chi = \chi_1\overline{\chi_2}$. Then $(\chi_1, \chi_2) = (\chi, 1)$, where 1 is the trivial character (sends everything to 1). Since $\chi_1 \neq \chi_2$, $\chi \neq 1$, so let $a \in \mathbb{Z}/N\mathbb{Z}$ with $\chi(a) \neq 1$. Then

$$\sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(x) = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(ax) = \chi(a) \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(x),$$

where multiplying by a just reindexes the elements of $\mathbb{Z}/N\mathbb{Z}$. So we have

$$(\chi_1, \chi_2) = (\chi, 1) = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^*} \chi(x) = 0. \qquad \square$$

16.2.2 The Fourier transform

Definition 16.4. Suppose f is a complex function on a finite group G. The Fourier transform $\tilde{f}$ is a function on G^*

$$\tilde{f}(\chi) = (\chi, f) = \sum_{x \in G} \chi(x) f(x).$$

Duality for infinite abelian groups (with a topology) follows a few rules:

1. The dualizing object is S^1.
2. Groups should be locally compact
3. Homomorphisms should be continuous.

Example 16.2. Let $G = \mathbb{Z}$. Then $G^* = \mathrm{Hom}(\mathbb{Z}, S^1) \cong S^1$. Let $H = S^1$. Then H^* is the continuous homomorphisms from $S^1 \to S^1$ ($z \mapsto z^n$ for $n \in Z$). These two groups are dual to each other.

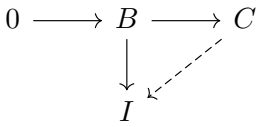
The fourier transform takes function on S^1 to a fourier series (a function on $\mathbb{Z}$) by sending

$$f \mapsto \sum_n c_n e^{2\pi i n z}, \qquad c_n = \int_{z \in S^1} e^{-2\pi i n z} f(z)\, dz.$$

If $G = \mathbb{R}$, then $G^* = \mathrm{Hom}(\mathbb{R}, S^1) \cong \mathbb{R}$. This gives the fourier transform on $\mathbb{R}$.

16.2.3 Existence of "enough" injective modules

Definition 16.5. An *injective module* I is a module with the following property. If the sequence $0 \to B \to A$ is exact, then any map $B \to I$ induces a homomorphism $A \to I$.



It is not immediately clear how we can find injective modules. The first step is to find a divisible abelian group.

We want to say that every module is a submodule of an injective module.

Definition 16.6. A group G is *divisible* if given $g \in G$ and $n \in \mathbb{Z}^+$, there exists some $h \in G$ with $nh = g$.

Example 16.3. $\mathbb{Q}/\mathbb{Z}$ is a divisible abelian group.

Finitely generated abelian groups are never divisible, except for the trivial group.

Proposition 16.3. *Let I be a module. If it is divisible as an abelian group, it is injective as a module.*

Proof. Pick $a \in A$ with $a \notin B$. We want to extend f to a. Pick the smallest $n > 0$ so that $na \in B$ if n exists. Extend f to a by putting $f(a) = g$, where $g \in I$ satisfies $ng = f(x)$. If n does not exist, then put $f(a)$ equals anything (it doesn't matter what we put here). Now extend f to all of A using Zorn's lemma (choose the maximal extension from submodules of A to I). □

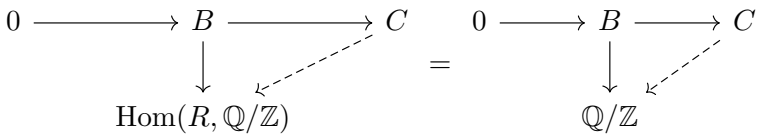
Proposition 16.4. *Every abelian group is contained in an injective module.*

Proof. By the previous proposition, $\mathbb{Q}/\mathbb{Z}$ is injective, and given an abelian group G with an element $a \neq 0$ in G, we can find a homomorphism $f : G \to \mathbb{Q}/\mathbb{Z}$ such that $f(a) \neq 0$. So any abelian group G is a subset of a (possibly infinite) product of $\mathbb{Q}/\mathbb{Z}$s. □

Proposition 16.5. *Let R be a ring. Then the dual R^* is an injective R-module*

Proof. The key point is that $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ is an injective R-module. This is the dual of R as a $\mathbb{Z}$-module. Be careful; $\mathbb{Q}/\mathbb{Z}$ is a $\mathbb{Z}$-module but not necessarily an $\mathbb{R}$-module. If $f \in \mathrm{Hom}(R, \mathbb{Z})$ and $r, s \in R$, define fr by $fr(x) = f(rs)$ This makes $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ a right R-module.

The second key point is that $\mathrm{Hom}_R(M, \mathrm{Hom}(R, \mathbb{Q}/\mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$; this is easy but confusing to actually write out, so we leave it as an exercise. So finding an induced homomorphism from $A \to \mathrm{Hom}(R, \mathbb{Q}/\mathbb{Z})$ is the same problem as finding an induced homomorphism from $A \to \mathbb{Q}/\mathbb{Z}$, which is possible because $\mathbb{Q}/\mathbb{Z}$ is injective.



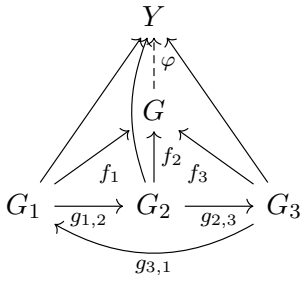
So $R^* = \mathrm{Hom}(R, \mathbb{Q}/\mathbb{Z})$ is injective, as claimed. □

17 Limits and Colimits

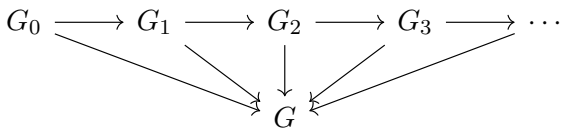
Recall from the lecture on category theory that a limit of a family $\{G_\alpha\}$ is a universal object with morphisms from $G \to G_\alpha$ for each α.

17.1 Colimits

Definition 17.1. A *colimit* G of the family $\{G_\alpha\}$ is universal object with morphisms from $G_\alpha \to G$ for each α. In other words, a colimit is the same concept as a limit, but the arrows (morphisms) go the other way.



A special case is that if $G_i \to G_{i+1}$ is injective for all i, then the colimit, G, is more or less the union of the G_i.

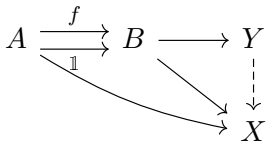


Example 17.1. $\mathbb{Q}/\mathbb{Z}$ is the union of $\mathbb{Z}/\mathbb{Z} \subseteq (\frac{1}{2}\mathbb{Z})/\mathbb{Z} \subseteq (\frac{1}{6}\mathbb{Z})/\mathbb{Z} \subseteq (\frac{1}{24}\mathbb{Z})/\mathbb{Z} \subseteq \cdots$.

17.1.1 Examples of colimits

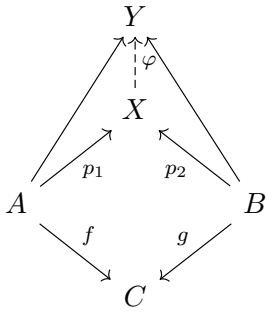
Recall that the kernel $f : A \to B$, where A, B are groups is the equalizer of f and $\mathbb{1}$, the trivial map from $A \to B$; this is the limit of A, B with the morphisms $f, \mathbb{1}$.

Definition 17.2. The *cokernel* X of A and B is the colimit of A, B with morphisms $f, \mathbb{1}$.



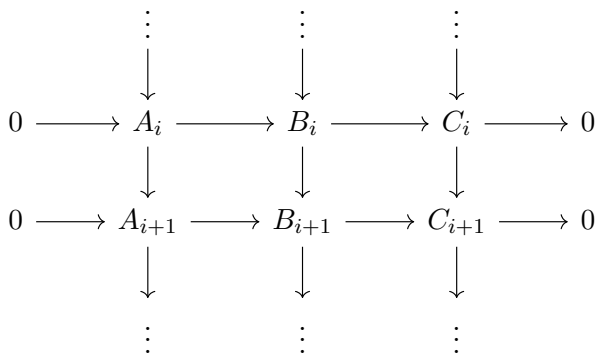
This can also be thought of as the coequalizer of $f, \mathbb{1}$, where the coequalizer has the same definition as the equalizer but with the arrows reversed.

Definition 17.3. The *push-out* X is the colimit of A and B with morphisms $f : A \to C$ and $g : B \to C$.



17.2 Exact sequences of colimits

When do colimits preserve exactlness? Say we have the following diagram with rows exact:

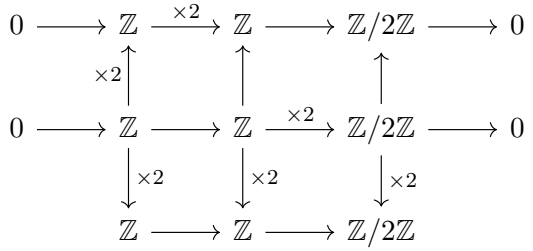


Then

$$\cancel{0 \to} \operatorname{colim} A_i \to \operatorname{colim} B_i \to \operatorname{colim} C_i \to 0$$

is right exact but not left exact.

Example 17.2. Here is an example where the colimit is not left exact.



The colimit $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not injective.

When do colimits preserve exactness, then?

Definition 17.4. A *directed set* S is a partially ordered set such that if $a, b \in S$, there exists a c with $a \leq c$ and $b \leq c$.

Example 17.3. The set $\mathbb{N}$ is directed under the usual ordering $\leq$.

Definition 17.5. A *direct limit* is a colimit of a family indexed by a directed set.

Proposition 17.1. *Direct limits preserve exactness.*

Proof. Suppose S is a directed set and we are taking the colimit over a family indexed by S. We have modules A_i for $i \in S$ with $A_i \to A_j$ with $i < j$. Every element of the colimit is represented by some $a \in A_i$ for some i. This is because any element of the colimit is represented by some sum of elements $a_j \in A_j$ for various $j \in S$; then we can pick $c \geq$ all these j, and take the sum of the images of a_j in A_c.

Now suppose we have exact sequences $0 \to A_i \to B_i \to C_i \to 0$ for $i \in S$. We want to show that $\operatorname{colim} A_i \to \operatorname{colim} B_i$ is injective. Pick $a \in \operatorname{colim} A_i$. Then a is represented by some $a_i \in A_i$ for some $i \in S$. Now suppose that a_i has image 0 in $\operatorname{colim} B_i$. If b_i is the image of s_i, then $b_i = 0$ in the colimit. So for some j, the image of b_i in B_j is 0. So if a_j is the image of a_i in A_j, then a_j has image 0. Then $a_j = 0$, which makes $A_j \to B_j = 0$, and so $s_j = 0$ in the colimit. □

17.3 Inverse limits and the p-adic integers

Look at $G = \mathbb{Z}[1/p]/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$. This is the colimit of $\mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{Z}/p^2\mathbb{Z} \subseteq \mathbb{Z}/p^3\mathbb{Z} \subseteq \cdots$. What is G^*? We get

$$\operatorname{Hom}(\mathbb{Z}/p\mathbb{Z}, S^1) \leftarrow \operatorname{Hom}(\mathbb{Z}/p^2\mathbb{Z}, S^1) \leftarrow \operatorname{Hom}(\mathbb{Z}/p^3\mathbb{Z}, S^1) \leftarrow \cdots$$

Definition 17.6. The *inverse limit* is the limit of a directed family $\{A_\alpha\}$.

So the dual of a direct limit is the inverse limit of the duals. The dual for our example above is the p-adic integers $\mathbb{Z}_p$. Look at

$$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots$$

Then the p-adic integers is the inverse limit of this. We get the set of sequences of base p expansions going to the left an infinite distance. For example, if $p = 3$, such a sequence would look like $(\ldots, 2, 1, 2, 2, 0, 1, 2)$. Addition and multiplication are indeed well-defined componentwise.

Does taking inverse limits preserve exactness? The answer is no, even if the set is directed.

Example 17.4. Take the following diagram, where the rows are exact:

$$\begin{array}{ccccccccc}
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & & \\
 & & \downarrow{\scriptstyle \times 3} & & \downarrow{\scriptstyle \times 3} & & \uparrow & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \times 3} & & \downarrow{\scriptstyle \times 3} & & \downarrow{\scriptstyle \times 2} & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0
\end{array}$$

The inverse limits give us $0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0$, but this is not exact.

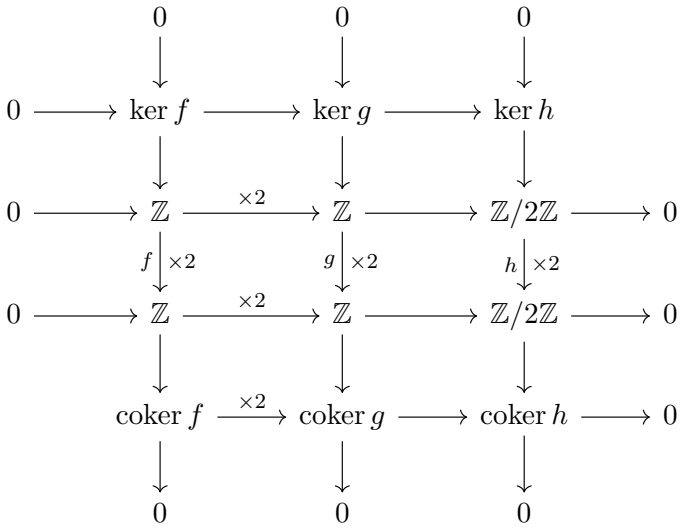
However, there is hope! Taking inverse limits preserve exactness if the A_i preserve the Mittag-Leffler[30] condition.

[30] This sounds like two people, but it is actually just one.

18 The Snake Lemma

18.1 Statement and proof of the snake lemma

Example 18.1. Consider the following commutative diagram with exact rows:



The map $\ker g \to \ker h$ is not surjective, and $\operatorname{coker} f \to \operatorname{coker} g$ is not injective. The snake lemma says that these are the same problem.

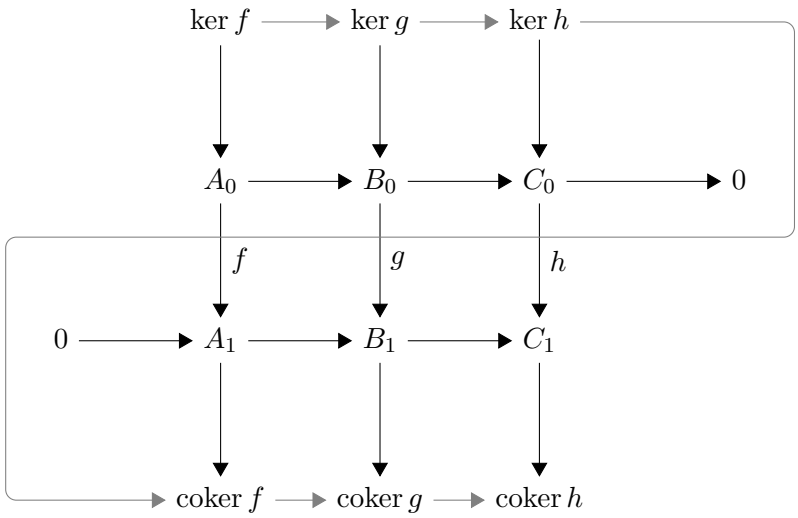
Lemma 18.1 (Snake)**.** *Suppose we have the following commutative diagram with exact rows:*

$$\begin{array}{ccccccc} & & A_0 & \longrightarrow & B_0 & \longrightarrow & C_0 \longrightarrow 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 \end{array}$$

Then there is a map $\ker h \to \operatorname{coker} f$ *that makes the "snake sequence"*

$$\ker f \to \ker g \to \ker h \to \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h$$

exact. This yields the commutative diagram[31]



Proof. We first construct the snake homomorphism by zigzaging through the diagram. Take $c \in \ker h$; then $c \in C$, so since $B_0 \to C_0$ is surjective, we can lift c to an element $b \in B_0$. Then we can map b to $b' \in B_1$. Since c was in $\ker h$ and the diagram is commutative, $B_1 \to C_1$ sends b' to 0. So $b' \in \ker(B_1 \to C_1) = \operatorname{im}(A_1 \to B_1)$, and we can lift b' to $a' \in A_1$. Note that a' is unique (given b) because $A_1 \to B_1$ is injective. Finally, let a'' be the image of a' under the map $(A_1 \to \operatorname{coker} f)$. So we map $c \mapsto a''$.

Is this well-defined? We have a choice of possibly different b. Suppose we picked some b_0 instead of b, and let a_1' be the corresponding element of A_1 we get. Note that $B_0 \to C_0$ sends $b - b_0$ to 0, so there exists some $a \in A_0$ such that $A_0 \to B_0$ maps a to $b - b_0$. Since the diagram is commutative, the map $A_1 \to B_1$ should send $f(a)$ to $g(b - b_0)$. Then since f is injective and $A_1 \to B_1$ sends $a' - a_0'$ to $g(b - b_0)$, we have that $a' - a_0' = f(a)$; then we have $a' - a_0' \in \operatorname{im}(f)$, so a' and a_0' have the same image in $\operatorname{coker} f = A_1/\operatorname{im} f$.

We claim that the snake sequence is exact. The hard part is exactness at $\ker h$ and $\operatorname{coker} f$. Suppose we want to prove exactness at $\operatorname{coker} f$. Suppose $a'' \in \operatorname{coker} f$ and is in the kernel of the map $\operatorname{coker} f \to \operatorname{coker} g$. Lift it to $a' \in A_1$, and let $b' \in B_1$ be the image of a'. b' maps to 0 in $\operatorname{coker} g$ by the definition of a'' (and because the diagram commutes), so lift it to $b \in B_0$. Map b to $c \in C_0$. Now note that $h(c) = 0$ because $g(b) = b' \in \operatorname{im}(A_1 \to B_1) = \ker(B_1 \to C_1)$. So $c \in \ker f$, and the snake homomorphism takes c to a'', so the sequence is exact at $\operatorname{coker} f$. The similar proof for $\ker h$ is left as an exercise. □

[31] The code for this diagram was modified from an answer on this StackExchange post.

18.2 Applications of the snake lemma

18.2.1 Exact sequences of tensor products of modules

Recall that if $0 \to A \to B \to C \to 0$ is exact, then so is

$$A \otimes M \to B \otimes M \to C \otimes M \to 0.$$

However, $A \otimes M \to B \otimes M$ is not always injective. What is the kernel? Choose free modules F_i, H_i so that

$$0 \to F_1 \to F_0 \to A \to 0, \qquad 0 \to H_1 \to H_0 \to C \to 0.$$

Extend this to the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & F_1 & \longrightarrow & F_1 + H_1 & \longrightarrow & H_1 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & F_0 & \xrightarrow{\times 2} & F_0 + H_0 & \longrightarrow & H_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0
\end{array}$$

Tensor every row with M and put in the kernels to get the diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker f & \longrightarrow & \ker g & \longrightarrow & \ker h & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F_1 \otimes M & \longrightarrow & (F_1 \otimes M) + (H_1 \otimes M) & \longrightarrow & H_1 \otimes M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & F_0 \otimes M & \longrightarrow & (F_0 \otimes M) + (H_0 \otimes M) & \longrightarrow & H_0 \otimes M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & A \otimes M & \longrightarrow & B \otimes M & \longrightarrow & C \otimes M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Note that the bottom row is the row of cokernels of the vertical maps f, g, h, so by the snake lemma, we get an exact sequence

$$0 \to \ker f \to \ker g \to \ker h \to A \otimes M \to B \otimes M \to C \otimes M \to 0.$$

we can also call these

$$0 \to \mathrm{Tor}(A, M) \to \mathrm{Tor}(B, M) \to \mathrm{Tor}(C, M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0.$$

Is $\mathrm{Tor}(A, M)$ well-defined? It seems to depend on the choice of $0 \to F_1 \to F_0 \to A \to 0$. It is, in fact, well-defined.

Let's calculate $\mathrm{Tor}(M, N)$ for finitely generated abelian groups M, N. First, we have $\mathrm{Tor}(M_1 \oplus M_2, N) \cong \mathrm{Tor}(M_1, N) \oplus \mathrm{Tor}(M_2, N)$, so it is enough to do the case where M, N are cyclic. If $M = N = \mathbb{Z}$, take the resolution $0 \to F_1 \to F_0 \to M \to 0$. If $M = \mathbb{Z}$ and $N = \mathbb{Z}/n\mathbb{Z}$, we have

$$0 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow 0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

So $\mathrm{Tor}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = 0$.

If $m = \mathbb{Z}/m\mathbb{Z}$ and $N = \mathbb{Z}/n\mathbb{Z}$, we have

$$0 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/n\mathbb{Z} \longrightarrow \cdots \longrightarrow 0$$

Then $\mathrm{Tor}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \ker(\mathbb{Z}/n\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/(m, n)\mathbb{Z}$.

So Tor(M,N) depends only on the torsion subgroups of M, N. In fact, if M, N are finite, $M \otimes N \cong Tor(M, N)$, although this isomorphism is not natrual.

Example 18.2. Here is a historical example from algebraic topology. This is where the idea of Tor came from. The universal coefficient theorem states that

$$H_i(M, G) = (H_i(M, \mathbb{Z}) \otimes G) \oplus \mathrm{Tor}(H_{i-1}(M, \mathbb{Z}), G),$$

where $H_i(M, G)$ is the homology of the manifold M with coefficients in G.

Example 18.3. As a specific case of the previous example, let $M = P^2$ (2-dimensional projective space). This is S^2, where we identify opposite points. Suppose we know $H_0(M, \mathbb{Z}) = \mathbb{Z}$, $H_1(M, \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, and $H_i(M, \mathbb{Z}) = 0$ for $i > 1$. Then

$$H_0(M, \mathbb{Z}/2\mathbb{Z}) = H_0(M, \mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$$

$$H_1(M, \mathbb{Z}/2\mathbb{Z}) = H_1(M, \mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} \oplus \operatorname{Tor}(H_0(M, \mathbb{Z}), \mathbb{Z}, 2\mathbb{Z})$$
$$H_2(M, \mathbb{Z}/2\mathbb{Z}) = H_2(M, \mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} \oplus \operatorname{Tor}(H_1(M, \mathbb{Z}), \mathbb{Z}, 2\mathbb{Z}),$$

which allows us to compute the homology[32] $H_2(M, \mathbb{Z}/2\mathbb{Z})$.

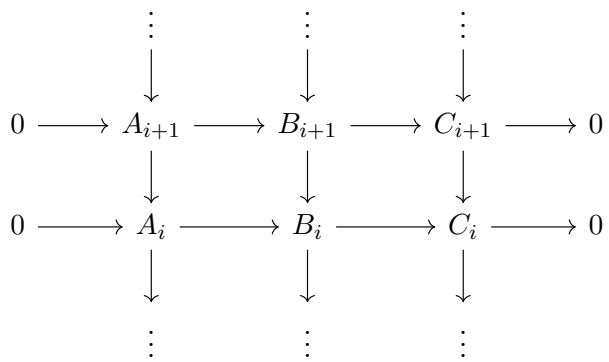
18.2.2 The Mitag-Leffler condition

Look at $\cdots \to A_3 \to A_2 \to A_1 \to A_0$. Does the sequence of images stabilize? In other words, does $\operatorname{im} A_i = \operatorname{im} A_{i+1} = \cdots$ for some i?

Definition 18.1. Let $\cdots \to A_3 \to A_2 \to A_1 \to A_0$. The *Mitag-Leffler condition* is that the sequence of images stabilizes for all A_n; that is, for each $n \in \mathbb{N}$, ther exists some $i \geq n$ such that $\operatorname{im} A_i = \operatorname{im} A_{i+1} = \cdots$.

Example 18.4. The Mitag-Leffler condition holds if all A_i are finite.

Theorem 18.1. *Suppose we have*



If the Mitag-Leffler condition is satisfied, then

$$0 \to \lim A_i \to \lim B_i \to \lim C_i \to 0.$$

Proof. We first do two easy cases:

1. Suppose all maps $A_{i+1} \to A_i$ are onto (so ML condition is satisfied). We want to show that $\lim B_i \to \lim C_i$ is onto. Pick some element of $\lim C_i$, which looks like $(c_0, c_1, \dots)$ for $c_i \in C_i$, where c_i is the image of c_{i+1}. We can lift the c_i to b_i. Is b_i the image of b_{i+1}? Pick $b_0 \in B_0$, and choose some $b_1 \in B_1$. Then $\operatorname{im}(b_1) - b_0 \in \ker(B_0 \to C_0) = \operatorname{im}(A_0 \to B_0)$, so let $a_0 \in A_0$ be its preimage. Then we can lift a_0 to $a_1 \in A_1$. Now replace b_1 by $b_1 + \operatorname{im}(a_1)$. Repeat this to find $b_2, b_3, \dots$. So b_i maps to c_i and b_{i-1}.

[32] In the first edition of Lang's book, there was an infamous exercise that said, "Take any book on homological algebra, and prove all the theorems without looking at the proofs given in that book." Professor Borcherds seemed dismayed that the exercise was removed in a later edition of the book.

2. Suppose for each i, we can find j so that $A_j \to A_i$ is 0 (this is the extreme opposite condition to case 1). Then the ML condition holds. We want to show that $\lim B_i \to \lim C_i$ iis onto. Pick A_{i_0}. Pick A_{i_1} so $A_{i_1} \to A_{i_0}$ is 0. Do the same over and over to get $\to Ai_2 \to A_{i_1} \to A_{i_0}$. Take the inverse limits over B_0, B_{i_1}, B_{i_2}, etc.. So we can assume all maps $A_{i+1} \to A_i$ are 0. Pick $(c_0, c_1, c_2, \dots)$, and pick b_i mapping to c_i. Is $\mathrm{im}(b_i) = b_{i-1}$? The image of $\mathrm{im}(b_2)$ is $\mathrm{im}(b_1)$ because $\mathrm{im}(b_2) - b_1$ is in the image of A_1, which is 0 in A_0. So the sequence $\mathrm{im}(b_1), \mathrm{im}(b_2), \mathrm{im}(b_3), \dots$ is in $\lim B_i$, and has image $(c_0, c_1, c_2, \dots)$.

Now we combine the special cases 1 and 2. Suppose A_i satisfied the ML condition. Put $X_i = \bigcap_{j \geq i} \mathrm{im}(A_j \to A_i)$. So $X_i \subseteq A_i$, and we get exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_i & \longrightarrow & A_i & \longrightarrow & A_i/X_i & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X_{i-1} & \longrightarrow & A_{i-1} & \longrightarrow & A_{i-1}/X_{i-1} & \longrightarrow & 0 \end{array}$$

where the down maps for the X_i are surjective. For each i, we can find j so that $\mathrm{im}(A_j/X_i \to A_i/X_i) = 0$.

Use the snake lemma. Recall that $0 \to A \to B \to C \to 0$ is exact implies that

$$A \otimes M \to B \otimes M \to C \otimes M \to 0$$

is exact and

$$\mathrm{Tor}(A, M) \to \mathrm{Tor}(B, M) \to \mathrm{Tor}(C, M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0$$

is exact.

Copy this argument since the limit is left exact. We do this by flipping all the arrows. We constructed Tor by taking $0 \to G_1 \to F_0 \to A \to 0$; this works when F is free or projective. So we can flip the arrows by replacing the projective modules by injective modules $0 \to A \to I_0 \to I_1 \to 0$; this uses our fact that every module is contained in an injective module.

So the analogue of Tor is $\lim^1(A_i)$. We get a sequence

$$0 \to \lim A_i \to \lim B_i \to \lim C_i \to \lim{}^1 A_i \to \lim{}^1 B_i \to \lim{}^1 C_i.$$

For this to be exact, we want $\lim^1 A_i = 0$. The proofs above show that this is true if either of the special cases hold. Now look at $0 \to X_i \to A_i \to A_i/X_i \to 0$. We have

$$0 \to \lim X_i \to \lim A_i \to \lim A_i/X_i \to \lim{}^1 X_i \to \lim{}^1 A_i \to \lim{}^1 A_i/X_i \to 0. \qquad \square$$

18.3 Unrelated: Finitely generated modules over a PID

Theorem 18.2. *Any finitely generate modules over PID are sums of cyclic modules of the form R/I.*

Proof. We don't have time in class to prove the whole theorem, so we will cheat and just do the case of Euclidean domains. The proof is the same as the one we gave for $\mathbb{Z}$. If M is any submodule of $\mathbb{Z}^n$, we can find a basis $b_1, \ldots, b_n$ of $\mathbb{Z}^n$. So M is spanned by $d_1 b_1, d_2 b_2, \ldots, d_n b_n$ for some d_i Then the finitely generated module $\mathbb{Z}^n/m = \bigoplus \mathbb{Z}/d_i\mathbb{Z}$. $\square$

19 Polynomials and Divisibility

19.1 Polynomial division with remainder

We start with some results you should already know.

Theorem 19.1. *Suppose f, g are polynomials in $R[x]$, where R is a commutative ring. Also suppose that f has leading coefficient 1, so $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $g(x) = f(x)q(x) + r(x)$, where $\deg(r) < \deg(f)$.*

Corollary 19.1. *If K is a field, $K[x]$ is a Euclidean domain.*

Proof. We can make the leading coefficient of any polynomial 1 by multiplying by a unit. Then apply the theorem. □

Corollary 19.2. *If K is a field, $K[x]$ is a principal ideal domain.*

Proof. All Euclidean domains are PIDs. □

Corollary 19.3. *If K is a field, $K[x]$ is a unique factorization domain.*

Proof. All PIDs are UFDs. □

Example 19.1. How can we find the prime elements of $F_2[x]$, where $F_2 = \mathbb{Z}/2\mathbb{Z}$, the field with 2 elements? Recall the sieve of Eratosthenes[33]. List all numbers > 1, identify the smallest number as prime, and cross out all multiples of it.

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, \ldots$$

Then, identify the first non-crossed out number as prime, and cross out all multiples of it.

$$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, \ldots$$

If we repeat this process, we can find all the prime numbers.

For $F_2[x]$, we list all elements (other than 0 or units) in order of degree.

$$x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, \ldots$$

Cross out all multiples of x.

$$x, x+1, \cancel{x^2}, x^2+1, \cancel{x^2+x}, x^2+x+1, \ldots$$

The next element, $x+1$, is prime, so we cross out multiples of it. Note that $x^2+1 = (x+1)^2$ in $F_2[x]$.

$$x, x+1, \cancel{x^2}, \cancel{x^2+1}, \cancel{x^2+x}, x^2+x+1, \ldots$$

[33] Erathosthenes was the first person to accurately calculate the circumference of the Earth.

The polynomials not divisible by x and $x+1$ are

$$x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x+1, \cancel{x^4+x^2+1}, x^4+x^3+1, x^4+x^3+x^2+x+1,$$

and we can continue the process.

Proposition 19.1. *Suppose a polynomial $f \in R[x]$ has a root a ($f(a)=0$). Then $f(x) = g(x)(x-a)$ for some g.*

Proof. Apply division to get that $f(x) = g(x)(x-a)+r$. We have $\deg(r) < 1$, so r is constant. Put $x=a$ to get $f(a) = g(a)(a-a)+r = \mathrm{r}$, so $r=0$. □

Corollary 19.4. *A polynomial $f \in R[x]$ of degree n over an integral domain R has $\leq n$ roots.*

Proof. If $a_1, \dots, a_k$ are roots, then $f(x) = (x-a_1)\cdots(x-a_k)g(x)$, so $k \leq n$. If the product is 0, then so is some factor $(x-a_i)$ because R is an integral domain. □

Example 19.2. Let $R = \mathbb{Z}/8\mathbb{Z}$, which is not an integral domain. Let $f(x) = x^2-1$, which has degree 2. Then $f(x)$ has 4 roots: 1, 3, 5, and 7.

Example 19.3. Let R be the quaternions (this is noncommutative), and look at $f(x) = x^2+1$. Then f has roots $\pm i, \pm j, \pm k$, and roots $ai+bj+ck$ for real a,b,c that satisfy $a^2+b^2+c^2=1$. This is an uncountable number of roots!

19.2 An application to field theory

We first prove a lemma.

Lemma 19.1. *Any abelian group G with $\leq n$ elements of order n ($\forall n \geq 1$) is cyclic.*

Proof. Recall that $G \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \cdots$. Suppose that $p_1 = p_2$; then G has p^2 elements x with $x^p = 1$ (since G contains $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$). This is impossible, so all p_i are distinct. Then G is cyclic by the Chinese remainder theorem ($\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if m,n are coprime). □

Proposition 19.2. *The group $(\mathbb{Z}/p\mathbb{Z})^*$ of units mod p is cyclic if p is prime.*

Proof. Since p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field. So any polynomial in $R[x]$ of degree n has $\leq n$ roots. So x^n-1 has $\leq n$ roots for any $n \geq 1$. Then G has $\leq n$ elements x with $x^n = 1$ (for $n \geq 1$). Using the lemma finishes off the proof. □

Example 19.4. This need not hold if p is not prime. $(\mathbb{Z}/12\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$, and these are both cyclic of order 2.

Definition 19.1. A generator of $(\mathbb{Z}/p\mathbb{Z})^*$ is called a *primitive root.*

We have shown that primitive roots always exist when p is prime.

Example 19.5. Let's find a primitive root of $p = 23$. The element should have order 22. Check the elements $-1, 1, 2, 3, 4, 5$. We find that 5 is the primitive root because $5^2, 5^{11} \not\equiv 1 \pmod{23}$.

The same argument shows that the following is true.

Theorem 19.2. *If F is a field, any finite subgroup of F^* is cyclic.*

Example 19.6. Let $F = \mathbb{C}$, and take the subgroup of 8th roots of unity. This has primitive root $e^{2i\pi/8}$.

This also gives us the following corollary.

Corollary 19.5. *If F is any finite field, then F^* is cyclic.*

19.3 Unique factorization in polynomial rings

We want to show that $\mathbb{Z}[x]$ is a UFD, and we know that $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, which is a UFD because $\mathbb{Q}$ is a field. We cannot do this as we usually do, because $\mathbb{Z}[x]$ is not a Euclidean domain or a PID. For example, $(2, x)$ is a non-principal ideal. So we use the fact that $\mathbb{Q}[x]$ is a UFD.

Definition 19.2. Let $f \in \mathbb{Q}[x]$. The *content* $c(f)$ is defined as follows: Suppose $f(x) = a_n x^n + \cdots + a_0$. For each prime p, $a_n = p^{m_n} b_n, a_{n-1} = p^{m_{n-1}} b_{n-1}, \ldots$ with $m_i \in \mathbb{Z}$ and b_i not having any factors of p in the numerator or denominator. Let $c(f) = p^{\min(m_i)} \times b$, where b is some number with no factors of p.

Example 19.7. Let $f(x) = (2/3)x^2 + 4$. Then $c(f) = 2/3$.

Proposition 19.3. *$\mathbb{Z}[x]$ is a unique factorization domain.*

Proof. The key point of the proof is that $c(fg) = c(f)c(g)$. We may assume that $c(f) = c(g) = 1$; otherwise, we multiply f and g by constants to make this so. We want to show that $c(fg) = 1$. We know that f has integer coefficients, so $c(f) \in \mathbb{Z}$. Suppose p is any prime in $\mathbb{Z}$; we show that p does not divide $c(fg)$.

Since $c(f) = c(g) = 1$, p does not divide all coefficients of f or all the coefficients of g. So $f = a_n x^n + \cdots + a_i x^i + \cdots + a_0$ and $g = b_m x^m + \cdots + b_j x^j + \cdots + b_0$ where i and j are the least indices such that a_i and b_j are not divisible by p. So the coefficient of x^{i+j} in fg is

$$a_0 b_{i+j} + a_1 b_{i+j-1} + a_2 b_{i+j-2} + \cdots + a_i b_j + \cdots + a_{i+j-1} b_1 + a_{i+j} b_0,$$

which has all terms except $a_i b_j$ divisible by p. This means that the coefficient of x^{i+j} in fg is not divisible by p. This is true for any prime p, so $c(fg) = 1$.

We sketch the rest of the proof. The main point is that we need to show that irreducible elements are prime. Recall that irreducible elements are such that $f \neq gh$ with $\deg(g), \deg(h) < \deg(f)$; prime elements are such that if f divides g, h, then f divides g or h.

The irreducibles of $\mathbb{Z}[x]$ are the primes $2, 3, 5, 7, \ldots \in \mathbb{Z}$ and the polynomials $f(x)$ of degree > 1 with $c(f) = 1$.

We leave the following two statements as exercises:

1. These are all the irreducibles of $\mathbb{Z}[x]$.

2. Any element of $\mathbb{Z}[x]$ is a product of irreducibles.

If $\deg(f) = 0$, then $f = p$ is prime in $\mathbb{Z}$. If f divides gh, this means that $c(gh)$ is divisible by p. So $c(g)$ or $c(h)$ is fivisible by p (since $c(gh) = c(g)c(h)$. So p divides gh. The case of $\deg(f) > 0$ is similar and left as an exercise. □

We have really proved the following theorem.

Theorem 19.3. *If R is a UFD, then so is $R[x]$.*

Proof. Perform the same proof but with a few modifications. First, $c(f)$ is now only defined up to multiplication by a unit. Also, irreducibles of $R[x]$ are either irreducibles of R ($\deg = 0$) or irreducibles of $K[x]$ with content 1, where K is the quotient field of R. □

Corollary 19.6. *$\mathbb{Z}[x_1, \ldots, x_n]$ is a unique factorization domain.*[34]

Corollary 19.7. *If K is a field, $K[x_1, \ldots, x_n]$ is a unique factorization domain.*

Proof. These two have the same proof: induction on the number of variables. □

19.4 Irreducibility tests in $\mathbb{Z}[x]$ (or $\mathbb{Q}[x]$)

Given $f \in Z[x]$, how do we factor f into irreducibles?

Example 19.8. Here is an algorithm, due to Kronecker:

Suppose that $f - gh$. We can assume $g, h \in Z[x]$. Then $f(n) = g(n)h(n)$ for any $n \in \mathbb{Z}$. So we factor $f(0), f(1), \ldots, f(m)$, where $m = \deg(f)$. Then $g(0)$ divides $f(0)$ or $g(1)$ divides $f(1)$, (and so on), so there are only a finite number of possibilities for $g(0), \ldots, g(m)$. But $\deg(g) \leq m$, so g is determined by $g(0), \ldots, g(m)$.

Kronecker's algorithm is pretty slow. There are faster algorithms.

[34] In fact, $\mathbb{Z}[x_1, x_2, \ldots]$ in infinitely many variables is a field, but we will not prove that here.

Example 19.9. The LLL algorithm[35] is fast but not necessarily precise. We can write $f = af_1f_2\cdots f_n$, where f_i is irreducible with degree > 0 and $a \in \mathbb{Z}$. We can do this in polynomial time, but to find a, we must factor an integer, which may not be possible in polynomial time.

To test for reducibility, we can use reduction mod p: If $f(x) = g(x)h(x)$, then $f(x) = g(x)h(x) \pmod p$ for any prime p.

Example 19.10. Is $9x^4+6x^3+26x^2+13x+3$ irreducible? Yes. It is $x^4+x+1 \pmod 2$, and we saw that this was irreducible $\pmod 2$.

Example 19.11. Let's test if $x^4 - x^2 + 3x + 1$ is irreducible.

$$\pmod 2 : x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1),$$

which are both irreducible $\pmod 2$.

$$\pmod 3 : x^4 - x^2 + 1 = (x^2 + 1)^2.$$

which is also irreducible $\pmod 3$.

Combine these results. The first one says that the only possible factorization is a degree 1 polynomial times a degree 3 polynomial. The second says that the only possible factorization is into 2 degree 2 polynomials. So the polynomial must be irreducible.

Theorem 19.4 (Eisenstein)**.** *Suppose $f(x)$ has the following properties:*

1. *The leading coefficient is 1.*
2. *All other coefficients are divisible by p.*
3. *The constant term is not divisible by p^2.*

Then f is irreducible.

We will not prove this right now. First, let's see some examples.

Example 19.12. The polynomial $x^5 - 4x + 2$ is irreducible by Eisenstein's criterion.

Example 19.13. Look at the p-th roots of 1. These are the roots of the polynomial $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$. We want to show that the latter term is irreducible by Eisenstein's criterion. We need a trick to make this work. Put $z = x - 1$. Then

$$x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} = \frac{(z + 1)^p - 1}{z}$$

[35] This stands for Lenstra, Lenstra, and Lovasz.

$$= \frac{(z^p + pz^{p-1} + \frac{p(p-1)}{2} z^{p-2} + \cdots + pz + 1) - 1}{z}$$
$$= z^{p-1} + pz^{p-2} + \cdots + p,$$

so Eisenstein applies, and $z^{p-1} + pz^{p-2} + \cdots + p$ is irreducible. So $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible, as desired.

Why does this work? The prime p is *totally ramified* in $\mathbb{Z}[\zeta]$, where $\mathbb{Z}^p = 1$. We have that p factorizes in $\mathbb{Z}[\zeta]$ as $(1 - \zeta)^{p-1}u$, where u is a unit.

20 More on Irreducibility Tests

20.1 Eisenstein's criterion

Last lecture, we were applying the Eisenstein criterion to $\frac{x^p-1}{x-1} = x^{p-1}+x^{p-1}+\cdots+x+1$. We saw that if we set $z = x-1$, this equaled $z^{p-1}+pz^{p-2}+\cdots+p$.

Why does this work? Let $\zeta = e^{2\pi i/p}$, and look at the ring $\mathbb{Z}[\zeta]$. Then p pactorizes as $(1-\zeta)^{p-1}u$ for some unit u. In an algebraic number theory course, we would say that p is "totally ramified," so Eisenstein's criterion applies. Notice that the polynomial has roots $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, the p-th roots of unity. We also have that $(\zeta^k-1) = (\zeta-1)(\zeta^{k-1}+\cdots+1)$. Conversely, $\zeta-1$ is divisible by ζ^k-1, so ζ^k is also a root of 1.

20.2 Rational roots

The only linear factors of $x^n+a_{n-1}x^{n-1}+\cdots+a_0$ are of the form $x-b$ for b dividing a_0. This is because $(cx+b)(\cdots) = x^n+\cdots+a_0$, so $1 = c\times *$ and $a_0 = b\times *$.

Example 20.1. It is not possible to trisect the angle of 120° with just a compass and straightedge.[36] We will show that we cannot construct $2\cos(40°)$. We will not prove this here, but any number that can be constructed cannot satisfy an irreducible polynomial of degree n unless n is a power of 2. We want to show that $2\cos(40°)$ satisfies an irreducible polynomial in $\mathbb{Z}[x]$ of degree 3.

Look at $z = e^{2\pi i/9} = \cos(2\pi/9)+i\sin(2\pi/9)$. This is an angle of 40°. Then $2\cos(40°) = z+z^{-1}$. So we have the polynomial

$$0 = z^9-1 = (z^3-1)(z^6+z^3+1),$$

which means that $z^6+z^3+1 = 0$. Rewriting this as $z^3+1+z^{-3} = 0$ and letting $c = (z+z^{-1})$ we get

$$c^3-3c+1 = 0.$$

To show that this is an irreducible polynomial, note that c^3-3c+1 has no linear factors over $\mathbb{Q}$. We just have to check that factors of the constant term 1 are not roots.

If a polynomial of degree ≤ 3 has no linear factors, it is irreducible.[37] So c^3-3c+1 is irreducible.

Example 20.2. The polynomials

$$x^{100}+2, \qquad x^{100}+3$$

[36] Professor Borcherds gets a lot of emails from people claiming to have proven Fermat's last theorem, Goldbach's conjecture, or that is is possible to trisect any angle.

[37] The same method makes it easy to check polynomials of degree ≤ 3, but, in Professor Borcherd's words "degree ≥ 4 is painful."

are both irreducible. This is in contrast to in general, where polynomials of the form $x^n + b$ can have "unexpected" factorizations. For example,

$$x^{100} + 4 = (x^{50} + 2x^{25} + 3)(x^{50} - 2x^{25} + 2).$$

21 Noetherian Rings and Hilbert's Theorem

21.1 Noetherian rings and Noether's theorem

Definition 21.1. A ring is *Noetherian*[38] if all ideals are finitely generated.

Theorem 21.1. *For a ring R, the following are equivalent:*

1. *R is Noetherian.*
2. *Every nonempty set of ideals has a maximal element.*
3. *Every strictly increasing chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ of ideals is finite.*

Proof. (2) $\iff$ (3): First note that (3) $\implies$ (2) is just Zorn's lemma in disguise. To get (2) $\implies$ (3), observe that if $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ is infinite, then the set $\{I_1, I_2, I_3, \ldots\}$ has no maximal element.[39]

(1) $\implies$ (3): Suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is a chain of ideals. Put $I = \bigcup_i I_i$. Then I is an ideal. By condition (1), $I = (x_1, \ldots, x_n)$, so all x_i are in some I_m. Then $I_m = I_{m+1} = \cdots$.

(3) $\implies$ (1): Pick an ideal I. We want to show that I is finitely generated. Pick any $x_1 \notin I$. If $I = (x_1)$, we are finished. Otherwise, pick $x_2 \in I$ with $x_2 \neq x_1$ and check if $I = (x_1, x_2)$. If we are still not finished, continue abd we get $(x_1) \subseteq (x_1, x_2) \subseteq (x_1, x_2, x_3) \subseteq \cdots$. The infinite chain must stop by condition (3), so $I = (x_1, \cdots, x_n)$ is finitely generated. □

Example 21.1. Let $R = K[x_1, x_2, \ldots]$. Then $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$, so R is not Noetherian.

Example 21.2. Let $R = \mathbb{Z}$. We have the infinitely *decreasing* chain of ideals $(2) \supsetneq (4) \supsetneq (8) \supsetneq (16) \supsetneq \cdots$. Rings without decreasing chains of ideals are called *Artinian*. It turns out that all Artinian rings are Noetherian.

Theorem 21.2 (Noether)**.** *If R is Noetherian, so is $R[x]$.*

[38] Emmy Noether found that a lot of theorems proven about polynomial rings using complicated techniques could be simplified by using this condition.

[39] You may notice that we did not use any properties of rings here. This part of the equivalence is just a general fact about partially ordered sets.

Proof. Suppose I is an ideal of $R[x]$. Look at the chain of ideals of R given by $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$, where I_k is the set of leading coefficients of polynomials in I of degree ≤ 0.

R is Noetherian, so for some m, $I_m = I_{m+1} = I_{m+2} = \cdots$. Pick the set of polynomials of degree 0 whose leading coefficients generate I_0 (which is finitely generated because R is Noetherian). Do this for polynomials of degree 1, 2, etc. We only need to do this finitely many times because $I_m = I_{m+1} = I_{m+2} = \cdots$. We now leave it as an exercise to show that these finite sets generate I. □

21.2 Hilbert's theorem

Theorem 21.3 (Hilbert)**.** *Any ideal of $K[x_1, \ldots, x_n]$ is finitely generated.*

Proof. Use induction on number of variables and then use Noether's theorem. □

The following example shows why this is important.

Example 21.3. Recall that ideals of $K[x]$ are generated by 1 element, but this need not be true for $K[x, y]$. Look at the ideal (x^3, x^2y, xy^2, y^2); this ideal must have at least 4 generators because no element in this set generates more than 1 of these 4 elements. In general, ideals of $K[x_1, \ldots, x_n]$ need not be generated by n elements.

Example 21.4. This need not hold for infinitely many variables. $K[x_1, x_2, x_3, \ldots]$ has the ideal $(x_1, x_2, x_3, \ldots)$, which cannot be generated by a finite number of elements.

Example 21.5. Look at the ideal (x) in $K[x, y]$. Then (x) is a ring (but without an identity element) and is not finitely generated as a ring. For example, a generating set could be $\{x, xy, xy^2, \ldots\}$. So we must pay attention to the distinction between being finitely generated as an ideal of a ring and being finitely generated as a ring.

21.3 Rings of invariants and symmetric functions

Suppose a group G acts on a vector space V with basis $\{x_1, \ldots, x_n\}$. So for $g \in G$,

$$g \cdot x_1 = g_{1,1}x_1 + g_{1,2}x_2 + \cdots + g_{1,n}x_n$$

G also acts on polynomials in $x_1, \ldots, x_n$ by $g \cdot (p + q = g \cdot p + g \cdot q$ and $g \cdot (pq) = (g \cdot p)(g \cdot q)$.

Definition 21.2. The *ring of invariants* is the set of polynomials fixed by G (that is, the polynomials p such that $g \cdot p = p$ for all $g \in G$).

Can we find a finite number of invariants so all invariants are polynomials in them with coefficients in K? Hilbert showed that this is often true, and about 50 years later, Nagata found a counterexample which showed that it is not always true.

Definition 21.3. Let V have basis $\{x_1, \dots, x_n\}$, and let G be the symmetric group on $\{x_1, \dots, x_n\}$. The ring of *symmetric functions* is the ring of invariant polynomials.[40]

Example 21.6. Here are some examples of symmetric functions:

$$x_1 + x_2 + x_3 + \cdots x_n$$

$$x_1 x_2 x_3 \cdots x_n$$

$$x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n$$

$$x_1x_2x_3 + x_1x_2x_4 + \cdots + x_1x_3x_4 + \cdots$$

Look at $(x - x_1)(x - x_2) \cdots (x - x_n) = x^n - (\sum x_i)x^{n-1} + (\sum_{i<j} x_i x_j)x^{n-2} + \cdots \pm \prod x_i$. The coefficients of this polynomial are called the *elementary symmetric functions.*

Theorem 21.4. *Any symmetric function is a polynomial in elementary symmetric functions.*

Proof. We produce an algorithm. The key point is to order the monomials in the right way.[41] We say $x_1^{n_1}x_2^{n_2} \cdots \geq x_1^{m_1}x_2^{m_2} \cdots$ if $(n_1, n_2, \dots) \geq (m_1, m_2, \dots)$ in the lexicographic order.

Suppose we have a symmetric polynomial p. Look at the biggest monomial in it, and kill this monomial by subtracting the polynomial

$$q = (x_1 + x_2 + \cdots)^{n_1 - n_2}(x_1x_2 + \cdots)^{n_2 - n_3}(x_1x_2x_3 + \cdots)^{n_3 - n_4}.$$

Note that all these terms are elementary symmetric functions. So $p - q$ has a smaller largest monomial. Repeating this process, we eventually get to 0 because it is not possible to have an infinite sequence of strictly decreasing monomials (exercise). □

[40] Symmetric functions have a very rich combinatorial theory, showing up in places such as the irreducible characters of the symmetric group and the number of Young tableau of a given shape. If you want to learn more about symmetric functions, you should check out my notes on Math 249, Algebraic Combinatorics!

[41] Ordering the monomials of a polynomial is very important in the study of Gröbner bases.

22 Symmetric Functions and Polynomial Invariants

22.1 Symmetric functions and Newton's identities

Last time, we saw that any symmetric polynomial f is a polynomial in the elementary symmetric functions. We took the monomial $x_1^{n_1}x_2^{n_2}\cdots$ in f which is largest, and subtracted

$$(x_1+\cdots+x_n)^{n_1-n_2}\cdots.$$

The key point was that since f is symmetric, n_1-n_2, n_2-n_3 and other terms are positive; if f has a term with $x_i^{n_i}x_j^{n_j}$ with $n_j<n_i$, then f also has $x_i^{n_j}x_j^{n_i}$.

22.1.1 Newton's identities

What is $x_1^4+x_2^4+x_3^4+\cdots$? Look at

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)=x^n-e_1x^{n-1}+e_2x^{n-2}+\cdots.$$

Take the logarithmic derivative, $\frac{d}{dx}\log f(x)=\frac{f'(x)}{f(x)}$. The log derivative of fg is the log derivative of f plus the log derivative of g.

So the log derivative of $x-x_1$ is

$$\frac{1}{x-x_1}=\frac{1}{x}+\frac{x_1}{x^2}+\frac{x_1}{x^3}+\cdots.$$

And we get that the log derivative of f is

$$\frac{n}{x}+\frac{x_1+x_2+\cdots}{x^2}+\frac{x_1^2+x_2^2+\cdots}{x^3}=\frac{p_0}{x}+\frac{p_1}{x^2}+\cdots$$

So $f(\sum p_m/x^{m+1})=f'$ gives us that

$$(x^n-e_1x^{n-1}+\cdots))(\frac{p_0}{x}+\frac{p_1}{x^2})=nx^{n-1}-(n-1)e_1x^{n-2}+\cdots.$$

Equating the powers of x, we have

$$p_0=n,\qquad p_1-e_1p_0=-(n-1)e_1,\qquad p_2-e_1p_1+e_2p_0=(n-2)e_2$$

Example 22.1. Let α,β,γ be the roots of z^3+z+1. What is $\alpha^5+\beta^5+\gamma^5$? We have

$$p_0=3,\quad p_1=0,\quad p_2+p_0=1,\quad p_2=-1,\quad p_3=-3,p_4=2.$$

and $p_5+p_3+p_2=0$. These are the coefficients of the polynomial.[42]

[42] In the 19th century, undergraduate students were expected to be able to calculate things like this involving symmetric functions.

22.2 The discriminant

What about polynomials in $x_1, \dots, x_n$ invariant under the alternating group, A_n?

Definition 22.1. A polynomials f in variables $x_1, \dots, x_n$ is *antisymmetric* if it changes sign under elements $\sigma \notin A_n$.

Proposition 22.1. *Suppose f is invariant under A_n. Then $f = g+h$, where g is symmetric and h is antisymmetric.*

Proof. Set

$$g = \frac{f + \sigma f}{2}, \qquad h = \frac{f - \sigma f}{2}.$$

□

The polynomial h changes sign if we switch x_i and x_j, so h is divisible by the polynomial $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\cdots$. So let

$$\Delta = \prod_{i<j}(x_i - x_j).$$

The invariant functions of A_n are generated by the symmetric functions $e_1, \dots, e_n$ and Δ. Note that Δ^2 is symmetric, so Δ^2 is some polynomial in $e_1, \dots, e_n$. This is called *syzygy*.[43]

Definition 22.2. The *discriminant*[44] of $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is $a_n^{2n-2}\Delta^2$.

The discriminant vanishes iff f has multiple roots.

Proposition 22.2. *A polynomial f has a multiple root iff f and f' have a common factor.*

Proof. If $f = (x - x_1)^2 \cdots$, then $f' = 2(x - x_1)\cdots + (x - x_1)^2 \cdots$, so $x - x_1$ is a common factor. The converse is an exercise. □

When do $f(x), g(x)$ have a common factor?

$$f(x) = a_m x^n + \cdots + a_0$$

$$g(x) = b_n x^n + \cdots + b_0$$

If f, g have a common factor, then $f(x)p(x) - g(x)q(x) = 0$ for some p, q with $\deg(p) < n$ and $\deg(q) < m$ (set $p = g/(x - \alpha)$ and $q = -f/(x - \alpha)$).

[43] This comes from syn, which means together, and zygon, which means yoke. This is not the longest word in the English language with no vowels; that honor goes to the word rhythms.

[44] Invariants tend to end with -ant. For example, we have the determinany, the resultant, and the catalecticant. Professor Borcherds is glad the last of these has fallen out of usage.

This is a set of linear equations for coefficients of p, q. This has a nonzero solution if some determinant vanishes. So the coefficients of linear equations are:

$$\begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & 0 & 0 \\ 0 & a_m & \cdots & a_1 & a_0 & 0 & 0 & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \cdots & a_n & \cdots & a_2 & a_1 & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & 0 & 0 & 0 \\ 0 & b_n & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \cdots & b_n & \cdots & b_2 & b_1 & b_0 \end{bmatrix}$$

This matrix with $n + m$ rows is called the *Sylvester matrix*.

Definition 22.3. The *resultant* is the determinant of the Sylvester matrix.

Say f, g have a common root at ∞ if $a_m = b_m = 0$. The resultant equals 0 iff f and g have a common factor, possibly at ∞. This is the same as saying in geometry that the projective line is complete.

Example 22.2. The polynomial $f(x) = x^n - e_1 x^{n-1} + \cdots$ has a multiple root if the resultant of $f, f' = 0$. $\Delta = 0$ iff f has tahe multiple root, so Δ should be a constant times the resultant.

Example 22.3. When is the cubic curve $y^2 = x^3 + bx + c$ nonsingular? Curve $f(x, y)$ is nonsingular if $g(x, y) = 0 = f_x(x, y) = f_y(x, y)$ has no solutions, where f_x is the partial derivative with respect to x. These are the conditions that $2y = 0$ (so $y = 0$) and $3x^2 + b = 0$ (so $g(x) = x^3 bx + c = 0$); then we need to check if g, g' have a common root x.

The resultant of $x^3 + bx + c$ and $3x^2 + b$, is

$$\det \begin{bmatrix} 1 & 0 & b & c & 0 \\ 0 & 1 & 0 & b & c \\ 3 & 0 & b & 0 & 0 \\ 0 & 3 & 0 & b & 0 \\ 0 & 0 & 3 & 0 & b \end{bmatrix}$$

which is $4b^3 + 27c^2$ (up to a sign).

22.3 The ring of invariants, revisited

Suppose a finite group G acts on a complex vector space V spanned by $\{x_1, \ldots, x_n\}$. Recal that the ring of invariant polynomials is the set of polynomials in $x_1, \ldots, x_n$ invariant under the action of$G$. Is this ring finitely generated (over $\mathbb{C}$)?

Example 22.4. If $G = A_n$ and $V = \mathbb{C}^n$, then the ring is generated by $e_1, \dots, e_n, \Delta$.

In general this can be "mindbogglingly difficult."[45] Hilbert showed that the ring of invariants is finitely generated over $\mathbb{C}$.

Definition 22.4. The *Reynolds operator*[46] ρ is the average of the group elements,

$$\rho = \frac{1}{|G|} \sum_{g \in G} g.$$

The Reynolds operator takes polynomials in $\mathbb{C}[x_{,1}, \dots, x_n]$ to invariants.

Example 22.5. Let $G = S_n$. Then if $f = x_1$, $\rho(f) = \frac{x_1 + x_2 + \cdots + x_n}{n}$.

Proposition 22.3. *They Reynolds operator has the following properties:*

1. $\rho(f + g) = \rho(f) + \rho(g)$
2. $\rho(1) = 1$
3. $\rho(fg) = \rho(f)\rho(g)$ *if* $f = \rho(f)$

Proof. Exercise. □

Theorem 22.1 (Hilbert)**.** *If G is finite, the ring of invariants is always finitely generated over $\mathbb{C}$.*

Proof. Look at the ring $\mathbb{C}[x_1, \dots, x_n]$. This is graded by degree, where $\deg(x_i) = 1$. Let I be the ring of invariants. Then $I = \mathbb{C} \oplus I_1 \oplus I_2 \oplus \cdots$, where I_m is the set of invariants homogeneous of degree m. Look at the ideal generated by $I_1 \oplus I_2 \oplus I_3 \oplus \cdots$. By Hilbert's theorem, this ideal is finitely generated. Pick generators $i_1, \dots, i_k$ of this ideal. We show that they generate the ring I.

Suppose the generate $I_1, I_2, \dots I_k$. We want to show that they generate I_{k+1}. Pick $f \in I_{k+1}$. Then f is in an ideal J, so $f = a_1 i_1 + a_2 i_2 + \cdots + a_n i_n$ for some $a_n \in \mathbb{C}[x_1, \dots, x_n]$ with $\deg(a_i) > 0$.

Apply the Reynolds operator. Then

$$\rho(f) = \rho(a_1) i_1 + \rho(a_2) i_2 + \cdots + \rho(a_n) i_n$$

because f is invariant. So $\deg(a_n) < K$ as $\deg(i_n) > 0$, so $\rho(a_n)$ is a polynomial in $i_1, \dots, i_n$ by induction. So f is a polynomial in $i_1, \dots, i_m$. □

[45] Professor Borcherds showed us an invariant where the first generator took 13 pages to write out. Someone in the 19th century had a lot of spare time.

[46] Reynolds actually studied fluid dynamics. He showed that fluid flow averaged over time was a group.

The following example illustrates the reason we need to be careful about showing that $i_1, \ldots, i_k$ generate I.

Example 22.6. Let $R = \mathbb{C}[x, y]$, and take the subring containing the ideal generated by x and 1. This subring is not finitely generated as a ring.

Example 22.7. Let $G = \mathbb{Z}/n\mathbb{Z}$ act on $\mathbb{C}[x, y]$. Suppose that G is generated by σ, where $\sigma^n = 1$. Let $\sigma(x) = \zeta x$ and $\sigma(y) = \zeta y$, where $\zeta = e^{2\pi i/n}$. The ring of invariants is the polynomials with all terms of degree $0, n, 2n, \ldots$. A set of $n + 1$ generators is $x^n, x^{n-1}y, x^{n-2}y^2, \ldots, y^n$. If we call these $a_n, a_{n-1}, \ldots, a_0$ respectively, there are many relations between the a_i. For example, $a_n a_{n-2} = a_{n-1}^2$.

Are the collection of syzygies finitely generated? Yes. The ring of invariants is given by a polynomial ring in generators $a_0, \ldots, a_n$ mod the ideal of syzygies. So the ideal of syzygies is finitely generated by Hilbert's theorem.

23 Formal power series

23.1 Definition, inverse limit, and multiplicative inverses

Definition 23.1. Let R be a ring. The ring of *Formal power series*, $R[\![x]\!]$, is the ring of series of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots$$

with $a_i \in R$.

When we say "formal," we mean that we don't care about convergence. So these usually do not define a function.

Example 23.1. Consider the formal power series in $\mathbb{C}[\![x]\!]$

$$1 + 1!x + 2!x^2 + 3!x^3 + \cdots .$$

This only converges for $x = 0$.

$R[\![x]\!]$ is the inverse limit of the rings $R[x]/(x^n)$, the polynomial rings truncated at degree n. The homomorphism $R[x]/(x^n) \to R[x]/(x^{n-1})$ just removes the x^n term. We also say that $R[\![x]\!]$ is the *completion* of R at the ideal (x). More generally, we can take $\varprojlim R/I^n$ for any ideal I.

Example 23.2. The map $R \to \varprojlim R/I^n$ need not be injective. Let

$$R = \mathbb{C}[x^{1/n}, \text{all } n > 0],$$

$$I = (x^{1/2}, x^{1/3}, x^{1/4}, \dots).$$

So $R/I^n = R/I = \mathbb{C}$ for all n, which makes $\varprojlim R/I^n = \mathbb{C}$.

We also consider $R[\![x_1, x_2, \dots, x_n]\!]$, the ring of formal power series in n variables. This is just the ring defined recursively as $R[\![x_1, \dots, x_{n-1}]\!][\![x_n]\!]$.

Proposition 23.1. *Let $K[\![x]\!]$ be a field. Suppose that $f(x) = a_0 + a_1 x + \cdots$ with $a_0 \neq 0$. Then f has an inverse.*

Proof. Put $a_0 = 1$ for simplicity. Then $f(x) = 1 + g(x)$, where $g(x) = a_1 x + a_2 x^2 + \cdots$. Then

$$1/f = 1/(1+g) = 1 - g + g^2 - g^3 + \cdots ,$$

which makes sense because the coefficient of x^n is a finite sum for every n. □

Example 23.3. Let $f = 1 + x + x^2$. The inverse is $1 - x + x^3 - x^4$.

23.2 Ideals of $R[\![x]\!]$

Proposition 23.2. *The only ideals of $K[\![x]\!]$ are (0), (1), and (n) for $n \geq 1$.*

Proof. Any element $a_n x^n + a_{n+1}x^{n+1} = x^n(a_n + a_{n+1}x + \cdots) = x^n u$ for a unit u. □

Corollary 23.1. *$K[\![x]\!]$ is a PID, and a UFD.*

What about $K[\![x, y]\!]$? This is not a principal ideal domain because it has the nonprincipal ideal (x, y). However, we have the following result.

Theorem 23.1. *If R is Noetherian, so is $R[\![x]\!]$.*

Proof. This is similar to the proof for polynomials. Let I be an ideal. Let I_n be the ideal of the coefficients of x^n in series with smallest term x^n. Then $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$. This stabilizes because R is Noetherian. Each of these is finitely generated, so I is finitely generated. □

Corollary 23.2. *If R is Noetherian, so is $R[\![x_1, \ldots, x_n]\!]$.*

Proof. Induct on n. □

23.3 Unique factorization

Recall that $K[x_1, \ldots, x_n]$ is a UFD. We want to prove the corresponding fact for formal power series. But this is not as straightforward to prove.

A bad attempt would be to try to show that if R is a UFD, so is $R[x]$; this is not true in general.[47]

If we try to copy the proof for $R[x]$, we need to define the content of a formal power series. But this need not exist.

Example 23.4. Let $R = Z$ and $f = 1 + x/p + x^2/p^2 + x^3/p^3 + \cdots$, where p is prime. Then the content would have to be $p^{-\infty}$ times something.

The following theorem lets us reduce formal power series proofs to polynomial proofs. We treat the $n = 2$ case, but the proof for n variables is similar but with more bookkeeping.

Theorem 23.2 (Weierstrass preparation)**.** *Suppose $f \in K[\![x, y]\!]$, were K is a field. Then $f = ug$, where u is a unit, g is a polynomial in y with coefficients in $K[\![x]\!]$, and the leading coefficient is a power of x.*

[47] Lang made this mistake in a previous version of the book. According to Professor Borcherds, there are many papers that point out various errors in Lang's book.

Proof. Pick the monomial $x^m y^n$ so that $a_{m,n} \neq 0$ and if $a_{b,c} = 0$, then $b < m$, or $b = m$ and $b < n$; this is the same as saying that (m, n) is least in the lexicographic ordering on the degrees of polynomials with nonzero coefficients.

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \\ 0 & a_{1,0} & a_{2,0} & a_{3,0} & \cdots \\ 0 & a_{1,3} & a_{2,3} & a_{3,3} & \cdots \\ 0 & \boxed{a_{1,2}} & a_{2,2} & a_{3,2} & \cdots \\ 0 & 0 & a_{2,1} & a_{3,1} & \cdots \\ 0 & 0 & a_{2,0} & a_{3,0} & \cdots \end{array}$$

By multiplying by units, $1 + cx^i y^j$, we can make the coefficients of every term $x^m y^k$ zero for $k > n$; we can do this infinitely many times because the infinite product just defines a power series.

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & * & * & \cdots \\ 0 & 0 & * & * & \cdots \\ 0 & a_{1,2} & * & * & \cdots \\ 0 & 0 & * & * & \cdots \\ 0 & 0 & * & * & \cdots \end{array}$$

We can then kill all the coefficients $x^{m+1} y^k$ with $k \geq 1$. Similarly, kill off the other coefficients of $x^\ell y^k$ with $k \geq m$.

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & a_{1,2} & 0 & 0 & \cdots \\ 0 & 0 & * & * & \cdots \\ 0 & 0 & * & * & \cdots \end{array}$$

So f is a unit times $x^m y^n + \sum b_{i,j} x^i y^j$ with $i \geq m + 1$ and $j \leq m$. Note that we have to kill all the coefficients in this order; if you kill $x^i y^j$ before you kill $x^{i-k} y^{j-\ell}$, when you kill $x^{i-k} y^{j-\ell}$, you might make $x^i y^j$ nonzero. □

It turns out that the Weierstrass preparation theorem is what we needed.

Theorem 23.3. *$K[\![x_1, \ldots, x_n]\!]$ is a UFD.*

Proof. We will treat the case of $n = 2$, $R[\![x, y]\!]$. We first show that every element has a factorization into irreducibles. The proof we gave for $R[x]$ works for any Noetherian ring, and $R[\![x]\!]$ is Noetherian.

To prove uniqueness, the key step is to show that irreducible elements are prime. Irreducible means that $g \neq gh$ with g, h not units, and prime means that if f divides gh, then f divides g or h. This follows from the Weierstrass preparation theorem. Suppose that f divides gh; we can assume f, g, h are polynomials in y with coefficients in $K[\![x]\!]$. By induction, $K[\![x]\!]$ is a UFD, so $K[\![x]\!][y]$ is a UFD since it is a polynomial ring over a UFD. So f divides g or h in $K[\![x]\!][y]$ and hence in $K[\![x]\!][\![y]\!]$. □

Example 23.5. Let $f(x, y) = y^2 - x^2 - x^3$. This is irreducible as a polynomial in $K[x, y]$, but it is not irreducible as a power series in $K[\![x, y]\!]$.

$$y^2 - x^2 - x^3 = (y + x\sqrt{1+x})(y - x\sqrt{1+x}),$$

where $\sqrt{1+x}$ is the formal power series

$$\sqrt{1+x} = 1 + \frac{1}{2}x + \frac{\frac{1}{2} \cdot \frac{-1}{2}}{2!}x^2 + \cdots.$$

Geometrically, the curve $y^2 = x^2 - x^3$ only has 1 component. Near 0, the curve looks reducible, however, because it looks like two intersecting curves, $y = x\sqrt{1+x}$ and $y = -x\sqrt{1+x}$. So this polynomial is reducible in $K[\![x, y]\!]$ iff the curve $y^2 - x^2 = x^3 = 0$ has two branches near $x = y = 0$ (the point where the ideal (x, y) vanishes).

23.4 Hensel's lemma

Lemma 23.1 (Hensel)**.** *Suppose $f(x, y) \in K[\![x, y]\!]$, and suppose the smallest nonzero coefficients are of degree d and form a polynomial $f_d(x, y)$. Suppose that $f_d(x, y) = g(x, y)h(x, y)$ with g, h coprime. Then $f(x, y) = G(x, y)H(x, y)$, where g and h are the smallest degree terms of G and H, respectively.*

We will not prove this. Instead, here are some examples.

Example 23.6. Let $f(x) = y^2 - x^2 - x^3$. Then $d - 2$ and $f_2 = y^2 - x^2$. So

$$fy^2 - x^2 = (y - x)(y + x),$$

which lifts to

$$y^2 - x^2 - x^3 = (y - x\sqrt{1+x})(y - x\sqrt{1+x}) = (y - x + \cdots)(y + x + \cdots).$$

Example 23.7. Let $f(x) = y^2 - x^3$. Then $d = 2$ and $f_d = y^2 = y \cdot y$. However, $y^2 - x^3$ does not factorize! This is because x^3 has no square root as a formal power series. Geometrically, $y^2 - x^3 = 0$ looks like a cusp, so we don't get two different curves around 0.

Here is an analogue of Hensel's lemma in number theory.

Lemma 23.2 (Hensel (number theory version))**.** *Suppose $f(x) = (x-a)g(x)$, and $f(x) = 0$ around p, where $f \in \mathbb{Z}[x]$. If $f'(x) \neq 0 \pmod{p}$ has a root in $\mathbb{Z}_p$ ($f(x) \equiv 0 \mod p^n$ for all $n \geq 1$).*

Example 23.8. Let $f(x) = x^2 = 7$ and $p = 3$. Then $f(1) = 1^2 - 7 \equiv 0 \pmod{3}$, and $f'(1) = 2 \not\equiv 0 \pmod{3}$. So $x^2 - 6 \equiv 0 \pmod{p}^n$ has a root for all $n \geq$. We get

$$x^2 - 7 = (x - \sqrt{7})(x + \sqrt{7})$$

Example 23.9. Let $f(x) = x^2 - 7$ and $p = 2$. $f(1) \equiv 0 \pmod{2}$, and $x^2 - 7$ has no roots $\pmod{2}^3 = 8$. And $f'(1) = 2 \equiv 0 \pmod{2}$.

24 Field Extensions

24.1 Field extensions and algebraic elements

Definition 24.1. Let K be a field. A *field extension* L of K is a field such that K is a subfield of L. This is written as $K \subseteq L$ or L/K.

Example 24.1. $\mathbb{C}$ is a field extension of $\mathbb{R}$.

Definition 24.2. The *degree* $[L : K]$ of K/L is $\dim L$ as a vector space over K.

Example 24.2.

$$[\mathbb{C} : \mathbb{R}] = 2.$$

Definition 24.3. An element $\alpha \in L$ is called *algebraic* over K if α is a root of some polynomial in $K[x]$.

Example 24.3. The real number $\sqrt[5]{2}$ is algebraic over $\mathbb{Q}$, as a root of $x^5 - 2$.

Example 24.4. Neither π nor e is algebraic over $\mathbb{Q}$. The proof of this is hard.

In general, it is difficult to prove whether something is algebraic or not. The following are still open problems:

1. Is $e + \pi$ algebraic?
2. Is $e\pi$ algebraic?

Example 24.5. Let $L = \mathbb{Q}(x)$ be the rational functions in x. Then $[L : \mathbb{Q}] = \infty$, and x is not algebraic.

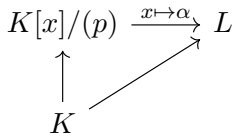
Theorem 24.1. *α is algebraic over K iff α is contained in a finite extension K_1 of K ($[K_1 : K] < \infty$).*

Proof. Suppose $\alpha \in K_1$ with $[K_1 : K] = n < \infty$. Look at $1, \alpha, \alpha^2, \ldots, \alpha^n$. This is $n + 1$ elements in an n-dimensional vector space over K, so we get

$$a_1 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

where $a_i \in K$ and the a_i are not all 0. So α is algebraic.

Suppose that α is algebraic. Then $p(\alpha) = 0$ for some $p \in K[x]$. We can assume p is irreducible. So $K[x]/(p)$ is a field, K_1. So $[K_1 : K] = \deg(p)$, with basis $1, x, x^2, \ldots, x^{\deg(p)-1}$. So we get a map $K[x]/(p) \to L$.



This map is injective since $K[x]$ is a field, so the image of the map is a field of degree $< \infty$ containing α. □

Lemma 24.1. *Let $K \subseteq K_1 \subseteq K_2$. Then*

$$[K_2 : K] = [K_2 : K_1][K_1 : K].$$

Proof. Let $x_1, \ldots, x_m$ be a basis of K_1 over K, and let $y_1, \ldots, y_n$ be a basis of K_2 over K_1. Then $x_i y_j$ form a basis of K_2 over K (exercise). So $[K_2 : K] = mn$. □

Proposition 24.1. *Suppose $\alpha, \beta \in L$ are algebraic over K. Then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. Say $\alpha \in K_1$ with $[K_1 : K]$ is finite. β satisfies an irreducible polynomial of degree $n < \infty$ over K, so β satisfies an irreducible polynomial of degree $\leq n$ over K_1. Then β is algebraic over K, say $\beta \in K_2$ with $[K_2 : K_1] < \infty$. Then

$$[K_2 : K] = [K_2 : K_1][K_1 : K],$$

so $[K_2 : K] = [K_2 : K_1][K_1 : K] < \infty$. $\alpha + \beta \in K_2$ and $\alpha\beta \in K_2$, so they are algebraic. □

Example 24.6. $\alpha = \sqrt{2} + \sqrt[3]{2} + \sqrt[5]{2}$ is algebraic. The smallest degree polynomial $p(x)$ with $p(\alpha) = 0$ has degree 30.

Example 24.7. All algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$ form a field.[48]

In general, we have the following fact.

Proposition 24.2. *$K[x]/p(x)$ is a field if p is irreducible.*

Proof. This is a quick consequence of a homework problem we have done, and should be done as an exercise. Use the fact that $K[x]$ is a PID. □

Suppose that p is not irreducible. Then for $p = fg$ for some coprime f, g. Then $K[x]/(p) \cong K[x]/(f) \times K[x]/(g)$ by the Chinese remainder theorem. So if p does not have multiple copies of the same factor, $K[x]/(p)$ is a product of fields. If p has multiple copies of a factor, $K[x]/(p)$ can be strange.

Example 24.8. Let $p = x^n$. Then $K[x]/(x^n)$ is the ring of truncated polynomials of the form $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ with $x^n = 0$ and $a_i \in K$. This has nilpotent elements, so it is not a product of fields.

Suppose that p is an irreducible polynomial in $K[x]$. We can find an extension field L so that p has a root in L, $L = K[x]/(p)$. Does P factorize into linear factors in L? Sometimes.

Example 24.9. Let $p(x) = x^3 - 2$ in $\mathbb{Q}[x]$. This is irreducible by Eisenstein's criterion. Let $L = \mathbb{Q}[x]/(x^3 - 3) = \mathbb{Q}[\sqrt[3]{2}] = \left\{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 : a_i \in \mathbb{Q}\right\}$. Does $x^3 - 2$ factor in linear factors in L? It does not. $L \subseteq \mathbb{R}$, and $x^3 - 2$ only has 1 real root. The others are $\sqrt[3]{2}e^{2\pi i/3}$ and $\sqrt[3]{2}e^{4\pi i/3}$.

[48] This is called the field of algebraic numbers and is studied in algebraic number theory.

Example 24.10. Let $p(x) = x^4 + 1$. This is irreducible; check by sending $x \mapsto x + 1$. We get $x^4 + 4x^3 + 6x^2 + 4x + 2$, which is irreducible by Eisenstein. Look at the complex roots: $e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4}$. So

$$L = \mathbb{Q}[x]/(x^4 + 1) \cong \mathbb{Q}[\zeta] = \left\{a_0\zeta + z_1\zeta + a_2\zeta^2 + z_3\zeta^3 : a_i \in \mathbb{Q}\right\}.$$

In this case, p factors as

$$p(x) = (x - \zeta)(x - \zeta^3)(x - \zeta^5)(x - \zeta^7).$$

24.2 Splitting fields

Definition 24.4. Suppose $p \in K[x]$ with $K \subseteq L$. L is a *splitting field* of p if

1. The polynomial p factors into linear factors in L.
2. L is generated by roots of p.

Example 24.11. $\mathbb{Q}[\zeta]$ is a splitting field of $x^4 + 1$.

Example 24.12. $\mathbb{Q}[\sqrt[3]{2}]$ is not a splitting field of $x^3 - 2$.

How do we find a splitting field? Let's find the splitting field of $x^3 - 2$. Form $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[x]/(x^3 - 2) = K_1$. In K_1, $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$, where the latter factor is in $K_1[x]$. Add the roots of this to K_1, forming $K_1[x]/(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$.

Here is the general construction of the splitting field of $p \in K[x]$: Factor p. If there are no factors of degree > 1, we are done. Otherwise, pick a factor q, where q is irreducible and of degree > 1. Form a new field $K[x]/(q)$. Over this field, p has one extra linear factor. Repeat this with p/q. We get

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_n,$$

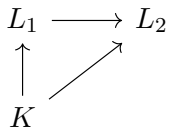
where at degree k, we add the root α_k of $p/((x - \alpha_1) \cdots (x - \alpha_{k-1}))$. So

$$[K_n : K] \leq n!$$

using our lemma about degrees. So the splitting field has degree $\leq \deg(p)!$.

The splitting field is essentially unique.

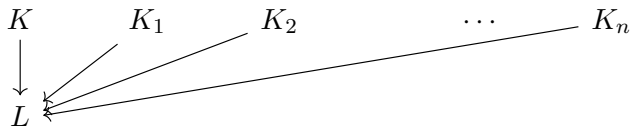
Proposition 24.3. *If L_1, L_2 are 2 splitting fields of K, $L_1 \to L_2$, we can find an isomorphism from $L_1 \to L_2$, fixing all elements of K.*



Proof. As before, construct the sequence of field extensions

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_n.$$

Suppose L is a splitting field of K. Then $K_1 \to L$ because $K_1 = K[x]/q_1(x)$, and L is a splitting field of P. We can form maps $K_i \to L$ for each i in this way.



Then the image of K_n is all of L since L is generated by the roots of p. So $K_n \cong L$. □

This isomorphism is not necessarily unique.

Example 24.13. $\mathbb{C}$ is the splitting field of $x^2 + 1$ over $\mathbb{R}$. What is $\sqrt{-1}$? It can be i or $-i$, depending on which isomorphism you use.

24.3 Application to finite fields

Proposition 24.4. *For each prime power p^n, there is a unique finite field F_{p^n} with p^n elements.*

Proof. The main idea of the proof is that F_{p^n} is the splitting field of $x^{p^n} - x$.

We first show that the splitting field of $x^{p^n} - x$ has p^n elements. This has p^n roots because the derivative is $p^n x^{p^n-1} - 1$, which is coprime to $x^{p^n} - x$. The key point is is that the roots form a field (closed under addition and multiplication) because $(a+b)^p = a^p + b^p$ in characteristic p, and because the roots are 0 or roots to $x^{p^n-1} = 1$. So the roots form a field of order p^n.

For uniqueness, we want to check that any field of order p^n is a splitting field of $x^{p^n} - x$. The key point here is that all elements are roots of $x^{p^n} - x$. If $x = 0$, it is a root. If $x \neq 0$, then $x \in L^*$ (order $p^n - 1$ and is a group), so $x^{p^n-1} = 1$ by Lagrange's theorem. □

Example 24.14. Let's construct the field of order $2^4 = 16$. We have proved that it exists, but the abstract proof is useless for construction. Find the irreducible factor p of $x^{16} - x$ of degree 4. Form $F_2[x]/p$. Any field of order 16 is a splitting field; for example $F_2[x]/p$ for any irreducible p of degree 4. Any irreducible polynomial in $F[x]$ of degree 4 divides $x^{16} - x$. So

$$x^{16} - x = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)x.$$

Note that 1,2, and 4 are the factors of 4.[49] This is divisible by $x^{2^2} - x$ and $x^{2^1} - 1$. To get an explicit construction of the field of order 2^4, use $F_2/(x^4 + x + 1)$, or quotient out by your favorite irreducible polynomial of degree 4 over F_2.[50]

Example 24.15. How many irreducible polynomials are there of degree 6 in $F_2[x]$? We have that

$$x^{2^6} - x = (\text{irred. polys of deg } 6)(\text{irred. polys of deg } 3)(\text{irred. polys of deg } 2)(x+1)x.$$

Using a kind of inclusion-exclusion argument, we get that the degree of the product of polynomials of degree 6 is $2^6 - 2^3 - 2^2 + 2^1$. Each polynomial has degree 6, so the number of polynomials is $(2^6 - 2^3 - 2^2 + 2^1)/6 = 9$.

24.4 Algebraic closure

Definition 24.5. L is called the *algebraic closure* of K if the following conditions hold:

1. Any element of L is algebraic over K.
2. Any polynomial in $L[x]$ has a root.

Example 24.16. $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

Proposition 24.5. *Any field has an algebraic closure, unique up to isomorphism. More generally, given any set of polynomials in $K[x]$, we can find a splitting field such that:*

1. *All polynomials in the set factorize into linear factors.*
2. *L is generated by the roots of the polynomials.*

Proof. Suppose there are a countable number of polynomials $p_1, p_2, p_3, \ldots$. Form

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots,$$

where K_n is a splitting field for p_n over K_{n-1}. The union is a splitting field. If we have an uncountable number of polynomials, use the magic words: Zorn's lemma. So we have found $L \supseteq K$ such that all polynomials in $K[x]$ have a root in L; we want that all polynomials in $L[x]$ have a root in L.

Suppose that p is irreducible in $L[x]$, and form $M = L[x]/p(x)$. Then the coefficients of p are all in K, so they all lie in some finite extension of K. So α is contained in a finite extension of K, so α is algebraic over K. This makes $\alpha \in L$ since any polynomial in $K[x]$ splits into linear factors in L.

Uniqueness of the algebraic closure is much like the uniqueness of splitting fields. □

[49] You may recall that these are the irreducible polynomials we computed in a previous lecture.

[50] In general, there is no preferred element to quotient out by. This is troublesome, because the fields you obtain are technically different, even though they are isomorphic.

It's difficult to find easy to explain examples of algebraic closures.

Example 24.17. Let K be the field of formal Laurent series over $\mathbb{C}$. This has elements $\cdots + a_{-n}z^{-n} + \cdots + a_0 + a_1 z + \cdots$ with $a_i \in \mathbb{C}$. The algebraic closure is

$$\bigcup_{k \geq 1} \text{formal Laurent series in } z^{1/k}.$$

These are called Puiseux series.[51]

[51] These date back to Newton, but they are not named after him because no one knew what algebraic closures were back then.

25 Normal, Separable and Galois Extensions

25.1 Normal extensions

Recall that the splitting field L of a polynomial p over K is a field such that all roots of p are in L, and L is generated by the roots.

Proposition 25.1. *L is the splitting field of some family of polynomials (over K) iff any irreducible $p \in K[x]$ splits into linear factors in L.*

Proof. Suppose p is irreducible in $K[x]$ and has a root $\alpha \in L$. Look at M, the algebraic closure of L. Any homomorphism $\varphi : K[\alpha] \to M$ extends to a homomorphism $\psi : L \to M$ as M is algebraically closed. But $\mathrm{im}(\psi)$ must be L as L is the splitting field of some family of polynomials; the splitting field is a uniquely determined subfield of M, as it is a subfield generated by a family. So α is already in L. □

Example 25.1. Reducible polynomials need not split into linear factors in L. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. $x^3 - 2$ has a root in L, but it does not split into linear factors.

Definition 25.1. A finite extension L/K is called *normal* if existence of 1 root of an irreducible polynomial p implies that p factors into linear factors.

So L/K is normal iff it its the splitting field of some family of polynomials.

Proposition 25.2. *Any degree 2 extension L/K is normal.*

Proof. Suppose α is a root of (say) $a^2 + ax + b = (a - \alpha)(a - \beta)$. We have that $\alpha + \beta = -a$, so $\beta = -a - \alpha$. So β is already in the field $K[\alpha]$. □

Example 25.2. $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not normal. $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$.

Example 25.3. Normal extensions of normal extensions need not be normal over the base field. $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ is not normal, but $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ are.

25.2 Separable extensions

Definition 25.2. A polynomial p is called *separable* if it has no multiple roots, i.e. if p, p' are coprime.

Definition 25.3. If L/K is an extension, $\alpha \in L$ is called *separable* if its irreducible polynomial is separable.

Definition 25.4. A field extension L/K is called *separable* if all its elements are separable.

Theorem 25.1. *L/K is separable if K has characteristic 0.*

Proof. α is a root of an irreducible p. We have that $\deg(p') < \deg(p)$, so p, p' have no common factors since p is irreducible. So p and p' are coprime. □

Remark 25.1. Why does this only work for characteristic 0? The statement that p, p' have no common factors does not hold if $p' = 0$; in algebra, this does not imply that p is constant if the characteristic of K is not 0.

Corollary 25.1. *Any extension F_q/F_p of finite fields is separable.*

Proof. Any element is a root of $x^q - x$. This has derivative -1, so $(f, f') = 1$. □

Example 25.4. Here is a non separable extension. Look at $F_p(t)$¡ the rational functions with coefficients in F_p (contains $F_p(t^p)$). $F_p(t^p) \subseteq F_p(t)$, so t is a root of $x^p - t^p$. This factors as $(x-t)^p$ because $(a+b)^p = a^p + b^p$, so all roots are the same. So t cannot be the root of any separable polynomial in $F_p(t^p)[x]$.

25.3 Galois extensions

25.3.1 Galois extensions and Galois groups

Definition 25.5. An extension is called *Galois* if it is separable and normal.

Definition 25.6. The *Galois group* $\mathrm{Gal}(L, K)$ of L/K is the group of automorphisms of L fixing all elements of K.

In a sense, the main point of Galois theory is that $\mathrm{Gal}(L, K)$ controls the extension L/K. So we can reduce facts about fields to facts about groups.

Lemma 25.1. *Suppose L/K is an extension of degree n and M/K is any extension. Then there are at most n ways to define a map $L \to M$ that acts as the identity on K.*

Proof. Suppose L is generated by α, so $L = K[\alpha]$. Then α is a root of a polynomial of degree $\leq n$. And $f(\alpha)$ is the root of a polynomial in M. This also have $\neq n$ roots in M, so there are $\leq n$ possibilities for $f(\alpha)$. So there are $\leq n$ possibilities for f.

Now suppose that L is generated by $\alpha, \beta, \gamma, \ldots$. Look at

$$K \subseteq K[\alpha] \subseteq K[\alpha, \beta] \subseteq \cdots$$

There are at most $[K[\alpha, \beta], K[\alpha]$ ways to extend a map from $K_[\alpha]$ to $K[\alpha, \beta]$. So there are $\leq [K[\alpha] : K][K[\alpha, \beta], K[\alpha]][K[\alpha, \beta, \gamma], K[\alpha, \beta]] \cdots$ ways to extend a map from K to L. But this is just $[L : K]$. □

So if L/K is an extension of degree n, there are at most N automorphisms of L fixing all elements of K.

Theorem 25.2. *For a finite extension L/K, the following are equivalent:*

1. *L is the splitting field of a separable polynomial.*

2. *L is Galois.*

3. *$[L : K] = |G|$, where G is the Galois group of L/K.*

4. *$K = L^G$ (the set of elements of L fixed by G).*

Proof. (1) $\implies$ (2): A splitting field is normal.

(2) $\implies$ (3): Look at $K \subseteq L \subseteq M$, where M is the algebraic closure of K. Look at maps $l \to M$ extending the identity map of K. Since L/K is separable, there are n such extensions ($n = [L : K]$). Why? Suppose L is generated by α of degree n (root of p). We can map α to any root of p in M, and p has n roots as it is separable. We leave the case where L is not generated by 1 element as an exercise.

L/K is normal, so the image of any map $L \to M$ lies in L. So there are $\geq n$ maps from L to L fixing K. From our lemma, we have that there are always $\leq [L : K]$ maps L to L, so $|g| = [L : K]$.

(3) $\implies$ (4): Look at $K \subseteq L^G \subseteq L$. There are $\geq n$ maps L to L extending L^G. So $[L : L^G] \geq n$. But $[L : K] = n$¡ so $K = L^G$.

(4) $\implies$ (1): Let $\alpha \in L$, Look at all conjugates of α under $G = \mathrm{Gal}(L/K)$. Look at $(x - \alpha)(x - \beta)(x - \gamma) \cdots$. This is in $K[x]$ as all coefficients are invaraiant under G, since $K = L^G$. So α is a root of a separabble polynomial as $\alpha, \beta, \gamma, \ldots$ are distinct. The polynomial splits into linear facts, which gives us normality. □

By our lemma, the third statement means that L is "as symmetric as possible."

Example 25.5. Take $x^3 - 2$ over $\mathbb{Q}$. This has 3 roots, $\sqrt[3]{2}$, $\sqrt[3]{2}w$, and $\sqrt[3]{2}w^2$, where w is a cube root of 1.

Let L be the splitting field. Then $[L : \mathbb{Q}] = 6$ because $[L : \mathbb{Q}[\sqrt[3]{2}]] = 2$, and $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. So $G = \mathrm{Gal}(L, \mathbb{Q})$ has order $6 = [L : \mathbb{Q}]$. It acts as permutations of α, β, γ, so it is the symmetric group S_3.

Example 25.6. Consider $\mathbb{C}/\mathbb{R}$. The Galois group has order 2, and is generated by complex conjugation $x + iy \mapsto x - iy$, which permutes the roots of $z^2 + 1 = 0$.

Example 25.7. Consider F_{16}/F_2. This is the splitting field of $x^{16} - x$, so it is Galois. So the galois grou[has order $4 = [F_{16} : F_2]$. What is it?

One element is the Frobenius element[52] φ, which takes $a \mapsto a^2$. Then $\varphi(ab) = \varphi(a)\varphi(b)$, and $\varphi(a + b) = \varphi(a) + \varphi(b)$ since $(a + b)^2 = a^2 + b^2$ in F_2. If a is fiixed by φ, then $a^2 = a$, so $a = 1$ or 0. So $a \in F_3$. So φ generates the Galois group, and $\varphi^4 = \mathrm{id}$. $\varphi 4(a) = (((a^2)^2)^2)^2 = a^{16} = a$. So the Galois group is $\mathbb{Z}/4\mathbb{Z}$.

[52] According to Professor Borcherds, the φ stands for Frobenius, even though Frobenius was German, not Greek. I can't tell if this was a joke or not.

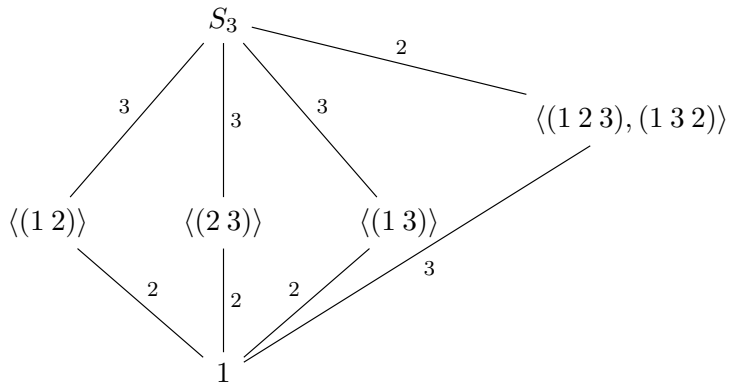
25.3.2 Galois groups and subextensions

Theorem 25.3. *Suppose M/K is a Galois extension with Galois group G. For any subextension L ($K \subseteq L \subseteq M$), $\mathrm{Gal}(M/L)$ is a subgroup of G. Conversely, any subgroup $H \subseteq G$ induces a subextension M^H, the elements fixed by H.*

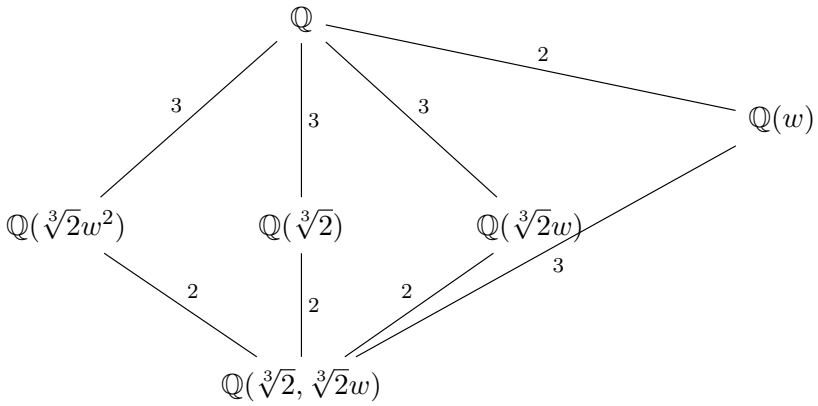
In effect, we want to prove a bijection between subfields of M containing K and subgroups of G. We have a major problem: bigger subfields correspond to smaller subgroups.[53]

This can really be a source of confusion. Suppose that $K \subseteq L \subseteq M$, where L, M are Galois extensions of K. Then $\mathrm{Gal}(M, K)$ is bigger than $\mathrm{Gal}(L, K)$.

Example 25.8. Let's find all fields between $\mathbb{Q}$ and the splitting field of $x^3 - 2$. Look at the Galois group S_3. The subgroups of S_3 are:



The subextensions of this splitting field are:



The indices of the subgroups will correspond to the degrees of the subextensions.

[53] Professor Borcherds has been doing Galois theory for decades, but this still trips him up sometimes.

Example 25.9. Let ζ be the a 7th root of unity in $\mathbb{C}$. Then $\zeta^7 = 1$, and $\zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta^+ 1 = 0$, where this polynomial is irreducible. This is $(x - \zeta)(x - \zeta^2) \cdots (z - \zeta^6)$. So $\mathbb{Q}[\zeta]$ is normal of degree 6.

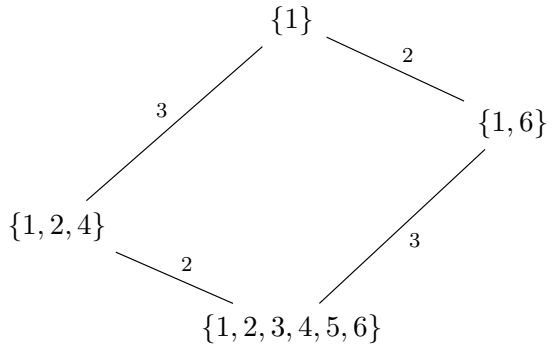
The Galois group has order $6 = [\mathbb{Q}[\zeta] : \mathbb{Q}]$. What is it? Suppose that σ is in the Galois group. Then $\sigma(\zeta)$ is a root of $x^6 + x^5 + x^4 + x^3 + x^2 + x^+ 1$, so it is ζ^k for some $1 \leq k \leq 6$. Similarly, for τ, $\tau(\zeta) = \zeta^\ell$, so $\sigma\tau(\zeta) = \zeta^{k\ell}$. So the Galoid group is the group is $(\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$, which is cyclic. There are 4 subgroups of orders 1, 2, 3, and 6, respectively (of index 6, 3, 2, and 1), so there are 4 extension of $\mathbb{Q}$ contained in $\mathbb{Q}[\zeta]$, of degrees 6, 3, 2, and 1.

26 The Fundamental Theorem of Galois Theory

26.1 Proof and an example

Here is the example of the fundamental theorem that we started last time:

Example 26.1. Last time we had $L = \mathbb{Q}[\zeta]$, where $\zeta = e^{2\pi i/7}$. We wanted to find all subfields of L. This had the Galois group $(\mathbb{Z}/7\mathbb{Z})^*$, which has subgroups



We should have 2 intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta)$, of degree 2 and 3. What are they?

Let's find the degree 2 field. The elements are fixed by $H = \{1, 2, 4\}$. One fixed element is $a = \zeta + \zeta^2 + \zeta^4$, which is not in $\mathbb{Q}$. What is a? We must find a quadratic equation with root a.

$$a^2 = \zeta + \zeta^2 + 2\zeta^3 + \zeta^4 + 2\zeta^5 + 2\zeta^6$$
$$a^2 + a = 2)\zeta + \zeta^2 + \cdots + \zeta^6$$

So $a^2 + a + 2 = 0$, which makes $a = \frac{-1+\sqrt{-7}}{2}$. So the degree 2 field is $\mathbb{Q}[a] = \mathbb{Q}[\sqrt{-7}]$.

Let's find the degree 3 subfield. Let $J = \{1, 6\}$. Look for an invariant element; we choose $\zeta + \zeta^6 = \zeta + \zeta^{-1}$. Note that $\zeta = e^{2\pi i/7} = \cos(2\pi/7) + i\sin(2\pi/7)$. So $\zeta + \zeta^{-1} = 2\cos(2\pi/7)$.

Alternatively, we can find the irreducible equation it satisfies. We have

$$(\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}.$$
$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2}.$$

Since $\zeta^3 + \zeta^2 + \zeta + \cdots + \zeta^{-3} = 0$, we have that $\zeta - \zeta^{-1}$ is a root of $x^3 + x^2 - 2x - 1$. The 3 roots of this polynomial are $2\cos(2\pi/7)$, $2\cos(4\pi/7)$, and $2\cos(8\pi/7)$.

Theorem 26.1 (Fundamental theorem of Galois theory)**.** *Let M/K be a Galois extension with Galois group G. Then there is a correspondence of subextensions L of M with subgroups H of G given by $L \mapsto \mathrm{Gal}(M/L)$. and $H \subseteq G \mapsto M^H$. Moreover, these maps are inverses of each other.*

Proof. We want to show that $L = M^{\mathrm{Gal}(M/L)}$. We have $L \subseteq M^{\mathrm{Gal}(M/L)}$, so it is enough to show that they have the same size. We show that they have the same index in M.

Similarly, we have that $H \subseteq \mathrm{Gal}(M : M^H)$., so to show that they are the same, it also suffices to show that they are the same size. So the theorem follows if we show:

1. $|\mathrm{Gal}(M : L)| = [M : L]$.
2. $[M : M^H] = |H|$.

The key point is to recall our lemma from last lecture: if $K \subseteq L$ and $K \subseteq M$, there are at most $[L : K]$ maps $L \to M$ extending the identity map of K.

To prove the first statement, observe that $|\mathrm{Gal}(M/L)| \leq [M : L]$ by the lemma. Now suppose it is strictly less. Look at $K \subseteq L \subseteq M$. Byt the multiplicativity of indices, there are $< [L : K][M : L] = [M : K]$ maps from $M \to M$. But since M/K is Galois, there are exactly $[M : K]$ maps $M \to M$, which is a contradiction.

The proof of the second statement is similar, and we leave it as an exercise. □

26.2 Applications of the fundamental theorem

26.2.1 Construction of a 17-sided regular polygon

We can use Galois theory to prove the existence of a construction of a 17-sided regular polygon using a ruler and compass.[54]

Example 26.2. We want to construct ζ, where $\zeta^{17} = 1$. We have $\frac{\zeta^{17}-1}{\zeta-1} = 0$. Recall that this was an irreducible polynomial of degree 16. The idea is that we can find intermediate fields $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\zeta)$. We can construct degree 2 extensions with a ruler and compass because we can construct square roots with a ruler and compass.

Look at the Galois group $(\mathbb{Z}/17\mathbb{Z})^* \cong \mathbb{Z}/16\mathbb{Z}$. This has subgroups $0 \subseteq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z} \subseteq \mathbb{Z}/8\mathbb{Z} \subseteq \mathbb{Z}/16\mathbb{Z}$, so we can find the desired field extensions. If we want to find out what the fields are, we can proceed as earlier. Explicitly, the subgroups are

$$\{0\} \subseteq \{1, 16\} \subseteq \{1, 4, 13, 16\} \subseteq \{1, 2, 4, 8, 9, 13, 15, 16\} \subseteq \mathbb{Z}/16\mathbb{Z},$$

so we can find the fixed fields of these subgroups:

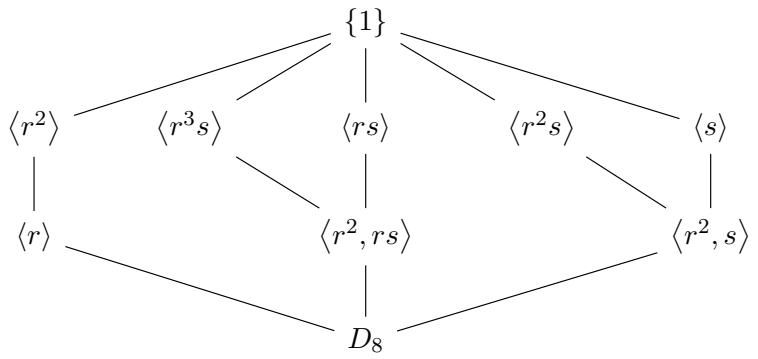
$$\mathbb{Q}(\zeta), \mathbb{Q}(\zeta + \zeta^1 6), \mathbb{Q}(\zeta + \zeta^4 + \zeta^{13} + \zeta^{16}), \mathbb{Q}(\zeta^1 + \zeta^2 + \zeta^4 + \cdots).$$

26.2.2 Subextensions of a splitting field

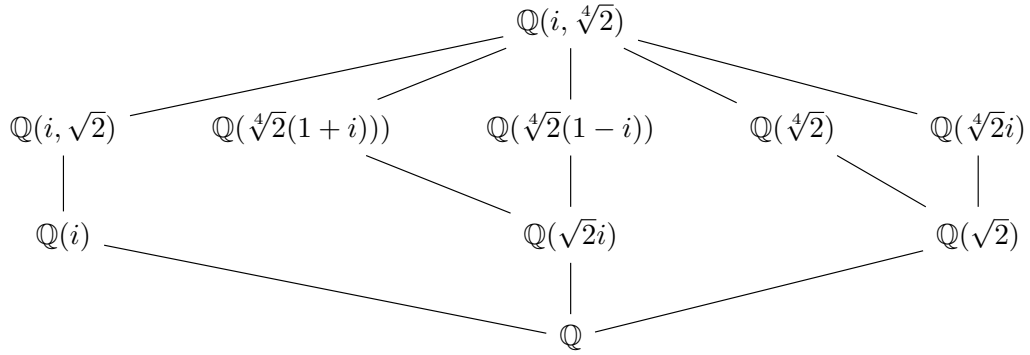
Example 26.3. Let's find all the subextensions of $x^4 - 2$ over $\mathbb{Q}$. This has the roots $\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}$, and $\sqrt[4]{2}i$. We have that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$, so the splitting field has degree 8 over $\mathbb{Q}$. If we draw out the roots in the complex plane, we get

[54] Gauss became famous as a teenager by becoming the first to give an explicit construction.

the vertices of the square. So the Galois group is the group of symmetries of the square, D_8. Its subgroups are:



So the subextensions are:



26.3 Extensions corresponding to normal subgroups and factor groups

In the previous example, The 3 subgroups of order 4 and the first subgroup of order 2 are normal. The other four subgroups of order 2 come in conjugate pairs. We can see that the corresponding extensions are normal. This is true in general.

Proposition 26.1. *Let $H \subseteq \mathrm{Gal}(L/K)$. Then H is normal iff L^K/K is a normal extension.*

Proof. H is normal iff all conjugates of H under G are the same as G. L/K is normal iff all conjugates of L under the Galois group are the same as L. □

Suppose L/K is a field extension corresponding to H and is normal. What is the Galois group of L/K? A standard blunder is to think that it is H, which is actually $\mathrm{Gal}(M/L)$. In fact, $\mathrm{Gal}(L/K) = G/H$. If we have $\mathrm{Aut}(M) \to \mathrm{Aut}(L)$, the kernel is everything fixing all elements of L. This is H.

26.4 Finding extensions corresponding to a given group

Proposition 26.2. *Let G be a finite group. Then there is a Galois extension L/K with Galois group G.*

Proof. First take $G = S_n$, and let $L = \mathbb{Q}(x_1, x_2, \ldots, x_n)$, all rational functions in L variables. Now let $K = L^{S_n}$, the symmetric rational functions. If G is any finite group acting on any field L, then L/L^G is Galois with group G. So L/L^{S_n} is a Galois extension with Galois group S_n. The same works for when G is a subgroup of S_n; L/L^G has Galois group G. The result follows by Cayley's theorem, that any finite group is a subgroup of some permutation group. □

This is very hard if you want a specific field K. The following is still an open problem: "Given a finite group G, is there an extension of $\mathbb{Q}$ with Galois group G?"

Example 26.4. Let $G = \mathbb{Z}/5\mathbb{Z}$ and let $\zeta^{11} = 1$. Notice that $\mathbb{Q}[\zeta]$ has Galois groups $\mathbb{Z}/11\mathbb{Z})^* \cong \mathbb{Z}/10\mathbb{Z}$, which has the quotient, $\mathbb{Z}/5\mathbb{Z}$. Explicitly, if we take the field $\mathbb{Q}(\zeta)^{\mathbb{Z}/2\mathbb{Z}}$, then its Galois group is $(\mathbb{Z}/10\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$.

Example 26.5. Let's find an extension of $\mathbb{Q}$ with Galois group S_5 (order 120). We take the splitting field of $x^5 - 4x + 2$. This is irreducible by Eisenstein's criterion. If you look at the graph, it has exactly 3 real roots (and hence 2 complex roots). The Galois group is a subgroup of S_5, the permutations of the 5 roots. The Galois group contains a 5-cycle, say $(1\,2\,3\,4\,5)$, so its order is divisible by 5. The Galois group also contains a transposition (complex conjugation). A 5 cycle and a transposition generate S_5 (exercise). So the Galois group of this splitting field is S_5.

This example generalizes into the following result:

Proposition 26.3. *If p is prime ,we can find an extension $L/\mathbb{Q}$ with Galois group S_p.*

Corollary 26.1. *If G is finite, we can find extiensions L/K of $\mathbb{Q}$ with* $\mathrm{Gal}(L/K) = G$.

Proof. Let L be the extension with $\mathrm{Gal}(L/\mathbb{Q}) = S_p$ for some large p. Take $G \subseteq S_p$, and let $K = L^G$. □

27 Examples in Galois Theory and Primitive Elements

27.1 Galois group of an irreducible degree 3 polynomial

Consider an irreducible polynomial $x^3 + ax^2 + bx + c = 0$. The Galois group $G \subseteq S_3$, the permutations of the roots. 3 divides the order of the Galois group, so $G = \mathbb{Z}/3\mathbb{Z}$, so $\mathbb{Z} = S_3$.

Example 27.1. Take $x^3 - 2$ over $\mathbb{Q}$. The Galois group is S_3.

Example 27.2. Take $x^3 + x + 1$ over F_2. The Galois group is $\mathbb{Z}/3\mathbb{Z}$.

We look at $\Delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$, where α, β, and γ are the roots of the polynomial. Δ is fixed by $\mathbb{Z}/3\mathbb{Z}$, but changes sign under odd permutations of α, β, γ. If the Galois group is $\mathbb{Z}/3\mathbb{Z}$, Δ must be in the base field. If the Galois group is S_3, $\Delta \mapsto -\Delta$ must be an automorphism. We must find if

$$\Delta^2 = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2$$

has a square root in the base field. This is a symmetric function of α, β, γ, and we can compute this as

$$\Delta^2 = -4b^3 - 27c^2$$

if $a = 0$.

Example 27.3. Take $x^3 - 3x - 1$ over $\mathbb{Q}$. $\Delta^2 = 81$, which is a square in $\mathbb{Q}$. So the Galois group is $\mathbb{Z}/3\mathbb{Z}$.

27.2 Algebraic closure of $\mathbb{C}$

We have enough tools to provide a mostly algebraic proof of the fundamental theorem of algebra: that $\mathbb{C}$ is algebraically closed.

Theorem 27.1. *$\mathbb{C}$ is algebraically closed.*

Proof. We will use the following facts about $\mathbb{R}, \mathbb{C}$:

1. $\mathbb{R}$ has characteristic 0.
2. Any polynomial of odd degree over $\mathbb{R}$ has a real root (follows from intermediate value theorem).
3. $[\mathbb{C} : \mathbb{R}] = 2$, and every element of $\mathbb{C}$ has a square root in $\mathbb{C}$.

Let L be a finite extension of $\mathbb{C}$; we want to show that $L = \mathbb{C}$. We may as well extend L to a Galois extension ($\text{char}(\mathbb{C}) = 0$, so L is automatically separable). So we have $R \subseteq \mathbb{C} \subseteq L$. Let $G = \text{Gal}(L/\mathbb{R})$. We want to show that G has order 2. Fact 2 above gives us that G has no subgroups of odd index > 1 as $\mathbb{R}$ has no extensions of odd degree. Let H be a subgroup of $\mathbb{C}$, so H has index 2 in G. Fact 3 gives us that H has no subgroups of index 2 (since $\mathbb{C}$ has no extensions of index 2).

Let S be a 2-Sylow subgroup of G. S has odd index, so $S = 6$ by fact 2. So $G = S$ has order 2^n for some n. So H has order 2^{n-1}. If $n - 1 > 0$, H has subgroups of index 2, which would contradict fact 3, so $|H| = 1$, and $|G| = 2$. So $\mathbb{C}$ is algebraically closed. □

27.3 Primitive elements of separable extensions

Lemma 27.1. *Suppose V is a vector space over an infinite field K. Then V is not a union of finitely many proper subspaces.*

Proof. By induction. Let $V_1, \ldots, V_n$ be proper subspaces. Choose v no in $V_1, \ldots, V_{n-1}$ by induction. Choose $w \notin V_n$. Look at $v + kq$ for $k \in K$. There is at most 1 value of k for which this is in V_i for any given i. Since K is infinite, we can choose k so that $v + kq$ is not in any V_j. □

Theorem 27.2. *If L/K is a finite separable extension, L is generated by 1 element; i.e. there exists some $\alpha \in L$ such that $L = K(\alpha)$.*

Proof. There are only finitely many extensions between K and L. Let M be a Galois extension containing L. Then there ares only finitely many extensions of K in M, as these correspond to subgroups of the Galois group. Each extension is a vector space over K. Suppose K is infinite. Then the vector space L is not a union of a finite number of subspaces, so some element $\alpha \in L$ is not in any smaller extension of K. So $L = K(\alpha)$. If K is finite, then L is finite, so L^* is cyclic. □

Example 27.4. Let $F_p(t^p, u^p) \subseteq F_p(t, u)$. This has degree p^2 because

$$[F_p(t,u) : F_p(t,u^p)] = [F_p(t,u^p) : F_p(t^p,u^p)] = (p)(p) = p^2.$$

Every element a of $F_p(t,u)$ generates an extension of degree p or 1. In fact, $a^p \in F_p(t^p, u^p)$ for t or u since $(x+y)^p = x^p + y^p$ and $(xy)^p = x^p y^p$. So this is true for all polynomials in t, u. So $F_p(t,u)$ is not generated by 1 element, and there are infinitely many extensions between $F_p(t^p, u^p)$ and $F_p(t,u)$.

This is an example of a *purely inseparable* extension. These tend to be very weird and break your intuition. [Jacobson: in some cases subfields iff subalgebras of Lie algebra]

27.4 Primitive elements of extensions with Galois group $\mathbb{Z}/p\mathbb{Z}$

Suppose L/K is a Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$ (cyclic). What can we say about L? Suppose $K = \mathbb{Q}(\zeta)$, where ζ is a primitive p-th root of unity. $L = K(\sqrt[p]{a})$ for some $a \in K$. This is a root of $x^p - a$. The other roots are $\sqrt[p]{a}$, $\sqrt[p]{a}\zeta$, $\sqrt[p]{a}\zeta^2, \ldots$. Any element of the Galois group takes $\sqrt[p]{a}$ to $\sqrt[p]{a}\zeta^i$ for some i. So the Galois groups is a subgroup of $\mathbb{Z}/p\mathbb{Z}$, making it 1 or $\mathbb{Z}/p\mathbb{Z}$ itself.

Suppose K contains all p-th roots of unity and K has characteristic $\neq p$. We want to show that $L = K(\sqrt[p]{a})$ for some a. How do we find this element? Let σ be a generator of the Galois group $\mathbb{Z}/p\mathbb{Z}$, so $\sigma^p = 1$. The key idea is to look at the action of σ on the vector space L over K (forget that L is a field). σ is a linear transformation, so we can look at its eigenvalues and eigenvectors. We hope to diagonalize σ.

$\sigma^p = 1$, so its eigenvalues are the roots of $x^p = 1$, which are contained in K. Now let's find eigenvectors. Pick any $v \in L$. Look at $v + \sigma v + \sigma^2 v + \cdots + \sigma^{p-1} v$, which has eigenvalue 1. Similarly, $v + \zeta\sigma v + \zeta^2\sigma^2 v + \cdots + \zeta^{p-1}\sigma^{p-1} v$ has eigenvalue ζ^{-1}. We then get $v + \zeta^{-1}\sigma v + \zeta^{-2}\sigma^2 v + \cdots + \zeta^{-(p-1)}\sigma^{p-1} v$ is an eigenvector with eigenvalue $\zeta = \zeta^{1-p}$. Note that v is the average of these, since $v = 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$. So L is a direct sum of p 1 dimensional subspaces, on which σ acts as $1, \zeta, \zeta^2, \zeta^3, \ldots$.

Pick w to be any eigenvector of σ with eigenvalue $\neq 1$ (so $q \notin K$, where K is an subspace with eigenvalue = 1). Then $\sigma w = \zeta w$, say, which gives $\sigma w^p = \zeta^p w^p = w^p$. So $w^p \in K$ as it is fixed by σ. Put $a = w^p \in K$. Then $L = K(\sqrt[p]{a})$. So we have shown that

Proposition 27.1. *If L/K is a Galois extension such that*

1. *$Gal(L/K) = \mathbb{Z}/p\mathbb{Z}$,*
2. *K contains roots of $1 + x + \cdots + x^{p-1} = 0$,*
3. *K has characteristic $\neq p$,*

then $L = K(\sqrt[p]{a})$ for some $a \in K$.

What if K has characteristic p? Assume that L/K is Galois, $[L : K] = p$. Again, let σ be a generator of the Galois group. L cannot be of the form $K(\sqrt[p]{a})$ because $x^p - a$ is inseparable (all roots are the same). So the splitting field is not Galois! Look at the eigenvalues and eigenvectors of σ on the vector space L. $\sigma^p = 1$, so $\sigma - 1)^p = 0$. So $\sigma - 1$ is nilpotent and not diagonalizable! The only eigenvalue is 1, and the eigenspace is K.

Nilpotent matrices look something like this:

$$M = \begin{bmatrix} 0 & * & * & * \\ & 0 & * & * \\ & & 0 & * \\ & & & 0 \end{bmatrix}$$

The eigenvectors of M are no use, but generalized eigenvectors, $(M-\lambda)^n = 0$, are useful. So try to find the easiest generalized eigenvector, $(\sigma-1)^2 v = 0$. This means that $(\sigma-1)v \in K$, as it is fixed by σ. So $\sigma v - v = a$ for some $a \in K$ and $v \in L$. Changing v to v/a, we get $\sigma v - v = 1$. This is the simplest substitute for an eigenvector. Instead of $\sigma v = \lambda v$, we have $\sigma v = \lambda v + 1$. So $\sigma v = v + 1$, and $\sigma v^p = v^p + 1$. Then $\sigma(v^p - v) = v^p - v$, so $v^p - v \in K$. So r is a root of $x^p - x - b = 0$ for some $b \in K$. This is called an *Artin-Schrier equation*, the analogue of $x^p - b$. So $L = K(v)$, where v is a root of an A-S polynomial.

Suppose v is a root of $x^p - x - b = 0$ in characteristic p. What are the other roots?

$$(v+1)^p - (v+1) - b = v^p + 1 - v - 1 - b = v^p - v - b = 0$$

So the other roots are $v, v+1, v+2, \ldots, v+(p-1)$. This is p distinct roots. So $K(v)$ is Galois because it is separable (distinct roots) and normal (given one root, we can find the others). The Galois group is a subgroup of $\mathbb{Z}/p\mathbb{Z}$.

Over characteristic p, there are 2 possibilities:

1. $x^p - x - b$ is irreducible, so it is a Galois extension with Galois group $\mathbb{Z}/p\mathbb{Z}$.
2. $x^p - x - b$ factors into linear factors (b is of the form $c^p - c$ for $c \in K$).

Example 27.5. We can apply this to the construction of finite fields. What was the issue with order p^2? $F_p(\sqrt[p]{a})$, a is not a square in F_p, but there is no neat way to write down a in general. We can choose a choice of irreducible polynomial. What about p^p? In this case, we can take a root of $x^p - x - 1$. Check that this has no roots over F_p. $x^p - x = 0$ for all $x \in F_p$.

Given a polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_n$, a classical problem is to find formulas for its roots. For example, $x^2 + bx + c$ has roots $x = \frac{-b \pm \sqrt{b^2-4c}}{2}$. There are no formulas for 5th degree polynomials; we will show this next time.

28 Cyclic Extensions and Cyclotomic Polynomials

28.1 Cyclic extensions

Definition 28.1. A *cyclic extension* is a Galois extension with a cyclic Galois group.

Last time, we determined that a cyclic extension L/K is $K[\sqrt[n]{a}]$ if the characteristic does not divide n and $K[\alpha]$ otherwise, where $\alpha^p - \alpha - b = 0$; also note that the former element is the solution to $a^p - a = 0$. The nice thing about this is that if we know one root, α, thenwe know other roots ($\alpha\zeta^i$ and $\alpha + i$, respectively).

Which polynomials can be "solved by radicals"? What we means is that roots can be written using addition, subtraction, multiplication, and k-th roots. For example, the roots to a quadratic equation $ax^2 + bx + c$ are $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.[55]

Theorem 28.1. *The Galois group is solvable iff roots can be given using radicals and Artin-Schrier equations (char > 0).*

Proof. Suppose an equation is solvable by radicals. Assume that the base field K contains all roots of 1 we need. Look at $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq L$, where L is the splitting field of the polynomial. $K_1 = K_0(\sqrt[n]{\alpha_1})$. Look at the Galois groups:

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq 1.$$

G_2 is normal in G_1, and G_1/G_2 is cyclic. G has a chain of subgroups, each normal in the next, and all quotients are cyclic. So G is solvable.

Suppose G is solvable (and K contains all roots of 1). We have

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq 1,$$

where G_i is normal in G_{i-1}, and G_{i-1}/G_i is cyclic of prime order. Look at the fields

$$K \subseteq \underbrace{K_1}_{=L^{G_1}} \subseteq \underbrace{K_2}_{=L^{G_2}} \subseteq \cdots \subseteq L.$$

K_{i+1}/K_i is a cyclic Galois extension, so $K_{i+1} = K_i(\sqrt[n]{\alpha_n})$ or Artin-Schrier. □

Example 28.1. Consider $x^5 - 4x + 2$. The Galois group is S_5, which has order 120. The only normal subgroups are 1, A_5, and S_5. This polynomial is not solvable by radicals.

Example 28.2. $x^5 - 2$ is irreducible and of degree 5, but it can be solve by radicals. The Galois group is solvable. The field extensions look like $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\zeta, \sqrt[5]{2})$. The corresponding groups of the wuotients of the Galois groups are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$, which are cyclic.

[55] Mathematicians used to duel for money and prestige, presenting each other with difficult problems to solve. Cardano came up with a general solution for finding roots of degree 4 polynomials, which became a valuable asset for him in these duels.

Example 28.3. All polynomials of degree ≤ 4 can be solved by radicals (in characteristic 0), the Galois groups is a subgroup of S_4, so it is solvable. We have

$$S_4 \supseteq A_4 \supseteq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \supseteq 1.$$

28.2 Cyclotomic polynomials

Over $\mathbb{Q}$, the roots of unity are the roots of $x^n - 1 = 0$. How does this factor into irreducibles? Look at $x^{12} - 1$. This is divisible by $x^6 - 1$, $x^4 - 1$, $x^3 - 1$, etc., but these have factors in common.

Definition 28.2. The n-th *cyclotomic polynomial* $\Phi_n(x)$ is the polynomial with roots the primitive n-th roots of unity (order exactly n).

Example 28.4. Let's compute some examples:

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^3 + x + 1 = \frac{x^3-1}{x-1}$
4	$x^2 + 1 = \frac{x^4-1}{x^2-1}$
5	$x^4 + x^3 + x^2 + x + 1 = \frac{x^5-1}{x-1}$
6	$x^2 - x + 1 = \frac{(x^6-1)(x-1)}{(x^3-1)(x^2-1)}$

Example 28.5. We have to make sure we're not dividing by factors multiple times, so we must put an $x - 1$ in the numerator:

$$\Phi_{12}(x) = \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 + 1$$

$$x^{12} - 1 = \Phi_{12}(x)\Phi_6(x)\Phi_4(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).$$

Example 28.6. Again, we make sure we don't divide by factors multiple times.

$$\Phi_{15}(x) = \frac{(x^{15} - 1)(x - 1)}{(x^5 - 1)(x^3 - 1)} = x^8 - x^7 + x^5 - x^4 + x^2 - x + 1.$$

If you want to really understand cyclotomic polynomials, try out the following exercise: Find the smallest n such that $\Phi_n(x)$ has a coefficient not 0 or ± 1.[56]

Theorem 28.2. *$\Phi_n(x)$ is irreducible over $\mathbb{Q}$. It's Galois group is $(\mathbb{Z}/n\mathbb{Z})^*$.*

[56] You may have to check $n > 100$, but do not just do this brute force. You should do small cases and notice some kind of pattern.

Proof. If b is prime, we have proved this using Eisenstein's criterion. A similar proof works for prime powers. For general n, we use a different argument. The first key idea is to reduce $\pmod p$ for primes p. The second key idea is to use the Frobenius map, $F(t) = t^p$, where the field has characteristic p; F is an automorphism.

Suppose f is an irreducible factor of $\Phi_n(x)$ (over $\mathbb{Q}$). Form $\mathbb{Z}[\zeta] = \mathbb{Z}[x]/f(x)$. This is an integral domain, and the quotient field $\mathbb{Q}(\zeta)$ is generated by a primitive n-th root ζ of 1. Use $\mathbb{Z}$, not $\mathbb{Q}$ to reduce mod p. $\mathbb{Z}[\zeta]$ contains n distinct roots of $x^n - 1$: $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$. Now choose an irreducible factor $g(x)$ of $f(x)$ in $F_p(x)$ (factor $f \pmod p$). In general, $\deg g < \deg f$. The key point is that since $x^n - 1$ has n distinct roots, $nx^{n-1} = \frac{d}{dx}(x^n - 1)$ and $x^n - 1$ are coprime.

Since ζ is a root of g (which is irreducible), ζ^p is also a root of g as $t \mapsto t^p$ is an automorphism of $F_p(\zeta)$. So in $\mathbb{Z}[\zeta]$, ζ^p is also a root of f. Then the map from roots of unity in $\mathbb{Z}[s]$ to roots of unity in $F_p[\zeta]$ is bijective. So if p does not divide n, then the roots of f are closed under the map $\zeta \mapsto \zeta^p$.

Now look at the Galois group of $\mathbb{Z}[\zeta]$. Automorphisms take $\zeta \mapsto \zeta^k$ for k, n coprime, so the Galois group is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. The Galois group contains $\zeta \mapsto \zeta^p$ for p, n coprime, which generate $(\mathbb{Z}/n\mathbb{Z})^*$. So the Galois group equals $(\mathbb{Z}/n\mathbb{Z})^*$, so $f = \Phi_n(x)$. □

Definition 28.3. A cyclotomic[57] field is a field generated by roots of unity.

28.3 Applications of cyclotomic polynomials

28.3.1 Primes modulo n

Theorem 28.3. *Suppose $n \in \mathbb{Z}$. There are infinitely many primes $p > 0$ with $p \equiv 1 \pmod n$.*[58]

Proof. The idea is to look at the primes P dividing $\Phi_n(a)$ for some a. Suppose p, n are coprime. Then all roots of $\Phi_n(x)$ are distinct mod p. So $\Phi_n(x)$ is coprime to $\Phi_m(x)$ in $F_p(x)$ for m dividing n. So if $p \mid \Phi_n(a)$, p does not divide $\Phi_m(a)$ for $m \mid n$. This says that if $\Phi_n(a) \equiv 0 \pmod p$, then $\Phi_m(a) \not\equiv 0 \pmod p$ when $m \mid n$. So if $a^n \equiv 1 \pmod p$, then $a^m \neq 1 \pmod p$ for $m \mid n$. So a has order exactly $n \pmod p$, so n divides $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$, so $p = 1 \pmod n$.

So if $p \mid \Phi_n(a)$, then either $p \mid n$ or $p \equiv 1 \pmod n$. Suppose $p_1, \ldots, p_k$ are $1 \pmod n$. Choose p dividing $\Phi_n(np_1 \cdots p_k)$. $\Phi_n(x) = 1 + x + \cdots$, so this is $1 \pmod n p_1 \cdots p_k$, so p does not divide $p_1 \cdots p_k$. Then p does not divide n. So we have found p, a new prime $\equiv 1 \pmod n$. □

[57] "Cyclo" means "circle," and "tomic" means "cut."

[58] Dirichlet proved this for $p \equiv a \pmod n$ for any a coprime to n, but the proof is not as nice. There seems to be no known way to extend the nice proof to this more general case, which frustrates some people.

Example 28.7. Let $n = 8$. Then $\Phi_8(a) = a^4 + 1$. if $a = 1$, we get 2, which divides 8. If $a = 2$, we get 9, which is 1 (mod 8). If $a = 3$, we get $82 = 41 \times 2$; $41 \equiv 1 \pmod 8$, and $2|8$.

28.3.2 Galois extensions over $\mathbb{Q}$

Recall the hard problem: given finite G, is G a Galois group of $K/\mathbb{Q}$ for some K?

Theorem 28.4. *If G is abelian, there exists some $K/\mathbb{Q}$, such that G is the Galois group of $K/\mathbb{Q}$.*

Proof. Write G as a product of cyclic groups:

$$G = (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots .$$

Choose distinct primes $p_1 \equiv 1 \pmod n)_1$, $p_2 \equiv 1 \pmod n)_2, \cdots$. $(\mathbb{Z}/n_1\mathbb{Z})$ is a quotient of $(\mathbb{Z}/p + 1\mathbb{Z})^*$. So G is a quotient of $\mathbb{Z}/p_1\mathbb{Z} \times \mathbb{Z}/p_2\mathbb{Z} \times \cdots)^* = (\mathbb{Z}/p_1p_2 \cdots \mathbb{Z})^*$, which is the Galois group of $x^{p_1,\cdots p_n} - 1$. So any quotient G/H is the Galois group of some extension $K/\mathbb{Q}$. □

Here is a type of converse, which we will not prove.

Theorem 28.5 (Kronecker-Weber-Hilbert)**.** *If K is a Galois extension of $\mathbb{Q}$ with abelian Galois group, then $K \subseteq \mathbb{Q}(\zeta)$ for some root of unity ζ.*

28.3.3 Finite division algebras

Can we find finite analogues of the quaternions $\mathbb{H}$? This is a division algebra that is a "non-commutative field."

Theorem 28.6 (Wedderburn)**.** *Any finite division algebra is a field (commutative).*

Proof. Recall that any group G is the union of its conjugacy classes, which have sizes $|G| / |H|$, where H is a subgroup centralizing a representative element of a conjugacy class.

Let L be a finite division algebra, and let K be its center, a field F_q of order q for some prime power q. Look at the group $G = L^*$, which has order $q - 1$. Suppose $a \in G$. The centralizer of a in L is a subfield of order q^k for some k, so the centralizer of a in G is a subfield of order $q^k - 1$ ($0 \notin G$). So

$$q^{n-1} = q - 1 + \sum_i \frac{q^n - 1}{q^{k_i - 1}},$$

where the sum is over conjugacy classes of orders > 1. Note that $k_1 < n$.

Now note that q^{n-1} is divisible by $\Phi_n(q)$. Also note that so is $(q^n - 1)/(q^{k_i - 1})$, as $k_1 < n$. So $q - 1$ is divisible by $\Phi_n(x) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*}(q - \zeta^i)$. But observe that $|q - \zeta_i| > q - 1$ unless $\zeta^i = 1$. So $n = 1$. So $L = K$, which makes L commutative. □

Definition 28.4. The *Brauer group* is the group of isomorphism classes of a finite dimensional division algebras over a field K with center K.

Example 28.8. The Brauer group of $\mathbb{R}$ has 2 elements: $\mathbb{R}$, and $\mathbb{H}$.

If D_1, D_2 are division algebras, $D_1 \otimes_K D_2 \cong M_n(D_3)$ for some n, D_3, where D_3 is the product of D_1, D_2 in the Brauer group.

Remark 28.1. Wedderburn's theorem shows that the Brauer group of a finite field is trivial.

28.4 Norm and trace in finite extensions

Let L/K be a finite extension, and choose $a \in L$. Multiplication by a is a linear transformation from $L \to L$, where L is viewed as a vector space over K.

Definition 28.5. The *trace* of a is defined as the trace of a as a linear transformation. The norm of a is the determinant of a as a linear transformation.

Definition 28.6. The *norm* of a is the determinant of a as a linear transformation.[59]

Example 28.9. Take $\mathbb{C}/\mathbb{R}$ and $a = x + iy \in \mathbb{C}$. A basis for $\mathbb{C}/\mathbb{R}$ is $\{1, i\}$. $a \cdot 1 = x + iy$, and $a \cdot i = -y + ix$. So a is given by the matrix

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix}.$$

So the trace of a is $2x$, and the norm is $x^2 + y^2$.

[59] Ignore Lang's definition. Professor Borcherds thinks it is "silly."

29 Norm and Trace

29.1 Norm and trace of finitely generated extensions

Let L/K be a field extension. The norm and the trace satisfy

$$N(ab) = N(a)N(b)$$

$$\operatorname{tr}(a+b) = \operatorname{tr}(a) + \operatorname{tr}(b),$$

so we can think of the norm and trace as homomorphisms $L^* \to K^*$ under $\times$ and $L \to K$ under $+$, respectively.

Suppose a generates L/K ($L = K(a)$). a satisfies an irreducible polynomial $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$. What are the trace and norm of a? Choose a basis for L over K, say $\{1, a, a^2, \ldots, a^{n-1}\}$. Then multiplying by a makes $1 \mapsto a$, $a \mapsto a^2$, ... So a is given by the matrix

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & -b_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -b_{n-2} \\ 0 & \cdots & 0 & 1 & -b_{n-1} \end{bmatrix}.$$

The trace is $-b_{n-1}$,and the norm is $\pm b_0$.

Suppose the polynomial has roots $a = a_1, a_2, \ldots, a_n$ in an algebraic closure of L. Then $b_{n-1} = a_1 + \cdots + a_n$, and $b_0 = \pm a_1 \cdots a_n$. So the trace is the sum of the roots of the polynomial, and the norm is the product of the roots.

Example 29.1. In $\mathbb{C}/\mathbb{R}$, we have

$$\operatorname{tr}(z) = z + \bar{z}$$

$$N(z) = z\bar{z}.$$

Suppose we have $K \subseteq K(a) \subseteq L$. Then $N(a)$ in L is $(N(a)(\text{in } K(a)))^{[L:K(a)]}$ and $\operatorname{tr}(a)$ in L is $(\operatorname{tr}(a)(\text{in } K(a))) \cdot [L : K(a)]$ (exercise).

Suppose $L : K$ is Galois with group G, then other roots are given by $\sigma_i(a)$ for $\sigma \in G$, so

$$N(a) = \prod_{\sigma \in G} \sigma(a),$$

$$\operatorname{tr}(a) = \sum_{\sigma \in G} \sigma(a).$$

29.2 The integers of a quadratic field

Recall that $\mathbb{Q}[\sqrt{-3}]$ contains the ring $\mathbb{Z}[\sqrt{-3}]$, which is not a UFD since $4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{3})$. It is also contained in $\mathbb{Z}[\frac{\sqrt{-3}+1}{2}]$, the Eisenstein integers, which is a UFD.

Given a field L containing $\mathbb{Q}$, what is a "nice" ring in it? The answer is that this is the ring of algebraic integers in K.

Definition 29.1. The ring of *algebraic integers* in K is the ring of elements in a field $K/\mathbb{Q}$ that are roots of polynomials in $\mathbb{Z}[x]$ with leading coefficient 1.

Proposition 29.1. *Let $L/\mathbb{Q}$ be a finite extension. Then for $\alpha \in L$, the following are equivalent:*

1. *α is algebraically independent (root of $x^n + \cdots = 0$).*
2. *We can find a finitely generated $\mathbb{Z}$-module A in L spanning L so that $\alpha A \subseteq A$.*

Proof. (1) $\implies$ (2): Take A to be spanned by $1, \alpha, \alpha^2, \ldots, a^{n-1}$. Then $\alpha\alpha^{n-1}$ is a linear combination of $1, \alpha, \alpha^2, \ldots, a^{n-1}$.

(2) $\implies$ (1): α is a linear transformation of a free $\mathbb{Z}$-module A. α is a root of its characteristic polynomial, which has leading coefficient 1 and other roots in $\mathbb{Z}$. □

Suppose $L = \mathbb{Q}(\sqrt{N})$, where N is a squarefree integer. We want to find the algebraic integers in L. The easiest examples are $m + n\sqrt{N}$, for $m, n \in \mathbb{Z}$. Sometimes, there are others, such as $\frac{\sqrt{3}+1}{2}$. The key point is that if α is an algebraic integer, so are $\mathrm{tr}(\alpha)$ and $N(\alpha)$. So $\mathrm{tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

What are the norm and trace of $m + n\sqrt{N}$? Choose the basis $\left\{1, \sqrt{N}\right\}$ for $L/\mathbb{Q}$. Multiplying by m makes $1 \mapsto m$ and $\sqrt{N} \mapsto m\sqrt{N}$, and multiplying by $n\sqrt{N}$ makes $1 \mapsto n\sqrt{N}$ and $\sqrt{N} \mapsto nN$. So we get the matrix

$$\begin{bmatrix} m & nN \\ n & m \end{bmatrix}.$$

These must be in $\mathbb{Z}$. $2m \in \mathbb{Z}$ makes $m \in \mathbb{Z}$, so $m^2 - n^2 \in \mathbb{Z}$. So $n \in \mathbb{Z}$, as n is squarefree. The other case is that $m \in \mathbb{Z} + 1/2$, so $m^2 = k + 1/4$. We need $m^2 - n^N \in \mathbb{Z}$, which is $1/4 - 4n^2 \in \mathbb{Z}$. So $1 \equiv (2n)^2 N \pmod 4$. If $N \equiv 2, 3 \pmod 4$, we have no solutions. So we must have $N \equiv 1 \pmod 4$. The integerrs of $\mathbb{Q}(\sqrt{N})$ are given by $\mathbb{Z}[\sqrt{N}]$ if $n \equiv 2, 3 \pmod 4$, and $\mathbb{Z}[\frac{1+\sqrt{N}}{2}]$ if $n \equiv 1 \pmod 4$.

The trace gives us a bilinear form on L/K with $(a, b) = \mathrm{tr}(ab)$. This is either 0 or nondegenerate.

Example 29.2. Here is an example when $(\cdot,\cdot)$ is zero. Let $K - F_p(t^p)$ and $L = F_p(t)$. $K \subseteq L$ and this is an inseparable extension. Any element of L is the root of an equation of the form $x^p - a$ for $a \in K$, where the coefficient of $x^{p-1} = 0$. This coefficient in the trace, so the trace is always 0.

For separable extensions L/K, the trace is not identically 0. This is trivial in characteristic 0 because $\mathrm{tr}(1) = [L : k] \neq 0$.

Definition 29.2. A *character* of a group G is a homomorphism from $G \to K^*$ (a "1-dimensional representation" of G).

Lemma 29.1 (Artin)**.** *Suppose G is a group (or monoid) and K is a field. If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters, they are linearly independent; i.e. if*

$$a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0$$

for all $g \in G$, then $a_1 = a_2 = \cdots = a_n = 0$.

Proof. Suppose $a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0$ for all g. Pick all a_i to be not all zero and n to be as small as possible. Since $\chi_1 \neq \chi_2$, pick $h \in G$ with $\chi_1(h) \neq \chi_2(h)$. Then

$$a_1\chi_1(gh) + a_2\chi_2(gh) + \cdots + a_n\chi_n(gh) = 0$$

for all g, which means that

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_2(h) + \cdots + a_n\chi_n(g)\chi_n(h) = 0.$$

If we multiply the original relation by $\chi_1(h)$, we get

$$a_1\chi_1(g)\chi_1(h) + a_2\chi_2(g)\chi_1(h) + \cdots + a_n\chi_n(g)\chi_1(h) = 0$$

If we subtract these two equations, we get

$$a_2(\chi_1(h) - \chi_2(h))\chi_2(g) + a_3(\chi_1(h) - \chi_3(h))\chi_3(g) + \cdots + a_n(\chi_1(h) - \chi_n(h))\chi_n(g) = 0.$$

Note that $\chi_1(h) - \chi_2(h) \neq 0$. So we have a smaller nonzero linear relation between $\chi_1, \ldots, \chi_n$, which is a contradiction since we chose n to be as small as possible. □

Proposition 29.2. *For a Galois extension L/K, the trace is not identically zero.*

Proof. We have that the trace is $\mathrm{tr}(a) = \sigma_1(a) + \sigma_2(a) + \cdots + \sigma_n(a)$ with $\sigma_i \in G$. If $\mathrm{tr}(a) = 0$ for all a, we have a linear relation between $\sigma_1, \ldots, \sigma_n$. This is not possible by Artin's lemma. So $\mathrm{tr}(a) \neq 0$ for some a. Separable extensions are similar and we leave that case as an exercise. □

29.3 Discriminant of a field extension L/K

Definition 29.3. The *discriminant* of L/K is the discriminant of the bilinear form $(a, b) = \mathrm{tr}(ab)$ on the vector space L.

Choose a basis $\{a_1, \ldots, a_n\}$ for L over K. The discriminant is $\det(B)$, where $B_{i,j} = (a_i, a_j)$. This depends on the choice of basis. If $\{b_1, \ldots, b_n\}$ is another basis, then some matrix times A gives a change of basis from $a_1, \ldots, a_n$ to $b_1, \ldots, b_n$. The discriminant for the bases is the discriminant for $b_1, \ldots, b_n$ times the determinant of A. So the discriminant is well-defined up to multiplication by squares of K. So $\mathrm{disc}(L/K) \in K^*/(K^*)^2$.

Example 29.3. Suppose $L = K(a)$. What is the discriminant of L/K? The element a is a root of some irreducible polynomial $p(a)$. Choose the basis $1, a, a^2, \ldots, a^{n-1}$ of L/K. The discriminant is equal to the determinant of

$$\begin{bmatrix} \mathrm{tr}(1) & \mathrm{tr}(a) & \mathrm{tr}(a^2) & \cdots & \mathrm{tr}(a^{n-1}) \\ \mathrm{tr}(a) & \mathrm{tr}(a^2) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix}$$

Assume L/K is Galois for simplicity. Then $\mathrm{tr}(a^k) = \sum_{\sigma \in G} \sigma(a^k)$, so we get

$$\begin{bmatrix} \sum \sigma(1 \cdot 1) & \sum \sigma(1 \cdot a) & \sum \sigma(1 \cdot a^2) & \cdots & \mathrm{tr}(a^{n-1}) \\ \sum \sigma(1 \cdot a) & \sum \sigma(1 \cdot a^2) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix}$$

This is the product of the matrices

$$\begin{bmatrix} \sigma_1(1) & \sigma_2(1) & \sigma_3(1) & \cdots & \sigma_n(1) \\ \sigma_1(a) & \sigma_2(a) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix} \begin{bmatrix} \sigma_1(1) & \sigma_1(a) & \sigma_1(a^2) & \cdots & \sigma_1(a^{n-1}) \\ \sigma_2(1) & \sigma_2(a) & \ddots & & \\ \vdots & \vdots & & & \end{bmatrix}$$

which are transposes of each other.

Recall the Vandemonde determinant

$$\det \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a & b & c & \cdots & \\ a^2 & b^2 & c^2 & \cdots & \\ \vdots & \vdots & \vdots & \ddots & \\ a^{n-1} & b^{n-1} & c^{n-1} & \cdots & \end{bmatrix} = \pm (a-b)(a-c)(a-d)(a-e) \cdots (b-c)(b-a) \cdots,$$

which is the product of the differences of different variables (where each difference is only counted once). These are equal because the degrees are the same, and the left side is

divisible by $a-b$ (and other terms) as if $a=b$, the the first two columns are the same. So they differ up to a constant, which is 1.

So the discriminant is the square of the determinant $\Delta = \pm\prod_{i<j}(\sigma_i(a)-\sigma_j(a))$. So Δ^2 is the discriminant of the polynomial $p(x)$. This means that the discriminant of the field extension is just the discriminant of the irreducible polynomial of a.

29.4 Applications of the discriminant of a field extension

Example 29.4. Look at the fields $\mathbb{Q}[x]/(x^2+x+1)$, $\mathbb{Q}[x]/(x^3-x-1)$, and $\mathbb{Q}[x]/(x^3-x+1)$. Which are isomorphic? The discriminants are -31, -31, and -23; remember to think of these as elements of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. The third differs from the first two; $-23/-31$ is not a square in $\mathbb{Q}^*$. The first two fields are isomorphic; change x to $-x$.

Example 29.5. Let's find algebraic integers in $L=\mathbb{Q}(\alpha)$, where $\alpha^2+\alpha+1=0$. Look at the discriminant of the basis $\{1,\alpha,\alpha^2\}$. The discriminant is -31. Let A be the $\mathbb{Z}$-linear span of $1,\alpha,\alpha^2$. Suppose B is the set of all algebraic integers. So $A\subseteq B$. $\operatorname{disc}(B) = \operatorname{disc}(A)\times\det(x)^2$, where x is the matrix taking the basis of A to the basis of B. The determinant is the order of the group B/A. Now note that -31 is squarefree. Then $\det(x)=1$, so $B=A$.

Example 29.6. Take $\mathbb{Q}(\sqrt{-3})$, so $\alpha=\sqrt{-3}$ and $\alpha^3+3=0$. This has discriminant -12, which is not squarefree. We have $\mathbb{Z}[\alpha]\subsetneq\mathbb{Z}[\frac{\sqrt{-3}+1}{2}]$, so you have to do more work.

Recall that the norm is a homomorphism $L^*\to K^*$. What are the kernel and the image of this map? These can be quite complicated.

Example 29.7. Look at $N:\mathbb{C}^*\to\mathbb{R}^*$ given by $N(z)=|z|^2=z\bar{z}$. The image is the positive reals.

Example 29.8. Look at $N:\mathbb{Q}(i)^*\to\mathbb{Q}^*$ given by $a+bi\mapsto a^2+b^2$. The image of the norm is the rational number that are sums of 2 squares. As you can see, this gets complicated, even in simple cases.

Theorem 29.1. *If L,K are finite fields, then $N:L^*\to K^*$ is onto.*

Proof. Recall[60] that the Galois group of L/K is cyclic, generated by the Frobenius element $x\mapsto x^q$, where $q=|K|$. The Galois group is $\{\}1,F,F^2,\dots,F^{n-1}$, where $n=[L:K]$.

$$\begin{aligned} N(a) &= aF(a)F^2(a)\cdots F^{n-1}(a) \\ &= aa^qa^{q^2}\cdots a^{q^{n-1}} \end{aligned}$$

[60] Maybe we should put "recall" instead. Professor Borcherds is unsure whether he actually remembered to introduce this when we went over finite fields.

$$= a^{q^{n-1}/(q-1)}.$$

So there are at most $q^{n-1}/(q-1)$ elements of norm 1. The image has at most $q-1$ elements. The order of kernel times the order of the image is the order of L^* (q^n-1), so the kernel and image indeed have order $q^{n-1}/(q-1)$ and $q-1$, respectively. □

What is the kernel of $N : L \to K$? Hilbert showed that if L/K is a cyclic extension generated by σ, then $N(a) = 1$ iff $a = \sigma(b)/b$ for some $b \in L^*$.

30 Hilbert's Theorem 90 and Galois Cohomology

30.1 Hilbert's theorem 90

We will begin by proving this oddly named[61] theorem we started last lecture.

Theorem 30.1 (Hilbert's theorem 90)**.** *Suppose L/K us cyclic. Then $N(a) = 1$ iff $a = b/\sigma b$ for some $b \in L^*$.*

Proof. If $a = a/\sigma b$, we leave it as an exercise to show that $N(a) = 1$.

We want to solve $a\sigma b = b$. Think of $a\sigma$ as a linear transformation on the vector space L; we want to find some $b \neq 0$ fixed by this linear transformation. Does $a\sigma$ have finite order? $(a\sigma)^2 = a\sigma a\sigma$, so it takes $b \mapsto a\sigma(a\sigma(b)) = a\sigma(a)\sigma^2(b)$. So $(a\sigma)^2 = a\sigma(a)\sigma^2$. We can continue this to get

$$(a\sigma)^n = \underbrace{a\sigma a\sigma^2 a \cdots \sigma^{n-1} a}_{N(a)=1} \underbrace{\sigma^n}_{=1} = 1.$$

A fixed vector of any G is given by $\sum_{g\in G} g(v)$. So the vector fixed by $(a\sigma)$ is given by $b = \sum i \in \mathbb{Z}(a\sigma)^i(\theta)$ for any $\theta \in L$. So b solves the problem, except we do not know that $b \neq 0$. What is the correct choice of theta? Note that this is

$$\begin{aligned}\theta + a\sigma(\theta) + (a\sigma)^2\theta + \cdots &= \theta + a\sigma\theta + a\sigma(a)\sigma^2(\theta) + a\sigma(a)\sigma^2(a)\sigma^3(\theta) \\ &= (a_0\sigma^0 + a_1\sigma^1 + a_2\sigma^2 + \cdots)(\theta)\end{aligned}$$

Use Artin's lemma to get that the σ_i are linearly independent. We can then find a θ so that the sum is 0.[62]

□

We will see later that this means that $H^{-1}(L^*) = 0$ for L/K cyclic. Here, $H^{-1}(L^*)$ is the *Tate cohomology group*.

30.2 Applications of Hilbert's theorem 90

Example 30.1. Suppose K contains a primitive n-th root ζ of unity. Take $a = \zeta$. Then $N(a) = \zeta\zeta\cdots\zeta = 1$. So $a = b/\sigma b$ for some b. So $\sigma(b) = \zeta b$. This makes $\sigma(b^n) = b^n$, so $b^n \in K^*$. So $L = K(\sqrt[n]{*})$.

[61] The name comes from Hilbert's "Zahlbericht" (number report) in 1897

[62] Professor Borcherds does not like the way Lang did this proof. Lang pulls out the second expression out of nowhere. Professor Borcherds says it seems like a "deus ex machina."

Example 30.2. Let's solve $x^3+x+1=0$. The discriminant is -31, which is not a square in $\mathbb{Q}$, so the Galois group of the splitting field of this polynomial over $\mathbb{Q}$ is S_3. This is a solvable group because we have $1 \subseteq \mathbb{Z}/3\mathbb{Z} \subseteq S_3$. This gives us the picture

$$\begin{array}{cc} L & 1 \\ \Big|3 & \Big|3 \\ K & \mathbb{Z}/3\mathbb{Z} \\ \Big|2 & \Big|2 \\ \mathbb{Q}(\omega) & S_3 \end{array}$$

What is K? K is a subfield of L fixed by $\mathbb{Z}/3\mathbb{Z}$. S_3 acts on $\alpha_1, \alpha_2, \alpha_3$. Let σ be a generator of $\mathbb{Z}/3\mathbb{Z}$. Then σ maps $\alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1$. K is generated by some α, where α is fixed by σ, but the elements of S_3 are not in $\mathbb{Z}/3\mathbb{Z}$. Try $\alpha = (\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)$ (find some polynomial in $\alpha_1, \alpha_2, \alpha_3$ fixed by $\mathbb{Z}/3\mathbb{Z}$ but not S_3. Now

$$\alpha^2 = (\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1)^2$$

is symmetric in α_i, so it is in the base field. It is the discriminant of x^3+x+1, which is -31. So $K = \mathbb{Q}(w, \sqrt{-31})$.

Next, we want to describe L in terms of K. L/K is a cyclic extension, so K contains cube roots of 1. So by Hilbert's theorem 90, $L = K(\sqrt[3]{*})$, where $*$ is an eigenvector of σ with eigenvalue equal to ω. Try $\alpha_1 + \omega^{-1}\sigma(\alpha_1) + \omega^{-1}\sigma^2(\alpha_1) = \alpha_1 + \omega^{-1}\alpha_2 + \omega^{-2}\alpha_3$. Call this y. Let $z = \alpha_1 + w\alpha_2 + w^2\alpha_3$. If we find $y, z, 0$, we can find $\alpha_1, \alpha_2, \alpha_3$ by linear algebra.

We know that $y^3, z^3 \in K$ and are fixe by σ.Expand these in polynomials in $\alpha_1, \alpha_2, \alpha_3$ to get that $y^3+z^3 = -27$ and $y^3b^3 = -27$. So we get that y^3 and z^3 are roots of $x^2+27z-27=0$. So $y^3, z^3 = 27/2 \pm 3\sqrt{3}i/2\sqrt{-31}$, which means that y, z are given by $y = -3.04\ldots$ and $z = 0.99\ldots$. So $\alpha_1 = (y+z)/3 \approx -0.68\ldots$.[63]

Example 30.3. Let's solve degree 4 equations x^4+bx^2+cd+d by radicals. We will provide a sketch. Look at the Galois group S_4, which is solvable because $1 \subseteq \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \subseteq A_4 \subseteq S_4$. We will have

$$\begin{array}{cc} M & 1 \\ \Big|4 & \Big|4 \\ L & (\mathbb{Z}/2\mathbb{Z})^2 \\ \Big|3 & \Big|3 \\ K & A_4 \\ \Big|2 & \Big|2 \\ \mathbb{Q}(\omega, i) & S_4 \end{array}$$

[63] Why do we put these approximate values? It's so you can check the answer for yourself!

To get to K from $\mathbb{Q}(\omega, i)$, we will adjoin a square root. Going up the diagram, we will then adjoin a cube root and then another square root.

Suppose the roots are $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Note that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. What is L? It is generated by things fixed under $(\mathbb{Z}/2\mathbb{Z})^2$. We wan to find a polynomial fixed by $(\mathbb{Z}/2\mathbb{Z})^2 \subseteq \S_4$. Try $y_1 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2/4 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$. It has conjugates

$$y_2 = (\alpha_1 + \alpha_3 - \alpha_2 - \alpha_4)^2/4$$

$$y_3 = (\alpha_1 + \alpha_4 4 - \alpha_2 - \alpha_3)^2/4$$

If we find $y_1, y_2, y_3,$, we can find $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ using some algebra.

y_1, y_2, y_3 generate a degree 6 extension of $\mathbb{Q}(\omega, i)$. The Galois group is $S_3 = S_4/(\mathbb{Z}/2\mathbb{Z})^2$. So y_1, y_2, y_3 are the roots of some cubic over $\mathbb{Q}$. In fact, there are the roots of $y^3 - 2by^2 + (b^2 - d)y_x^2 = 0$, which you can obtain via some messy algebra.[64] We can solve this cubic to find y_1, y_2, y_3 and use those to find the α_i.

30.3 Galois cohomology

30.3.1 Exact sequences

No one ever understands Galois cohomology the first time the encounter it.[65]

Suppose G is a group acting on some module M. Look at

1. M^G, the subset of things fixed by G (the invariants of G on M).
2. $M_G = M/\{m - gm : m \in M, g \in G\}$.

The former of these is the largest submodule of M where G acts trivially, and the latter is the largest quotient of M where G acts trivially.

Suppose that $0 \to A \to B \to C \to 0$ is an exact sequence. Act on it by G. Is this exact? No, we get

$$0 \to A^G \to B^G \to C^G \not\to 0.$$

Similarly, we get that

$$\not 0 \to A_G \to B_G \to C_G \to 0.$$

Example 30.4. Take $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$. with $G = \mathbb{Z}/2\mathbb{Z}$ acting as -1 on $\mathbb{Z}$. We get

$$0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2|Z \to 0.$$

[64] Mathematicians tried to find this for degree 5, but it turns out to be a degree 6 polynomial, which is even worse than what you started with. The underlying fact driving this occurrence is that S_5 is not solvable.

[65] Professor Borcherds says that no one ever understands Galois cohomology the first time they encounter it. He even referred to this section as a "futile attempt" to explain it.

Note that $M^G = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$, where $\mathbb{Z}G$ is the group ring of G and $\mathrm{Hom}_{\mathbb{Z}G}$ is the homomorphisms preserving the action of G. So M is a module over $\mathbb{Z}G$. $\mathbb{Z}$ is a module over $\mathbb{Z}G$ iwth elements of G acting trivially ($g \cdot n = n$).

We had earlier in the course that $\mathrm{Hom}(*, *)$ does not preserve exactness, but the failure was controlled by "Ext." Similarly,

$$M_G = \mathbb{Z} \otimes_{\mathbb{Z}G} M.$$

The tensor product does not preserve exactness, but the failure is controlled by "Tor." Put $H^0(G, M) = M^G$. The zeroth cohomology is $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$. Put $H^i(G, M) = \mathrm{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, M)$.

A long exact sequence of Ext gives us that if

$$0 \to A \to B \to C \to 0$$

is exact, then so is

$$0 \to H^0(A) \to H^0(B) \to H^0(C) \to H^1(A) \to H^1(B) \to H^1(C) \to H^2(A) \to \cdots$$

Similarly, put $H_0(G, M) = M_G$ and $H_i(G, M) = \mathrm{Tor}_i^{\mathbb{Z}G}(\mathbb{Z}, M)$. We get

$$\cdots \to H_1(C) \to H_0(A) \to H_0(B) \to H_0(C) \to 0$$

So H^1 and H_1 control the lack of exactness of M^G and M_G.

30.3.2 Lang's definition of cohomology

How does this relate to Lang's definition? Lang defines the first cohomology group as follows:

Definition 30.1. A *crossed homomorphism* is a map $G \to M$ sending $\sigma \mapsto a_\sigma$ with $a_{\sigma\tau} = a_\sigma + \sigma a_\tau$.

This is a homomorphism from $G \to M$ except if G acts trivially on M, then this is just $\mathrm{Hom}(G, M)$ as groups.

Definition 30.2. A *principal crossed homomorphism* is a crossed homomorphism such that $a_\sigma = b/\sigma b$ for some fixed b.

Lang defines the first cohomology group as

$$H^1(G, M) = \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}}.$$

30.4 Hilbert's theorem 90 for all Galois extensions

Theorem 30.2 (Hilbert's theorem 90)**.** *Let L/K is a Galois extension with Galois group G. Then $H^1(G, L^*) = 0$.*

Proof. We are given $a_\sigma \in L^*$ with $a_{\sigma\tau} = a_\sigma \cdot \sigma a_\tau$ (multiply, not add, since we are dealing with L^*, which is a multiplicative group). We want to find b with $a_\sigma = b/\sigma b$ for all σ. What is a crossed homomorphism? Look at $\sigma \mapsto a_\sigma \sigma$. This is a linear map $L \to L$, so $\sigma\tau \mapsto a_{\sigma\tau}\sigma\tau = a_\sigma \sigma a_\tau \tau = (a_\sigma \sigma)(a_\tau \tau)$. So this map is a homomorphism G *to* $\mathrm{End}(L)$. We will continue the proof next class. □

31 Infinite Extensions and Galois Cohomology

31.1 Hilbert's Theorem 90

Let's introduce the notation Lang uses for his version of Hilbert's theorem 90. Let G be a group and A be an abelian group with $G \circlearrowright A$.

Definition 31.1. A *1-cocycle* of G in A is a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ such that

$$\alpha_{\sigma\tau} = \alpha_\sigma + \sigma\alpha_\tau.$$

Definition 31.2. A *1-coboundary* of G in A is a family of elements $\{\alpha_\sigma\}_{\sigma \in G}$ such that there exists a fixed $\beta \in A$ such that $\alpha_\sigma = \sigma\beta - \beta$ for all $\sigma \in G$.

Theorem 31.1 (Hilbert's Theorem 90)**.** *Let L/K be Galois with Galois group G. Then $H^1(G, L^*) = 1$.*

Proof. A 1-cocycle gives a twisted action $G \circlearrowright L$ given by $\sigma \mapsto a_\sigma\sigma$. So $(a_\sigma\sigma)(a_\tau\tau) = a_{\sigma\tau}\sigma\tau$ by the 1-cocycle condition. We want to find b with $a_\sigma\sigma b = b$ for all σ; b is fixed by the twisted action and $b \neq 0$.

Find a fixed vector under G as $\sum_{\sigma \in G} \sigma v$, which is always fixed by G. A fixed vector under the twisted action is given by $b = \sum_{\sigma \in G} a_\sigma \cdot \sigma v$. We want to find v so b is nonzero. This is possible by Artin's theorem on the independence of σ, since otherwise, we could find a nonero linear relation between these homomorphisms equal to 0. □

Suppose G is cyclic, and let $N(a) = 1$ and $a = b/\sigma b$, where σ generates G. What is a 1-cocycle? Put $a_1 = 1$, $a_\sigma = a$, $a_{\sigma^2} = a_\sigma\sigma a_\sigma = a\sigma a$, and in general, $a_{\sigma^n} = a\sigma(a)\sigma^2(a)\cdots\sigma^{n-1}(a) = a_1 = 1$. So $N(a) = 1$ for this to give a 1 cocycle.

So since $N(0) = 1$, we get a 1-cocycle as above. Note that $a = b/\sigma b$ iff there is a cocycle given by $a_{\sigma^i} = b/\sigma^i b$ for all i, so a 1-cocycle is a 1-coboundary.

Theorem 31.2 (Hilbert's theorem 90)**.** *$H^1(G, L) = 0$, where L is considered as an additive group.*

Proof. As a module over $K[H]$, L is isomorphic to $K[G]$, so it is a free module. L has a basis of the form $\{\sigma w : \sigma \in G\}$ for some fixed w; this is a result called the normal basis theorem.[66] This shows that $H^i(G, L) = 0$ for $i > 0$. □

Does $H^i(G, L^*) = 1$ for $i > 0$? No. $H^2(G, L^*)$ is often nonzero. This is related to the *Brauer group*. $H^1(G, L^*)$ is related to the *Picard group*. The Picard group of integers of a number field is a *class group*.

Why is Lang's definition of H^1 as cocycles/coboundaries ($a_{\sigma\tau} = a_\sigma + \sigma(a_\tau)$) the same as Borcherd's definition $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, M)$? Here is a sketch of a proof that they are the same.

[66] Professor Borcherds never remembers the proof, so see Lang.

To find $\mathrm{Ext}(A, B)$, Take the free resolution of A. So we want a free resolution of $\mathbb{Q}$ by free $\mathbb{Z}$-modules.

$$\mathbb{Z}[G] \otimes \mathbb{Z}[G] \otimes \mathbb{Z}[G] \to \mathbb{Z}[G] \otimes \mathbb{Z}[G] \to \mathbb{Z}[G] \to 0$$

These have respective $\mathbb{Z}$-bases

$$g_0 \otimes g_1 \otimes g_2, \qquad g_0 \otimes g_1, \qquad g_0, \qquad 1$$

And we can map the basis elements by a map d, which sends a component to the identity. G acts by acting on each component. You should check that $d^2 = 0$ and that if $da = 0$, then $a = db$ for some b.

Now form the exact sequence

$$\leftarrow \mathrm{Hom}(F_0, B) \leftarrow \mathrm{Hom}(F_1, B) \leftarrow \mathrm{Hom}(F_0, B)$$

where F_i is the *free resolution*.

Check that $d(a_\sigma) = 0$ iff the a_σ are a 1-cocycle (exercise). Then $\{a_\sigma\} = d(*)$ iff the a_σs are a 1-coboundary.

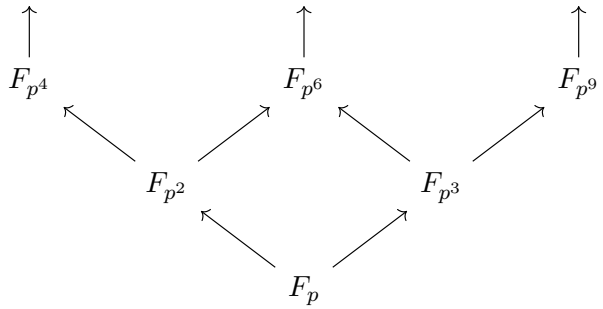
31.2 Infinite Galois extensions

We want to look at extensions that are algebraic, normal, and separable.

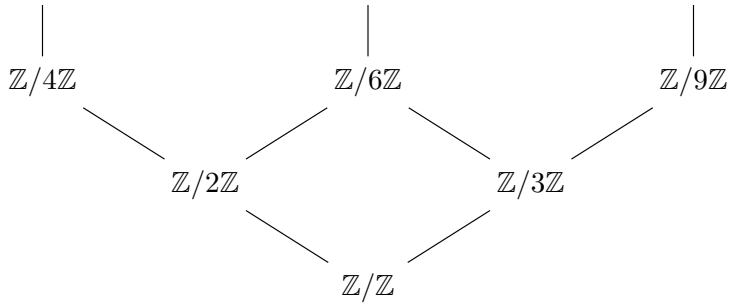
Example 31.1. Take $\bar{\mathbb{Q}}/\mathbb{Q}$, where $\bar{\mathbb{Q}}$ is the algebraic closure.

Suppose L/K is an infinite Galois extension. What does the Galois group look like? Any automorphism of L gives automorphisms of all finite extensions L_i/K. An element of $\mathrm{Aut}(L/K)$ is a set of elements of $\mathrm{Aut}(L_i/K)$ that are compatible. So $\mathrm{Gal}(L/K)$ is the inverse limit of the groups $\mathrm{Gal}(L_i/K)$.

Example 31.2. Let $K = F_p$, and let $L = \bar{F_p}$. $L = \bigcup_{p \geq 1} F_{p^k}$. We have the following picture:



So the groups will look like this:



So $\mathrm{Gal}(\bar{F}/F) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$. This is called the *profinite completion* of $\mathbb{Z}$.

Definition 31.3. A *profinite group* is an inverse limit of finite groups

Definition 31.4. The *profinite completion* of G is

$$\varprojlim_{\substack{G_i \text{ normal} \\ G/G_i \text{ finite}}} G/G_i.$$

This is a subset of $\prod G/G_i$, with the discrete topology. There is a universal map from G to a profinite group. The image of G is dense in the *Krull topology*[67], so $\varprojlim G/G_i$ is a sort of completion of G.

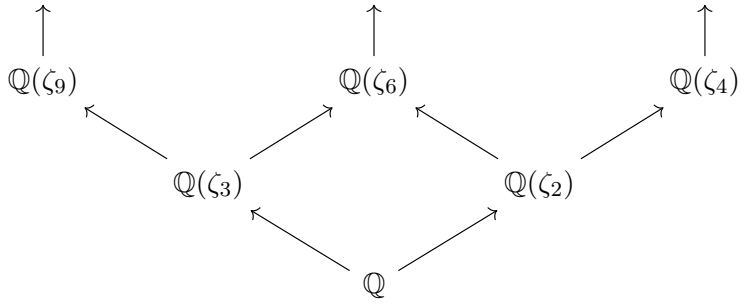
Example 31.3. Recall that $\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, where $n = \prod p_i^{k_i}$ (by the Chinese remainder theorem). Then $\varprojlim \mathbb{Z}/n\mathbb{Z} = \prod \varprojlim_{k_i} \mathbb{Z}/p_i^{k_i}\mathbb{Z} = \prod_p \mathbb{Z}_p$, the p-adic integers.

For finite extensions, we get a 1 to 1 correspondence between extensions of K in L and subgroups of $\mathrm{Gal}(L/K)$. Is the same true for infinite extensions? No. Suppose $\alpha \in L$. Look at $K(\alpha)/L$. The set of things in the Galois group fixing α is closed in the Krull topology; this is the set of things fixing α in M/K, where M is the normal closure of α. A subgroup fixing any element $\alpha \in L$ is always closed in the Krull topology. So a subgroup fixing all elements of an extension M is an intersection of closed subgroups and is hence closed.

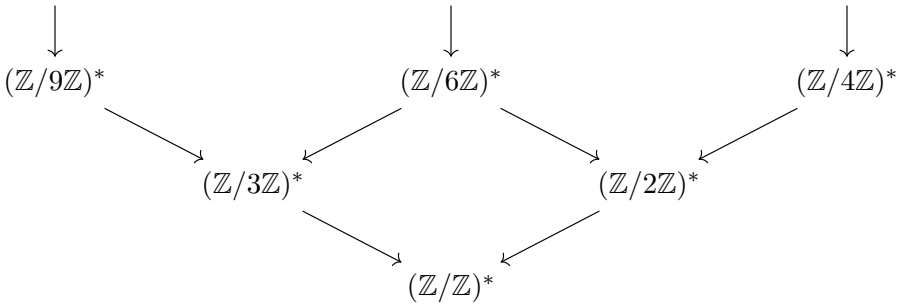
Instead, we get a 1 to 1 correspondence between extensions of K in L and closed subgroups of $\mathrm{Gal}(L/K)$. We leave this as an exercise. The proof relies on the theorem for finite Galois extensions and some bookkeeping.

[67] Professor Borcherds expressed his displeasure with the fact that there is a Marvel villain named Krull.

Example 31.4. Let $K = \mathbb{Q}$, and let L be the cyclotomic extension of $\mathbb{Q}$ ($\mathbb{Q}$(all roots of unity). $L = \bigcup \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity. we get the picture



We know that $\operatorname{Gal}\mathbb{Q}[\zeta_n]/\mathbb{Q} = (\mathbb{Z}/n\mathbb{Z})^*$. So $\operatorname{Gal}(\mathbb{Q}_{\text{cycl}}/\mathbb{Q})$ is given by the inverse limit of



As before, $(\mathbb{Z}/n\mathbb{Z})^* = \prod(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$. So $\varprojlim(\mathbb{Z}/n\mathbb{Z})^* = \prod_p(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^* = \prod_p \mathbb{Z}_p^*$. This is equal to $\bar{\mathbb{Z}}^*$, where $\bar{\mathbb{Z}}$ is the profinite completion of the ring $\mathbb{Z}$. Nicely enough, it is abelian.

Example 31.5. Let $K = \mathbb{Q}$ and $L = \bar{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. Let $G = \operatorname{Gal}(\bar{Q}/\mathbb{Q})$. G is not known. The abelianization of G is known. This is $\lim(\mathbb{Z}/n\mathbb{Z})^* = \operatorname{Gal}(\mathbb{Q}_{\text{cycl}}/\mathbb{Q})$. We have the exact sequence

$$0 \to \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{cycl}}) \to \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Gal}(\mathbb{Q}_{\text{cycl}}/\mathbb{Q}) \to 0.$$

What is $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}_{\text{cycl}})$? This is unknown. There is a conjecture of Shafarevich that this is isomorphic to the profinite completion of a countable free group. $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is related to the Langlands program and "automorphic forms."[68] Part of Andrew Wiles' proof of Fermat's last theorem is about understanding some of the structure of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

[68]Professor Borcherds says that to understand what automorphic forms are, it takes a semester, and to understand what "related to" means, it takes a lifetime of study.

31.3 Abelian Kummer theory

We want to find abelian extensions of K, given that K has enough roots of unity. Let $\bar{K}$ be the separable algebraic closure of K, the largest separable extension in the algebraic closure. Look at

$$1 \to \mu_n \to \bar{K}^* \to \bar{K}^* \to 1,$$

where μ_n is the n-th roots of unity in K. This is an exact sequence of groups acted on by $\mathrm{Gal}(\bar{K}/K)$. Take the invariants under $\mathrm{Gal}(\bar{K}/K)$.

$$1 \to \mu_n \to K^* \xrightarrow{x \mapsto x^n} K^* \to H^1(G, \mu_n) \to \underbrace{H^1(G, \bar{K}^*)}_{=1} \to \underbrace{H^1(G, \bar{K})}_{=1} \to \cdots.$$

where these last two are 1 by Hilbert's theorem 90. The definition of the first homomology is the same as for when G is finite, except cocycles must be continuous.

So we get

$$k^* \xrightarrow{x \mapsto x^n} K^* \to \mathrm{Hom}(G, \mu_n) \to 1,$$

and $\mathrm{Hom}(G, \mu_n) = H^*/(K^*)^n$, which is cyclic of order n. The kernels of homomorphisms in this group are isomorphic to subgroups H of G with G/H cyclic and of order dividing n. This is isomorphic to extensions L of K with $\mathrm{Gal}(L/K)$ cyclic and of order n. This is the same as our previous description: cyclic extensions of the form $K(\sqrt[n]{*})$.

31.4 Artin-Schrier extensions

Let L/K be cyclic of order p, where p is the characteristic of K. Then $L = K(\alpha)$, where α is a root of $x^p - x - b = 0$ for $b \in K$. Rewrite this in terms of infinite extenions and Galois cohomology. Let $\bar{K}$ be the separable closure of K. Use

$$0 \to F_p \to \bar{K} \xrightarrow{x \mapsto x^p - x} \bar{K} \to 0,$$

the exact sequence of modules acted on by $\mathrm{Gal}(\bar{K}/K)$. Take the invariants

$$0 \to F_p \to K \xrightarrow{x \mapsto x^p - x} K \to \underbrace{H^1(G, F_p}_{=\mathrm{Hom}(G, F_p)} \to \underbrace{H^1(G, \bar{K})}_{=0} \to \underbrace{H^1(G, \bar{K})}_{=0} \to \cdots.$$

$H^i(G, \bar{K}) = 0$ for $i > 0$ by the normal basis theorem.

So $\mathrm{Hom}(G, F_p) = K/\operatorname{im}(x^p - x)$ correspond to normal subgroups of index p in $\mathrm{Gal}(\bar{K}/K)$. which correspond to cyclic extensions of degree p.

What about extensions L/K with group $\mathbb{Z}/p^n\mathbb{Z}$ and $n > 1$? The answer is to use *Witt vectors*; see the exercises in Lang. We get

$$0 \to \mathbb{Z}/p^n\mathbb{Z} \to W \to W \to 0,$$

where W is the ring of Witt vectors.