HIGHER ALGEBRA I (MATH 570)
COURSE NOTES

EYAL Z. GOREN
MCGILL UNIVERSITY

Contents

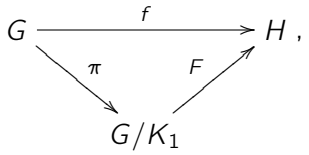
1. Groups

1.1. **Our starting point.** We assume the following notions and results: group, subgroup, normal subgroup, coset, quotient group, homomorphism, Lagrange theorem, familiarity with the symmetric group S_n, cycles, unique factorization into cycles of a permutation, even and odd permutations, the alternating group A_n. The centre of a group, the commutator subgroup.

We also assume the four isomorphism theorems for groups, that we recall for convenience.

Let G be a group:

(1) Let $f: G \to H$ be a homomorphism of groups with kernel K and let K_1 be a normal subgroup of G contained in K. There is a unique factorization giving a commutative diagram



where π is the canonical homomorphism $g \mapsto gK_1$. The kernel of F is $K/K_1 \lhd G/K_1$. In particular, if f is surjective, there is an induced isomorphism $F: G/K \to H$.

(2) Let $H \lhd G$ and $K < G$. Then HK is a subgroup of G, $H \cap K$ a normal subgroup of K, and

$$HK/H \cong K/(H \cap K).$$

(3) Let $H \lhd G$, $K \lhd G$, such that $K \subset H$. Then H/K is a normal subgroup of G/K and

$$(G/K)/(H/K) \cong G/H.$$

(4) Let $f: G \to H$ be a surjective homomorphism of groups. There is a $1:1$ correspondence between subgroups of H and subgroups of G that contain $K := \mathrm{Ker}(f)$. It preserves inclusion and the notion of being a normal subgroup. The correspondence is

$$H_0 \subseteq H \mapsto K_0 := f^{-1}(H_0).$$

1.2. **Group actions.** Let G be a group and S a non-empty set. An **action** of G on S is a function

$$G \times S \to S, \qquad (g, s) \mapsto g * s,$$

(although we mostly write gs) such that for all $s \in S, g_1, g_2 \in G$:

(1) $1 * s = s$;
(2) $g_1 * (g_2 * s) = (g_1 g_2) * s$.

In particular, every $g \in G$ defines a function $\sigma_g: S \to S$ by $s \mapsto g * s$. This function has an inverse, which is the function associated to g^{-1} (use the two axioms) and so is a permutation. Further, axiom (2) tells us that

$$\sigma_{g_2} \circ \sigma_{g_1} = \sigma_{g_1 g_2}.$$

And so we get the following lemma.

Lemma 1.2.1. *Let S be a non-empty set, G a group and Σ_S the group of permutations of S. There is a natural correspondence between (i) group actions of G on S; (ii) group homomorphisms $G \to \Sigma_S$.*

The following definitions are basic to this theory:

Definition 1.2.2. (Orbit) Let $s \in S$. The **orbit** of s, denoted $\mathrm{Orb}(s)$ is the subset of S given by

$$\mathrm{Orb}(s) = \{g * s : g \in G\}.$$

Being in the same orbit is an equivalence relation and so S *is a disjoint union of orbits*.

Definition 1.2.3. (Stabilizer) Let $s \in S$. The **stabilizer** of s in G is the following subgroup of G,

$$\mathrm{Stab}(s) = \{g \in G : g * s = s\}.$$

There is a natural bijection

$$G/\mathrm{Stab}(s) \to \mathrm{Orb}(s), \quad g \cdot \mathrm{Stab}(s) \mapsto g * s.$$

In particular, if the orbit is a finite set then $\mathrm{Stab}(s)$ is of finite index (and vice-versa) and

$$\sharp\, \mathrm{Orb}(s) = [G : \mathrm{Stab}(s)].$$

Example 1.2.4. Let G be a group and H a subgroup of G. Then, H acts on G by

$$(h, g) \mapsto hg$$

where hg is the product of h and g in the group G. Then, $\mathrm{Orb}(s) = Hs$ is a right coset of H. The stabilizer of any s is trivial and so every coset has $[H : \{1\}] = \sharp H$ number of elements. Finally, G is divided into disjoint orbits, namely, disjoint cosets of H, each having the same size $\sharp\, H$ and so,

Lagrange Theorem: Let G be a finite group and H a subgroup of G then $\sharp H | \sharp G$. In fact,

$$\sharp G = [G : H] \cdot \sharp H.$$

Example 1.2.5. The Orbit-Stabilizer relationship can be used to understand structures of groups very effectively. Here is an example[1]: Consider the group of rotational symmetries G of the cube. The cube has 6 faces and one easily sees that G acts transitively on the set of faces. This is a transitive action of G on a set of 6 elements. The stabilizer of a face is the group of order 4 of rotations around an axes passing through the centre of the face. It has order 4. We conclude that $\sharp G = 4 \times 6 = 24$. We also conclude the existence of cyclic subgroups of order 4. Let H be such a subgroup. A face and its opposite have the same stabilizer, but this is the only case when stabilizers are equal. Thus, H is normalized by an element taking a face to its opposite and, in fact, $[N_G(H) : H] = 2$.

Similarly, G acts transitively on the set of vertices, and there are 8 of which. The stabilizer J of a vertex has thus order 3. Indeed, it's generated by a rotation fixing the vertex and rotating cyclically the 3 faces with that vertex. It must then permutes cyclically the remaining 3 faces as well (as the remaining 3 faces are a union of orbits of a cyclic group of order 3 and it is easy to see it cannot fix the 3 faces). It follows that J is also the stabilizer of one more vertex. We conclude that $[N_G(J) : J] = 2$ and that there are at least 4 subgroups of order 3. (In fact, an easy application of Sylow's theorem (to be proven later) shows that there are precisely 4 subgroups of order 3.) Furthermore, by consider the action on the set of 12 edges, we find that G has a subgroup K of order 2 such that $K \cap H = \{1\}$.

[1] I learned of this nice example from the blog of Gowers.

1.3. **The class equation.** Now we take both the group and the set to be the same. Every group G acts on itself by conjugation:

$$G \times G \to G, \quad (g,h) \mapsto {}^g h := ghg^{-1}.$$

An element s of G has orbit of size 1, namely, an orbit consisting just of itself, if and only if for all $g \in G$ we have $gsg^{-1} = s$. That is, if and only if $s \in Z(G)$, the centre of G. The stabilizer of a general element s is written in this case as $C_G(s)$, the centralizer of G in S and

$$C_G(s) = \{g \in G : gs = sg\}.$$

The orbit of s is called its **conjugacy class** $\text{conj}(s) = \{gsg^{-1} : g \in G\}$. The group G is divided into disjoint conjugacy classes and for a finite group G we have

$$\sharp G = \sharp Z(G) + \sum_s \sharp \text{conj}(s), \tag{1}$$

where the sum extends over representatives for the conjugacy classes of size greater than 1. Note, once more, that $\sharp\text{conj}(s) = [G : C_G(s)]$. We thus can also write the class equation (1) as

$$\sharp G = \sharp Z(G) + \sum_{\text{reps.} s \notin Z(G)} \frac{\sharp G}{\sharp C_G(s)}. \tag{2}$$

1.4. p-**groups.** Let p be a prime number. A finite group G is called a **p-group** if $\sharp G = p^r$, for some $r \geq 0$. It is called a non-trivial p-group if $r > 0$.

Theorem 1.4.1. *Let G be a nontrivial p-group then the centre of G is nontrivial.*

Proof. Suppose that $\sharp G = p^r$, $r > 0$. If $Z(G)$ is trivial, then $\sharp Z(G) = 1$. The class equation then gives

$$p^r = 1 + \sum_{\text{reps.} s \notin Z(G)} \frac{\sharp G}{\sharp C_G(s)}.$$

But, each summand under the summation sign is a positive power of p. This is a contradiction since then p divides the left hand side, but not the right hand side. □

We can strengthen this theorem as follows (but we leave the proof as an exercise).

Theorem 1.4.2. [2] *Let G be a non-trivial p group and $H \lhd G$ a non-trivial normal subgroup. Then, $H \cap Z(G)$ is a non-trivial subgroup.*

Corollary 1.4.3. *Let G be a p-group and $H \lhd G$ a subgroup of order p. Then $H \subseteq Z(G)$.*

Theorem 1.4.4. *Let G be a finite p group, $|G| = p^n$.*

1. *For every normal subgroup $H \lhd G$, $H \neq G$, there is a subgroup $K \lhd G$ such that $H < K < G$ and $[K : H] = p$.*
2. *There is a chain of subgroups $H_0 = \{1\} < H_1 < \cdots < H_n = G$, such that each $H_i \lhd G$ and $|H_i| = p^i$.*

Proof. (1) The group G/H is a p-group and hence its center is a non-trivial group. Take an element $e \neq x \in Z(G/H)$; its order is p^r for some r. Then $y = x^{p^{r-1}}$ has exact order p. Let $K' =< y >$. It is a normal subgroup of G/H of order p (y commutes with any other element). Let $K = \pi_H^{-1}(K')$. Then K is a normal subgroup of G, and $K/H \cong K'$ so $[K : H] = p$.

[2] Taking $H = G$ gives the theorem.

(2) The proof just given shows that every p-group has a normal subgroup of p elements. Now apply repeatedly the first part.

□

END OF LECTURE 1 (September 5)

1.5. **Examples of p groups.**

1.5.1. *Groups of order p.* Every such group is cyclic, thus isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

1.5.2. *Groups of order p^2.* Every such group G is commutative. Indeed, let x be an element of order p contained in the centre of G. Let y be an element of G such that its image in the group $G/\langle x\rangle$ of order p is a generator (any $y \notin \langle x\rangle$ would do). Then, every element of G is of the form $y^a x^b$. Because x is in the centre, $y^a x^b y^c x^d = y^{a+c} x^{b+d} = y^c x^d y^a x^b$ and G is commutative. If G has an element of order p^2 then G is cyclic, isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$. Else, every element of G is of order p and G is commutative. It follows that we can view G is a vector space (with p^2 vectors) over the finite field $\mathbb{Z}/p\mathbb{Z}$, where for $a \in \mathbb{Z}/p\mathbb{Z}, g \in G$ we let $ag = g + \cdots + g$, a-times. From the theory of vector spaces we conclude that $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

1.5.3. *Groups of order p^3.* First, there are the abelian groups $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z})^3$.

An argument similar to the one used for groups of order p^2 shows that if G is not abelian then $G/Z(G)$ cannot be cyclic. It follows that $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ and $G/Z(G) \cong (\mathbb{Z}/p\mathbb{Z})^2$. One example of such a group is provided by the matrices

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

where $a, b, c \in \mathbb{F}_p$. The centre consists of the matrices with $a = c = 0$. Note that if $p \geq 3$ then every element in this group is of order p (use $(I + N)^p = I + N^p$), yet the group is non-abelian. (This group, using a terminology to be introduced later, is a semi-direct product $(\mathbb{Z}/p\mathbb{Z})^2 \ltimes \mathbb{Z}/p\mathbb{Z}$.) More generally the upper unipotent matrices in $\mathrm{GL}_n(\mathbb{F}_p)$ are a group of order $p^{n(n-1)/2}$ in which every element has order p if $p \geq n$. Notice that these groups are non-abelian.

Getting back to the issue of non-abelian groups of order p^3, one can prove that there is precisely one additional non-abelian group of order p^3. It is generated by two elements x, y satisfying: $x^p = y^{p^2} = 1, xyx^{-1} = y^{1+p}$. (This group is a semi-direct product $(\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$. We will return to this example in §1.8)

Example 1.5.1. Let $p = 2$. The two non-isomorphic non-abelian groups of order 8 are: (i) D_4, the dihedral group of order 8 - the symmetries of the square; (ii) the quaternion group Q_8 of order 8, consisting of the elements $\{\pm 1, \pm i, \pm j, \pm k\}$ with -1 a central element such that $-1^2 = 1$, $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j$ (and so $ij = -ji$ and so on).

1.6. **The coset representation.**

This is one of the most important examples of a group action. Let G be a group and H a subgroup of G. Consider the set S of left cosets gH of H. Then, G acts on S by left multiplication:

$$G \times S \to S, \qquad (a, gH) \mapsto agH.$$

This is a transitive action and this action, or the corresponding homomorphism $G \to \Sigma_S$, are called the **coset representation**. We leave it as an exercise to show that to give a subgroup of G of index n is the same thing as to give a pointed set (S, s_0) (namely, a set S with an element $s_0 \in S$)

of n elements, together with an action of G. In one direction - from subgroups to actions - this is the coset representation. As a consequence, one easily concludes that if G is finitely generated, it has finitely many subgroups of index n for a given n (and, in fact, a bound on the number of subgroups of index n).

The kernel of this homomorphism $f : G \to \Sigma_{\{gH\}}$ is $\{a \in G : agH = gH, \forall g \in G\} = \{a \in G : a \in gHg^{-1}, \forall g \in G\}$, that is

$$\mathrm{Ker}(f) = \cap_{g \in G} gHg^{-1}.$$

We conclude the following:

Proposition 1.6.1. *Let G be a group and H a subgroup of index n of G. Then H contains a subgroup K, such that $K \lhd G$ and $[G : K] \leq n!$.*

Proof. Let $K = \mathrm{Ker}(f)$, where $f : G \to \Sigma_{\{gH\}}$ is the coset representation. Then $K \subseteq H$ and K, being a kernel of a homomorphism, is a normal subgroup. Further,

$$G/K \hookrightarrow \Sigma_{\{gH\}} \cong S_n.$$

Since the order of S_n is $n!$, we have $[G : K] \leq n!$ (in fact $[G : K] | n!$). □

Using these techniques, one can draw some beautiful consequences (left as exercises).

Proposition 1.6.2. *Let G be a finite group, p the smallest prime dividing the order of G (it is allowed that $p^2 | \sharp G$). Let H be a subgroup of G of index p, then H is normal.*

The case $p = 2$ of this proposition is worth special attention: a subgroup of index 2 is always normal.

Proposition 1.6.3. *Let G be a finite simple group. If G has a subgroup of index $n > 1$ then $\sharp G < n!$.*

For example, A_5 is a simple group of order 60. It therefore doesn't have subgroups of index $2, 3$ or 4. Is it easy to prove directly?

1.7. **The Sylow theorems.** We shall prove the Sylow theorems by making use of various group actions.

Theorem 1.7.1. *(**Sylow**) Let p be a prime and G a finite group of order $p^r m$, where $p \nmid m$ and $r > 0$.*

1. *Every maximal p-subgroup of G has order p^r (such a subgroup is called a p-**Sylow subgroup**) and such a subgroup exists.*
2. *All Sylow p-subgroups are conjugate to each other.*
3. *The number n_p of Sylow p-subgroups satisfies: (i) $n_p | m$; (ii) $n_p \equiv 1 \pmod{p}$.*

Remark 1.7.2. To say that a subgroup P is conjugate to a subgroup Q means that there is a $g \in G$ such that $gPg^{-1} = Q$. Recall that the map $x \mapsto gxg^{-1}$ is an automorphism of G. This implies that P and Q are isomorphic as groups.

Another consequence is that to say there is a unique p-Sylow subgroup is the same as saying that a p-Sylow is normal. This is often used this way: given a finite group G the first check in ascertaining whether it is simple or not is to check whether the p-Sylow subgroup is unique for some p dividing the order of G. Often one engages in combinatorics of counting how many p-Sylow subgroups can be, trying to conclude there can be only one for a given p, and hence getting a normal subgroup and concluding the G is not simple. The converse is not true; G is not simple does not imply that one of the p-Sylow subgroups is normal. Take for example S_4. It has 4 3-Sylow subgroups and 3 2-Sylow subgroups.

Note that a consequence of Sylow's theorem is that if $p|\sharp G$ then G has an element of order p. Indeed, pick any element different from the identity in some p-Sylow subgroup of G and, if needed, raise it to some power so that it's order becomes exactly p. This holds whether G is abelian or not. The proof of Sylow's theorems starts by establishing this conclusion for abelian groups.

Lemma 1.7.3. *Let A be a finite abelian group, let p be a prime dividing the order of A. Then A has an element of order p.*

Proof. We prove the result by induction on $|A|$. Let N be a maximal proper subgroup of A. If p divides the order of N we are done by induction. Otherwise, let $x \notin N$ and let $B =< x >$. By maximality the subgroup BN is equal to A. On the other hand $|BN| = |B| \cdot |N|/|B \cap N|$. Thus, p divides the order of B. That is the order of x is pa for some a and so the order of x^a is precisely p. □

Proposition 1.7.4. *There is a p-subgroup of G of order p^r.*

Proof. We prove the result by induction on the order of G. Assume first that p divides the order of the centre $Z(G)$. Let x be an element of $Z(G)$ of order p and let $N =< x >$, a normal subgroup. The order of G/N is $p^{r-1}m$ and by induction it has a p-subgroup H' of order p^{r-1}. Let H be the preimage of H'. It is a subgroup of G such that $H/N \cong H'$ and thus H has order $|H'| \cdot |N| = p^r$.

Consider now the case where p does not divide the order of $Z(G)$. Consider which summands are divisible by p in the class equation

$$|G| = |Z(G)| + \sum_{\text{reps.} x \notin Z(G)} \frac{|G|}{|C_G(x)|}.$$

We see that for some $x \notin Z(G)$ we have that p does not divide $\frac{|G|}{|C_G(x)|}$. Thus, p^r divides $C_G(x)$. The subgroup $C_G(x)$ is a *proper* subgroup of G because $x \notin Z(G)$. Thus, by induction, $C_G(x)$, and hence G, has a p-subgroup of order p^r. □

Lemma 1.7.5. *Let P be a maximal p-subgroup and Q any p-subgroup then*

$$Q \cap P = Q \cap N_G(P).$$

Proof. Since $P \subset N_G(P)$ also $Q \cap P \subset Q \cap N_G(P)$. Let $H = Q \cap N_G(P)$. Then, since $P \lhd N_G(P)$ we have that HP is a subgroup of $N_G(P)$. Its order is $|H| \cdot |P|/|H \cap P|$ and so a power of p. Since P is a maximal p-subgroup we must have $HP = P$ and thus $H \subset P$. □

Proof. (Of Theorem) Let P be a Sylow subgroup of G. Such exists by Proposition 1.7.4. Let

$$S = \{P_1, \dots, P_a\}$$

be the set of conjugates of $P = P_1$. That is, the subgroups gPg^{-1} one gets by letting g vary over G. Note that for a fixed g the map $P \to gPg^{-1}$, $x \mapsto gxg^{-1}$ is a group isomorphism. Thus, every P_i is a Sylow p-subgroup. Our task is to show that every maximal p-subgroup is an element of S and find out properties of a.

Let Q be any p-subgroup of G. The subgroup Q acts by conjugation on S. The size of $Orb(P_i)$ is $|Q|/|\text{Stab}_Q(P_i)|$. Now $\text{Stab}_Q(P_i) = Q \cap N_G(P_i) = Q \cap P_i$ by Lemma 1.7.5. Thus, the orbit consists of one element if $Q \subset P_i$ and is a proper power of p otherwise.

Take first Q to be P_1. Then, the orbit of P_1 has size 1. Since P_1 is a maximal p-subgroup it is not contained in any other p-subgroup, thus the size of every other orbit is a power of p. It follows, using that S is a disjoint union of orbits, that $a = 1 + tp$ for some t. Note also that $a = |G|/|N_G(P)|$ and thus divides $|G|$.

We now show that all maximal p-subgroups are conjugate. Suppose, to the contrary, that Q is a maximal p-subgroup which is not conjugate to P. Thus, for all i, $Q \neq P_i$ and so $Q \cap P_i$ is a proper

subgroup of Q. It follows then that S is a union of disjoint orbit all having size a proper power of p. Thus, $p|a$. This is a contradiction. □

1.7.1. *Examples and applications.*

Example 1.7.6. p-groups. Every finite p-group is of course the only p-Sylow subgroup (trivial case).

Example 1.7.7. $\mathbb{Z}/6\mathbb{Z}$. In every abelian group the p-Sylow subgroups are normal and unique. The 2-Sylow subgroup is $< 3 >$ and the 3-Sylow subgroup is $< 2 >$.

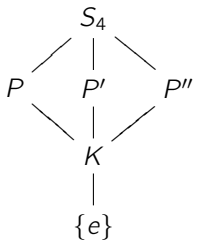
Example 1.7.8. S_3. Consider the symmetric group S_3. Its 2-Sylow subgroups are given by $\{1, (12)\}$, $\{1, (13)\}, \{1, (23)\}$. Note that indeed $3|3 = 3!/2$ and $3 \equiv 1 \pmod 2$. It has a unique 3-Sylow subgroup $\{1, (123), (132)\}$. This is expected since $n_3|2 = 3!/3$ and $n_3 \equiv 1 \pmod 3$ implies $n_3 = 1$.

Example 1.7.9. S_4. We want to find the 2-Sylow subgroups. Their number $n_2|3 = 24/8$ and is congruent to 1 modulo 2. It is thus either 1 or 3. Note that every element of S_4 has order $1, 2, 3, 4$. The number of elements of order 3 is 8 (the 3-cycles). Thus, we cannot have a unique subgroup of order 8 (it will contain any element of order 2 or 4). We conclude that $n_2 = 3$. One such subgroup is $D_8 \subset S_4$; the rest are conjugates of it.

Further, $n_3|24/3$ and $n_3 \equiv 1 \pmod 3$. If $n_3 = 1$ then that unique 3-Sylow would need to contain all 8 element of order 3 but is itself of order 3. Thus, $n_3 = 4$.

Remark 1.7.10. A group of order 24 is never simple, though it does not mean that one of the Sylow subgroups is normal, as the example of S_4 shows. However, consider the representation of a group G of order 24 on the cosets of P, where P is its 2-Sylow subgroup. It gives us, as we have seen in the past, a normal subgroup of G, contained in P, whose index divides $6 = [G : P]!$ and hence is non-trivial.

Call this subgroup K. Then, we see that $|K| = 4$; it is preserved under conjugation hence is a subgroup of all three 2-Sylow subgroups, say P, P', P''. We have the following picture



Example 1.7.11. Groups of order pq. Let $p < q$ be primes. Let G be a group of order pq. Then $n_q|p$, $n_q \equiv 1 \pmod q$. Since $p < q$ we have $n_q = 1$ and the q-Sylow subgroup is normal (in particular, G is never simple). Also, $n_p|q$, $n_p \equiv 1 \pmod p$. Thus, either $n_p = 1$, or $n_p = q$ and the last possibility can happen only for $q \equiv 1 \pmod p$.

We conclude that if $p \not| (q - 1)$ then both the p-Sylow P subgroup and the q-Sylow subgroup Q are normal. Note that the order of $P \cap Q$ divides both p and q and so is equal to 1. Let $x \in P, y \in Q$ then $[x, y] = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1}) \in P \cap Q = \{1\}$. Thus, PQ, which is equal to G, is abelian.

We shall later see that whenever $p|(q - 1)$ there is a non-abelian group of order pq (in fact, unique up to isomorphism). The case of S_3 falls under this.

Example 1.7.12. Groups of order p^2q. Let G be a group of order p^2q, where p and q are distinct primes. We prove that G is not simple:

If $q < p$ then $n_p \equiv 1 \pmod p$ and $n_p|q < p$, which implies that $n_p = 1$ and the p-Sylow subgroup is normal.

Suppose that $p < q$, then $n_q \equiv 1 \pmod q$ and $n_q | p^2$, which implies that $n_q = 1$ or p^2. If $n_q = 1$ then the q-Sylow subgroup is normal. Assume that $n_q = p^2$. Each pair of the p^2 q-Sylow subgroups intersect only at the identity (since q is prime). Hence they account for $1 + p^2(q-1)$ elements. Suppose that there were 2 p-Sylow subgroups. They intersect at most at a subgroup of order p. Thus, they contribute at least $2p^2 - p$ new elements. All together we got at least $1 + p^2(q-1) + 2p^2 - p = p^2 q + p^2 - p + 1 > p^2 q$ elements. That's a contradiction and so $n_p = 1$; the p-Sylow subgroup is normal.

Remark 1.7.13. A theorem of Burnside states that a group of order $p^a q^b$ with $a + b > 1$ is not simple. We leave it as an exercise to show that groups of order pqr ($p < q < r$ primes) are not simple. Note that $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$ and A_5 is simple. A theorem of Feit and Tompson says that a finite simple group is either of prime order, or of even order.

END OF LECTURE 2 (September 10)

1.8. **Semi-direct product.** Given two groups B, N we can construct their direct product $G = N \times B$. Identifying B, N with their images $\{1\} \times B, N \times \{1\}$ in G, we find that:

(1) $G = NB$;
(2) $N \cap B = \{1\}$;
(3) $N \lhd G, B \lhd G$.

Conversely, one can easily prove that if G is a group with subgroups B, N such that: (i) $G = NB$, (ii) $N \lhd G, B \lhd G$, (iii) $N \cap B = \{1\}$, then $G \cong N \times B$. The definition of a semi-direct product relaxes the conditions a little.

Definition 1.8.1. Let G be a group and let B, N be subgroups of G such that:

(1) $G = NB$;
(2) $N \cap B = \{1\}$;
(3) $N \lhd G$.

Then we say that G is a **semi-direct product** of N and B.

Let N be any group. Let $\mathrm{Aut}(N)$ be the set of automorphisms of the group N. It is a group in its own right under composition of functions. Let B be another group and $\phi : B \to \mathrm{Aut}(N), b \mapsto \phi_b$ be a homomorphism (so $\phi_{b_1 b_2} = \phi_{b_1} \circ \phi_{b_2}$). Define a group

$$G = N \rtimes_\phi B$$

as follows: as a set $G = N \times B$, but the group law is defined as

$$(n_1, b_1)(n_2, b_2) = (n_1 \cdot \phi_{b_1}(n_2), b_1 b_2).$$

We check associativity:

$$\begin{aligned}
[(n_1, b_1)(n_2, b_2)](n_3, b_3) &= (n_1 \cdot \phi_{b_1}(n_2), b_1 b_2)(n_3, b_3) \\
&= (n_1 \cdot \phi_{b_1}(n_2) \cdot \phi_{b_1 b_2}(n_3), b_1 b_2 b_3) \\
&= (n_1 \cdot \phi_{b_1}(n_2 \cdot \phi_{b_2}(n_3)), b_1 b_2 b_3) \\
&= (n_1, b_1)(n_2 \cdot \phi_{b_2}(n_3), b_2 b_3) \\
&= (n_1, b_1)[(n_2, b_2)(n_3, b_3)].
\end{aligned}$$

The identity is clearly $(1_N, 1_B)$. The inverse of (n_2, b_2) is $(\phi_{b_2^{-1}}(n_2^{-1}), b_2^{-1})$. Thus G is a group. The two bijections

$$N \to G, \quad n \mapsto (n, 1); \qquad B \to G, \quad b \mapsto (1, b),$$

are group homomorphisms. We identify N and B with their images in G. We claim that G is a semi-direct product of N and B.

Indeed, clearly the first two properties of the definition hold. It remains to check that N is normal and it's enough to verify that $B \subset N_G(N)$. According to the calculation above:

$$(1, b)(n, 1)(1, b^{-1}) = (\phi_b(n), 1).$$

We now claim that every semi-direct product is obtained this way: Let G be a semi-direct product of N and B. Let $\phi_b : N \to N$ be the map $n \mapsto bnb^{-1}$. This is an automorphism of N and the map

$$\phi : B \to \mathrm{Aut}(N)$$

is a group homomorphism. We claim that $N \rtimes_\phi B \cong G$. Indeed, define a map

$$(n, b) \mapsto nb.$$

It follows from the definition that the map is surjective. It is also bijective since $nb = 1$ implies that $n = b^{-1} \in N \cap B$ hence $n = 1$. It remains to check that this is a group homomorphism, but $(n_1 \cdot \phi_{b_1}(n_2), b_1 b_2) \mapsto n_1 \phi_{b_1}(n_2) b_1 b_2 = n_1 b_1 n_2 b_1^{-1} b_1 b_2 = (n_1 b_1)(n_2 b_2)$.

Proposition 1.8.2. *A semi-direct product $N \rtimes_\phi B$ is the direct product $N \times B$ if and only if $\phi : B \to \mathrm{Aut}(N)$ is the trivial homomorphism.*

Proof. Indeed, that happens iff for all $(n_1, b_1), (n_2, b_2)$ we have $(n_1 \phi_{b_1}(n_2), b_1 b_2) = (n_1 n_2, b_1 b_2)$. That is, iff for all b_1, n_2 we have $\phi_{b_1}(n_2) = n_2$, which implies $\phi_{b_1} = id$ for all b_1. That is, ϕ is the trivial homomorphism. □

Example 1.8.3. The Dihedral group D_{2n} is a semi-direct product. Take $N =< x > \cong \mathbb{Z}/n\mathbb{Z}$ and $B =< y > \cong \mathbb{Z}/2\mathbb{Z}$. Then $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$ with $\phi_1 = -1$.

1.8.1. *Application to groups of order pq.* We have seen in § 1.7.11 that if $p < q$ and $p \not| (q-1)$ then every group of order pq is abelian. Assume therefore that $p|(q-1)$.

Proposition 1.8.4. *If $p|(q-1)$ there is a unique non-abelian group, up to isomorphism, of order pq.*

Proof. Let G be a non-abelian group of order pq. We have seen that in every such group G the q-Sylow subgroup Q is normal. Let P be any p-Sylow subgroup. Then $P \cap Q = \{1\}$ and $G = QP$. Thus, G is a semi-direct product of Q and P.

It is thus enough to show that there is a non-abelian semi-direct product and that any two such products are isomorphic. We may consider the case $Q = \mathbb{Z}/q\mathbb{Z}, P = \mathbb{Z}/p\mathbb{Z}$.

Lemma 1.8.5. $\mathrm{Aut}(Q) = (\mathbb{Z}/q\mathbb{Z})^\times$. *In fact, for any positive integer N, $\mathrm{Aut}(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, the group of units of the ring $\mathbb{Z}/N\mathbb{Z}$.*

Proof. Since $\mathbb{Z}/N\mathbb{Z}$ is cyclic any group homomorphism $f : \mathbb{Z}/N\mathbb{Z} \to H$ to a group H is determined by its value on a generator of $\mathbb{Z}/N\mathbb{Z}$, say 1. Conversely, if $h \in H$ is of order dividing N then there is such a group homomorphism with $f(1) = h$. Now take $H = \mathbb{Z}/N\mathbb{Z}$. The image of f is the cyclic subgroup $< h >$ and thus f is surjective (equivalently, an isomorphism) iff h is a generator. Thus, any element $h \in (\mathbb{Z}/N\mathbb{Z})^\times$ determines an automorphism f_h of $\mathbb{Z}/N\mathbb{Z}$ by $a \mapsto ah$. Note that $f_h(f_g)(a) = f_h(ag) = agh = f_{hg}(a)$ and so the association $h \leftrightarrow f_h$ is a group isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/N\mathbb{Z})$. □

Since $(\mathbb{Z}/q\mathbb{Z})^\times$ is a cyclic group of order $q-1$ (because it is the group of non-zero elements of a finite field), and since $p|(q-1)$, there is an element h of exact order p in $(\mathbb{Z}/q\mathbb{Z})^\times$. Let ϕ be the homomorphism determined by $\phi_1 = f_h$ and let $G = Q \rtimes_\phi P$. G is not abelian by Proposition 1.8.2

We now show that G is unique up to isomorphism. If H is another such semi-direct product then $H = \mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$, where ψ_1 is an element of order p (if it is the identity H is abelian) and thus $\psi_1 = \phi_1^r = \phi_r$ for some r prime to p.

Define a map

$$\mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \rtimes_\phi \mathbb{Z}/p\mathbb{Z}, \quad (n, b) \mapsto (n, rb).$$

This function is easily checked to be injective, hence bijective. We check it is a group homomorphism:

In G we have $(n_1, rb_1)(n_2, rb_2) = (n_1 + \phi_{rb_1}(n_2), r(b_1 + b_2)) = (n_1 + \psi_{b_1}(n_2), r(b_1 + b_2))$ which is the image of $(n_1 + \psi_{b_1}(n_2), b_1 + b_2)$, the product $(n_1, b_1)(n_2, b_2)$ in H. □

Example 1.8.6. Is there a non-abelian group of order 165 containing $\mathbb{Z}/55\mathbb{Z}$?

In such a group G, the subgroup $\mathbb{Z}/55\mathbb{Z}$ must be normal (its index is the minimal prime dividing the order of G). Since there is always a 3-Sylow, we conclude that G is a semi-direct product $\mathbb{Z}/55\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. This is determined by a homomorphism $\mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/55\mathbb{Z}) \cong (\mathbb{Z}/55\mathbb{Z})^\times$. The right hand side has order $\varphi(55) = 4 \cdot 10$. Thus, the homomorphism is trivial and G is a direct product. It follows that G must be commutative.

1.8.2. *Cases where two semi-direct products are isomorphic.* It is useful to generalize the last argument. Consider a map $\phi : B \to \mathrm{Aut}(N)$ be a homomorphism and consider the group

$$G = N \rtimes_\phi B.$$

Consider two automorphisms $f : N \to N, g : B \to B$. Let S be G considered as a set and consider the self map

$$S \to S, \quad (n, b) \mapsto (f(n), g(b)).$$

We may define a new group law on S by

$$\begin{aligned}(n_1, b_1) \star (n_2, b_2) &= f \circ g \left[(f^{-1}(n_1), g^{-1}(b_1))(f^{-1}(n_2), g^{-1}(b_2))\right] \\ &= f \circ g \left[(f^{-1}(n_1) \cdot [\phi(g^{-1}(b_1))](f^{-1}(n_2)), g^{-1}(b_1)g^{-1}(b_2))\right] \\ &= (n_1 \cdot f([\phi(g^{-1}(b_1))](f^{-1}(n_2))), b_1 b_2)\end{aligned}$$

Clearly, S with the new group law is isomorphic as groups to G. This suggests the following, define an action of $\mathrm{Aut}(B) \times \mathrm{Aut}(N)$ on $\mathrm{Hom}(B, \mathrm{Aut}(N))$ via the embedding $\mathrm{Aut}(B) \times \mathrm{Aut}(N) \to \mathrm{Aut}(B) \times \mathrm{Aut}(\mathrm{Aut}(N))$. That is, $g \in \mathrm{Aut}(B)$ acts by $\phi \mapsto \phi \circ g$ and $f \in \mathrm{Aut}(N)$ acts by $\phi \mapsto c_f \circ \phi$, where c_f is conjugation by f. That is, $(c_f \circ \phi)(b) = f\phi(b)f^{-1}$. Then, we see that every orbit for this action gives isomorphic groups $N \rtimes_\phi B$. Note that the action of $\mathrm{Aut}(B) \times \mathrm{Aut}(N)$ on $\mathrm{Hom}(B, \mathrm{Aut}(N))$ factors through $\mathrm{Aut}(B) \times \mathrm{Aut}(N)/Z(\mathrm{Aut}(N))$.

Example 1.8.7. As we have seen, this action shows that there is a unique non-abelian group of order pq, where $p < q, p|(q-1)$, up to isomorphism. Indeed, first we showed that such a group is a semi-direct product $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ relative to $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/q\mathbb{Z}^\times$. The homomorphism θ is determined by $\theta(1)$ which is an element of order p. Now, $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^\times$ and an element b acts on θ by $\theta \mapsto \theta \circ b$. As $\theta \circ b(1) = \theta(b) = \theta(1)^b$, which is another element of order p of $\mathbb{Z}/q\mathbb{Z}^\times$. In fact, any element of order p is of the form $\theta(1)^b$ for some b (the cyclic subgroup $\mathbb{Z}/q\mathbb{Z}^\times$ of order $(q-1)$ has a unique cyclic subgroup of order p; every element of order p of $\mathbb{Z}/q\mathbb{Z}^\times$ thus belongs to it, and thus there are $p-1$ elements of order p which are all powers of each other). This already shows that all the non-abelian semi-direct products $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ are isomorphic. The other action, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ acting on itself by conjugation is trivial because $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ is an abelian group.

Example 1.8.8. We consider non-abelian semi-direct products

$$\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}.$$

$\mathbb{Z}/p^2\mathbb{Z}^\times$ is a cyclic group of order $p(p-1)$, a fact left as an exercise. It thus has precisely $p-1$ elements of order p, comprising the non-trivial elements of the unique subgroup of p elements. They are each powers of each other. Again, a nontrivial homomorphism $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ is determined by $\theta(1)$, which is an element of exact order p. An argument as above shows that any two non abelian semidirect products are isomorphic $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. The group we get has an element of order p^2. In fact, for $p > 2$, any non-abelian group of order p^3 having an element of order p^2 is isomorphic to this group. To prove that one only needs to show that such a group is a semi-direct product $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. This is not that easy, and a guided proof appears in the exercises.

END OF LECTURE 3 (September 12)

1.8.3. *Groups of small order.* Using our results thus far, we can get a pretty good idea of the groups of small order.

order	abelian	non-abelian
2	$\mathbb{Z}/2\mathbb{Z}$	–
3	$\mathbb{Z}/3\mathbb{Z}$	–
4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/4\mathbb{Z}$	–
5	$\mathbb{Z}/5\mathbb{Z}$	–
6	$\mathbb{Z}/6\mathbb{Z}$	$S_3 \cong D_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
7	$\mathbb{Z}/7\mathbb{Z}$	–
8	$(\mathbb{Z}/2\mathbb{Z})^3$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/8\mathbb{Z}$	$Q = \{\pm 1, \pm i, \pm j, \pm k\}$ $D_4 \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
9	$(\mathbb{Z}/3\mathbb{Z})^2$ $\mathbb{Z}/9\mathbb{Z}$	–
10	$\mathbb{Z}/10\mathbb{Z}$	$D_5 \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
11	$\mathbb{Z}/11\mathbb{Z}$	–
12	$(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$ $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$A_4 \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$ $D_6 \cong \mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$ $T \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
13	$\mathbb{Z}/13\mathbb{Z}$	–
14	$\mathbb{Z}/14\mathbb{Z}$	$D_7 \cong \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$
15	$\mathbb{Z}/15\mathbb{Z}$	–

In the following table we list for every n the number $G(n)$ of subgroups of order n (this is taken from J. Rotman/*An introduction to the theory of groups*):

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$G(n)$	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1

n	20	21	22	23	24	25	26	27	28	29	30	31	32
$G(n)$	5	2	2	1	15	2	2	5	4	1	4	1	51

There are 2328 isomorphism classes of groups of order 128.[3]

[3] James, Newman and O'Brien, Journal of Algebra **129**, Issue 1, 1990, 136 -158.

1.9. **The Cauchy-Frobenius formula and applications to combinatorics.**

Theorem 1.9.1. (CFF) *Let G be a finite group acting on a finite set non-empty S. Let N be the number of orbits of G in S. Define*

$$\mathrm{Fix}(g) = |\{s \in S : g \star s = s\}|$$

(the number of elements of S fixed by the action of g). Then

$$N = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g). \tag{3}$$

Remark 1.9.2. If $N = 1$ we say that G acts **transitively** on S. It means exactly that: For every $s_1, s_2 \in S$ there exists $g \in G$ such that $g \star s_1 = s_2$.

Proof. We define a function

$$T : G \times S \to \{0, 1\}, \quad T(g, s) = \begin{cases} 1 & g \star s = s \\ 0 & g \star s \neq s \end{cases}.$$

Note that for a fixed $g \in G$ we have

$$\mathrm{Fix}(g) = \sum_{s \in S} T(g, s),$$

and that for a fixed $s \in S$ we have

$$|\mathrm{Stab}(s)| = \sum_{g \in G} T(g, s).$$

Let us fix representatives $s_1, \ldots, s_N$ for the N disjoint orbits of G in S. Now,

$$\begin{aligned}
\sum_{g\in G} \mathrm{Fix}(g) &= \sum_{g\in G}\left(\sum_{s\in S} T(g,s)\right)\\
&= \sum_{s\in S}\left(\sum_{g\in G} T(g,s)\right)\\
&= \sum_{s\in S} |\mathrm{Stab}(s)|\\
&= \sum_{s\in S} \frac{|G|}{|\mathrm{Orb}(s)|}\\
&= \sum_{i=1}^{N}\sum_{s\in \mathrm{Orb}(s_i)} \frac{|G|}{|\mathrm{Orb}(s)|}\\
&= \sum_{i=1}^{N}\sum_{s\in \mathrm{Orb}(s_i)} \frac{|G|}{|\mathrm{Orb}(s_i)|}\\
&= \sum_{i=1}^{N} \frac{|G|}{|\mathrm{Orb}(s_i)|}\cdot |\mathrm{Orb}(s_i)|\\
&= \sum_{i=1}^{N} |G|\\
&= N\cdot |G|.
\end{aligned}$$

□

Corollary 1.9.3. *Let G be a finite group acting transitively on a finite non-empty set S. Suppose that $|S| > 1$. Then there exists $g \in G$ without fixed points.*

Proof. By contradiction. Suppose that every $g \in G$ has a fixed point in S. That is, suppose that for every $g \in G$ we have

$$\mathrm{Fix}(g) \geq 1.$$

Since $\mathrm{Fix}(e) = |S| > 1$ we have that

$$\sum_{g\in G} \mathrm{Fix}(g) > |G|.$$

By Cauchy-Frobenius formula, the number of orbits N is greater than 1. Contradiction. □

1.9.1. *Applications to combinatorics.*

Example 1.9.4. How many roulettes with 11 wedges painted 2 blue, 2 green and 7 red are there when we allow rotations?

Let S be the set of painted roulettes. Let us enumerate the sectors of a roulette by the numbers $1, \ldots, 11$. The set S is a set of $\binom{11}{2}\binom{9}{2} = 1980$ elements (choose which 2 are blue, and then choose out of the nine left which 2 are green).

Let G be the group $\mathbb{Z}/11\mathbb{Z}$. It acts on S by rotations. The element 1 rotates a painted roulette by angle $2\pi/11$ anti-clockwise. The element n rotates a painted roulette by angle $2n\pi/11$ anti-clockwise. We are interested in N – the number of orbits for this action. We use **CFF**.

The identity element always fixes the whole set. Thus $\mathrm{Fix}(0) = 1980$. We claim that if $1 \leq i \leq 10$ then i doesn't fix any element of S. Indeed, suppose that $1 \leq i \leq 10$ and i fixes s. Then so does $\langle i \rangle = \mathbb{Z}/11\mathbb{Z}$ (the stabilizer is a subgroup). But any coloring fixed under rotation by 1 must be single colored! Contradiction.

Applying **CFF** we get

$$N = \frac{1}{11}\sum_{n=0}^{10} \mathrm{Fix}(n) = \frac{1}{11} \cdot 1980 = 180.$$

Example 1.9.5. How many roulettes with 12 wedges painted 2 blue, 2 green and 8 red are there when we allow rotations?

Let S be the set of painted roulettes. Let us enumerate the sectors of a roulette by the numbers $1, \ldots, 12$. The set S is a set of $\binom{12}{2}\binom{10}{2} = 2970$ elements (choose which 2 are blue, and then choose out of the ten left which 2 are green).

Let G be the group $\mathbb{Z}/12\mathbb{Z}$. It acts on S by rotations. The element 1 rotates a painted roulette by angle $2\pi/12$ anti-clockwise. The element n rotates a painted roulette by angle $2n\pi/12$ anti-clockwise. We are interested in N – the number of orbits for this action. We use **CFF**.

The identity element always fixes the whole set. Thus $\mathrm{Fix}(0) = 2970$. We claim that if $1 \leq i \leq 11$ and $i \neq 6$ then i doesn't fix any element of S. Indeed, suppose that i fixes a painted roulette. Say in that roulette the r-th sector is blue. Then so must be the $i + r$ sector (because the r-th sector goes under the action of i to the $r + i$-th sector). Therefore so must be the $r + 2i$ sector. But there are only 2 blue sectors! The only possibility is that the $r + 2i$ sector is the same as the r sector, namely, $i = 6$.

If i is equal to 6 and we enumerate the sectors of a roulette by the numbers $1, \ldots, 12$ we may write i as the permutation

$$(1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 11)(6\ 12).$$

In any coloring fixed by $i = 6$ the colors of the pairs $(1\ 7), (2\ 8), (3\ 9), (4\ 10), (5\ 11)$ and $(6\ 12)$ must be the same. We may choose one pair for blue, one pair for green. The rest would be red. Thus there are $30 = 6 \cdot 5$ possible choices. We summarize:

element g	$\mathrm{Fix}(g)$
0	2970
$i \neq 6$	0
$i = 6$	30

Applying **CFF** we get that there are

$$N = \frac{1}{12}(2970 + 30) = 250$$

different roulettes.

Example 1.9.6. In this example S is the set of necklaces made of four rubies and four sapphires laid on the table. We ask how many necklaces there are when we allow rotations and flipping-over.

We may talk of S as the colorings of a regular octagon, four vertices are green and four are red. The group $G = D_{16}$ acts on S and we are interested in the number of orbits for the group G.

The results are the following

element g	Fix(g)
e	70
x, x^3, x^5, x^7	0
x^2, x^6	2
x^4	6
yx^i for $i = 0, \ldots, 7$	6

We explain how the entries in the table are obtained:

The identity always fixes the whole set S. The number of elements in S is $\binom{8}{4} = 70$ (chossing which 4 would be green).

The element x cannot fix any coloring, because any coloring fixed by x must have all sections of the same color (because $x = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$). If x^r fixes a coloring s_0 so does $(x^r)^r = x^{(r^2)}$ because the stabilizer is a subgroup. Apply that for $r = 3, 5, 7$ to see that if x^r fixes a coloring so does x , which is impossible. [4]

Now, x^2 written as a permutation is $(1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. We see that if, say 1 is green so are $3, 5, 7$ and the rest must be red. That is, all the freedom we have is to choose whether the cycle $(1\ 3\ 5\ 7)$ is green or red. This gives us two colorings fixed by x^2. The same rational applies to $x^6 = (8\ 6\ 4\ \ 2)(7\ 5\ 3\ 1)$.

Consider now x^4. It may written in permutation notation as $(1\ 5)(2\ 6)(3\ 7)(4\ 8)$. In any coloring fixed by x^4 each of the cycles $(1\ 5)(2\ 6)(3\ 7)$ and $(4\ 8)$ must be single colored. There are thus $\binom{4}{2} = 6$ possibilities (Choosing which 2 out of the four cycles would be green).

It remains to deal with the elements yx^i. We recall that these are all reflections. There are two kinds of reflections. One may be written using permutation notation as

$$(i_1\ i_2)(i_3\ i_4)(i_5\ i_6)$$

(with the other two vertices being fixed. For example $y = (2\ 8)(3\ 7)(4\ 6)$ is of this form). The other kind is of the form

$$(i_1\ i_2)(i_3\ i_4)(i_5\ i_6)(i_7\ i_8).$$

(For example $yx = (1\ 8)(2\ 7)(3\ 6)(4\ 5)$ is of this sort). Whatever is the case, one uses similar reasoning to deduce that there are 6 colorings preserved by a reflection.

One needs only apply **CFF** to get that there are

$$N = \frac{1}{16}(70 + 2 \cdot 2 + 6 + 8 \cdot 6) = 8$$

distinct necklaces.

Example 1.9.7. Suppose we have n-colours and we want to count the number of distinct colourings of a tetrahedron under rotational symmetries (we colour the faces). Number the vertices as $\{1, 2, 3, 4\}$ to represent the symmetries as a subgroup of S_4, that clearly contains all 3-cycles. It must then be isomorphic to either A_4, S_4. But the symmetry (12) is not rotational (it doesn't preserve orientation). Thus, the group of symmetries we are interested in is A_4. It has the identity elements, 8 elements that are 3-cycles, and 3 elements that form the Klein four group $\{(12)(34), (13)(24), (14)(23)\}$.

The number of possible colourings is n^4. Each colouring is preserved by the identity. A 3-cycle leaves on face stable, and permutes cyclically the other 3. Thus, a 3-cycle preserves n^2 colourings (n

[4] $x^{(3^2)} = x^9 = x$ because $x^8 = e$, etc.

choices for the fixed face, n choices for the colour of the 3 faces permuted cyclically). A permutation such as (12)(34) switches the faces in pairs and so again fixed n^2 colourings. Applying the CFF formula, we find that there are

$$\frac{1}{12}(n^4 + 11n^2)$$

distinct colourings of the tetrahedron using n colours. It is a healthy instinct to check at this point that this number is always an integer (it is!).

1.10. **Simplicity of** $\mathrm{PSL}_n(\mathbb{F}_q)$**.** You have seen in the first course on group theory that the alternating groups A_n are simple for $n \geq 5$. Here we provide another infinite family of finite simple groups. This family is constructed from algebraic groups. The construction applies to other algebraic groups and by the classification theorem of finite simple groups - one of the monumental achievements of the 20^{th} century - this list, together with the cyclic groups of prime order, covers all finite simple groups except for a very short list of exceptional groups, called the sporadic groups.

Let $\mathbb{F}$ be a finite field with $q = p^r$ elements, where p is a prime. The group $\mathrm{SL}_n(\mathbb{F})$ is the group of $n \times n$ matrices with entries in $\mathbb{F}$ and determinant 1. The set of scalar matrices in SL_n is a normal subgroup, consisting of the matrices $\{\mathrm{diag}(\mu, \mu, \ldots, \mu) : \mu \in \mathbb{F}, \mu^n = 1\}$, and has order $d = \gcd(n, q-1)$. In fact, it is the centre of $\mathrm{SL}_n(\mathbb{F})$. Denote it by K. We wish to prove that for $n > 1$,

$$\mathrm{PSL}_n(\mathbb{F}) := \mathrm{SL}_n(\mathbb{F})/K,$$

is a simple group, except in the two cases $n = 2$ and $q \leq 3$.

We say that a group acts **faithfully** on a set S if the homomorphism $G \to \Sigma_S$ is injective. That is, if $g \in G$ is not the identity element then there is an $s \in S$ such that $gs \neq s$. We say that G acts **doubly-transitively** on S if for each $a \neq b$ in S and $c \neq d$ in S there is an element $g \in G$ such that $ga = c, gb = d$.

We say that G acts **primitively** on a set S if G acts transitively, $|S| > 1$, and there is no partition of S preserved by the action of G besides the trivial partitions ($S = S$ and $S = \coprod_{s \in S}\{s\}$). For example, if the action is 2-transitive, it's primitive. If $|S| > 2$ there is no need to require that the action of G is transitive in the definition of primitive action; it is so automatically.

Lemma 1.10.1. *Let G act transitively on a set S. Then, G acts primitively if and only if the point stabilizer of a point of S is a proper maximal subgroup of G.*

Proof. We prove the direction needed in the sequel. Suppose that G acts primitively and let $s \in S$ with stabilizer H. We may assume without loss of generality that the action is the action of G on the cosets space G/H. Suppose that there is a proper subgroup J that strictly contains H. G acts on the coset space G/J. Each coset of J is a disjoint union of cosets of H and that produces a non-trivial partition of G/H, which is preserved by the action of G. □

Lemma 1.10.2 (Iwasawa)**.** *Let G be a finite* **perfect** *group, i.e., $G = G'$, acting faithfully and primitively on a set S, such that the stabilizer H of some point in S has a normal abelian subgroup A whose conjugates generate G, then G is simple.*

Proof. Suppose not. Let K be a non-trivial normal subgroup of G. K doesn't fix *every* element of S, because of the faithfulness assumption. Remark that the conditions of the lemma hold for every point $s \in S$ if they hold for one point in S. Therefore, we may choose a point stabilizer H such that $K \not\subset H$. Say H is the stabilizer of s_0.

Since K is normal, HK is a subgroup of G and it strictly contains H. The action being primitive implies that H is a maximal subgroup of G. Therefore,

$$HK = G.$$

It follows that every element of G is of the form hk with $h \in H$ and $k \in K$. If $a \in A$ then $k^{-1}h^{-1}ahk = k^{-1}a'k \in AK$. Therefore, all the conjugates of A lie in the subgroup AK and thus, $G = AK$. But then

$$G/K = AK/K \cong A/A \cap K,$$

is a non-trivial abelian group, contradicting the assumption that G is perfect. □

END of lecture 4 (September 17)

It remains to examine when does $\mathrm{PSL}_n(\mathbb{F})$ satisfy the assumptions of the Lemma. We first explain the set on which $\mathrm{PSL}_n(\mathbb{F})$ acts. This set S is the set of lines in the vector space $\mathbb{F}^n$; it is called the **projective space** of dimension $n-1$ over $\mathbb{F}$ and denoted $\mathbb{P}^{n-1}_{\mathbb{F}}$ (and in many other ways too). The natural action of $\mathrm{SL}_n(\mathbb{F})$ factors through $\mathrm{PSL}_n(\mathbb{F})$. Moreover, the action is 2-transitive, hence primitive. The stabilizer of a line H is the matrices in $\mathrm{PSL}_n(\mathbb{F})$ of the form $\begin{pmatrix} t & * \\ 0 & M \end{pmatrix}$, where $t \cdot \det(M) = 1$. As our subgroup A we take the matrices of the form $\begin{pmatrix} 1 & v_{n-1} \\ 0 & I_{n-1} \end{pmatrix}$, where v_{n-1} is any vector of length n. It is an abelian subgroup which is normal in H, being the kernel of the homomorphism to $\mathrm{GL}_{n-1}(\mathbb{F})$, $\begin{pmatrix} t & * \\ 0 & M \end{pmatrix} \mapsto M$.

We note that every element of H is a transvection: a transformation T such that $T - I_n$ has rank 1 and $(T - I_n)^2 = 0$. We claim that every transvection of $\mathrm{SL}_n(\mathbb{F})$ is conjugate within $\mathrm{SL}_n(\mathbb{F})$ to a transvection in A. Indeed, the minimal polynomial of a transvection is $(x-1)^2$. The Jordan canonical form together with the rank condition supply us with a basis $u_1, \ldots, u_n$ for which $(T - I_n)(u_i) = 0$, except for $(T - I_n)(u_2) = u_1$. This being true for every transvection proves that they are all conjugate in $\mathrm{GL}_n(\mathbb{F})$. Thus, given two transvections S, T there is matrix M such that $MSM^{-1} = T$, where we suppose T is represented by $\begin{pmatrix} 1 & 1 & 0 & \ldots & 0 \\ & 1 & 0 & \ldots & 0 \\ & & I_{n-2} & & \end{pmatrix}$. To make M have determinant 1 we replace it by $M \times \mathrm{diag}(d, 1, \ldots, 1)$ at the cost of arriving at

$$\mathrm{diag}(d, 1, \ldots, 1) \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 \\ & 1 & 0 & \ldots & 0 \\ & & I_{n-2} & & \end{pmatrix} \mathrm{diag}(d^{-1}, 1, \ldots, 1) = \begin{pmatrix} 1 & d & 0 & \ldots & 0 \\ & 1 & 0 & \ldots & 0 \\ & & I_{n-2} & & \end{pmatrix}.$$

Lemma 1.10.3. *The group* $\mathrm{SL}_n(\mathbb{F})$ *is generated by transvections.*

Proof. We leave the proof as an exercise. It amounts to the statement that every matrix of determinant 1 can be reduced to the identity matrix using column and row operations of the form $c_i \mapsto c_i + \lambda c_j$ and $r_i \mapsto r_i + \lambda r_j$, noting that we can use *any* transvection. □

At this point, we have our group, our set and the subgroup A. The only thing missing is the following.

Lemma 1.10.4. *The group* $\mathrm{SL}_n(\mathbb{F})$*, and hence* $\mathrm{PSL}_n(\mathbb{F})$*, is perfect, except for the case* $\mathrm{SL}_2(\mathbb{F}_2)$ *and* $\mathrm{SL}_2(\mathbb{F}_3)$*.*

Proof. Since the derived group is normal, it is enough to show that every transvection of the form $\begin{pmatrix} 1 & t & 0 & \dots & 0 \\ 0 & & I_{n-1} & & \end{pmatrix}$ is a commutator. One checks that

$$\left[\begin{pmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which, by the calculation above (taking M to be the permutation matrix of the transposition (23) and $d = -1$) is conjugate to $\begin{pmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. That shows that all transvections belong to the commutator subgroup if $n \geq 3$.

For $n = 2$ we check that

$$\left[\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & y(x^2-1) \\ 0 & 1 \end{pmatrix}.$$

For $q > 3$ this is an arbitrary element of A. □

2. The Jordan-Hölder theorem and solvable groups

2.1. **Composition series and composition factors.** Let G be a group. A **normal series** for G is a series of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}.$$

A **composition series** for G is a series of subgroups

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

such that G_{i-1}/G_i is a nontrivial simple group for all $i = 1, \ldots, n$. The **composition factors** are the quotients $\{G_{i-1}/G_i : i = 1, 2, \ldots, n\}$. The quotients are considered up to isomorphism, where the order of the quotients doesn't matter, but we do take the quotients with multiplicity. For example, the group D_4 has a composition series

$$D_4 \rhd \langle y \rangle \rhd \langle y^2 \rangle \rhd \{1\}.$$

The composition factors are $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\}$.

A group G is called **solvable** if it has a normal series in which all the composition factors are abelian groups. If G is finite then G is solvable if and only if it has a composition series whose composition factors are cyclic groups of prime order.

2.2. **Jordan-Hölder Theorem.** The Jordan-Holder theorem clarifies greatly the yoga behind the concept of composition series.

Theorem 2.2.1. *Let G be a finite group. Any two composition series for G have the same composition factors (considered with multiplicity).*

Note that a consequence of the theorem is that any two composition series have the same length, since the length determines the number of composition factors.

The proof of the theorem is quite technical, unfortunately. It rests on the following lemma.[5]

Lemma 2.2.2. *(Zassenhaus) Let $A \lhd A^*$, $B \lhd B^*$ be subgroups of a group G. Then*

$$A(A^* \cap B) \lhd A(A^* \cap B^*), \qquad B(B^* \cap A) \lhd B(B^* \cap A^*),$$

and

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}.$$

Before the proof, recall some easy to prove facts: (i) Let $S \lhd G$, $T < G$ be subgroups of a group G. Then ST is a subgroup of G (and $ST = TS$). (ii) If also $T \lhd G$ then $ST \lhd G$.

Proof. Let D be the following set:

$$D = (A^* \cap B)(A \cap B^*).$$

We show that D is a normal subgroup of $A^* \cap B^*$, $D = (A \cap B^*)(A^* \cap B)$ and

$$\frac{B(B^* \cap A^*)}{B(B^* \cap A)} \cong \frac{A^* \cap B^*}{D}.$$

The lemma then follows from the symmetry of the roles of A and B.

It is easy to check directly from the definitions that $(A^* \cap B) \lhd A^* \cap B^*$ and, similarly, $(A \cap B^*) \lhd A^* \cap B^*$. It follows that $D \lhd A^* \cap B^*$ and that $D = (A \cap B^*)(A^* \cap B)$. The subtle point of the proof is to construct a homomorphism

$$f : B(B^* \cap A^*) \to \frac{A^* \cap B^*}{D}.$$

[5] Our proof follows Rotman's in *An introduction to the theory of groups*.

Let $x \in B(B^* \cap A^*)$, say $x = bc$ for $b \in B, c \in (B^* \cap A^*)$. Let

$$f(x) = cD$$

(which is an element of $\frac{A^* \cap B^*}{D}$.)

First, f is well defined. If $x = b_1c_1$ then $c_1c^{-1} = b_1^{-1}b \in (B^* \cap A^*) \cap B \subset D$. As $D \lhd (B^* \cap A^*)$ and $c_1 \in (B^* \cap A^*)$ also $c^{-1}c_1 \in D$, and so $cD = c_1D$. Next, f is a homomorphism. Suppose that $x = bc, y = b_1c_1$ and so $xy = bcb_1c_1$. Note that $cb_1c^{-1} \in B$ (as B is normal in B^* and $c \in B^*$) and so $xy = bb'cc_1$ for some $b' \in B$. It now follows that $f(xy) = f(x)f(y)$.

It is clear from the definition that f is a surjective homomorphism. When is $x = bc \in \mathrm{Ker}(f)$? This happens if and only if $c \in D$, that is $x \in B(A^* \cap B)(A \cap B^*) = B(A \cap B^*)$. This shows that $B(A \cap B^*) \lhd B(A^* \cap B^*)$ and the desired isomorphism. □

END of lecture 5 (September 19)

Theorem 2.2.3. *Let G be a group. Any two finite composition series for G are equivalent; namely, have the same composition factors.*

Proof. More generally, we prove that any two normal series for G have refinements that are equivalent; namely, have the same composition factors (with the same multiplicities). This holds also for infinite groups that may not have composition series, and so is useful in other situations. In the case of composition series, since they cannot be refined in a non-trivial, as the quotients are simple groups, we get that any two composition series for G (if they exist at all) are equivalent.

Thus, let

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

and

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = \{1\}.$$

First, use the second series to refine the first. Define:

$$G_{ij} = G_{i+1}(G_i \cap H_j).$$

For fixed i, this is a descending series of sets, beginning at $G_{i0} = G_i$ and ending at $G_{im} = G_{i+1}$. Taking in the Zassenhaus lemma $A = G_{i+1}, A^* = G_i, B = H_{j+1}, B^* = H_j$ gives us that $G_{i,j+1} = A(A^*B) \lhd G_{ij} = A(A^* \cap B^*)$ (and, in particular, that these are subgroups).

Similarly, now use the first series to refine the second by defining

$$H_{ij} = H_{j+1}(H_j \cap G_i).$$

As above, the series $H_j = H_{0j} \supset H_{1j} \supset \cdots \supset H_{nj} = H_{j+1}$ is a series of subgroups, each normal in the former. Finally, applying the Zassenhaus lemma again to $A = G_{i+1}, A^* = G_i, B = H_{j+1}, B^* = H_j$, we find that

$$\frac{G_{ij}}{G_{i,j+1}} = \frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)} = \frac{H_{ij}}{H_{i+1,j}}.$$

This gives a precise matching of the factors. □

Note that every finite group G has a composition series. While the composition series itself is not unique, the composition factors are. So, in a sense, the Jordan-Hölder theorem is a unique factorization theorem for groups. From this point of view, the simplest groups are the solvable groups. These are the groups with the simplest factors - cyclic groups of prime order. We therefore now focus our attention on solvable groups for a while. Their study is further motivated by Galois theory and we shall return to this point later in §**??**.

2.3. **Solvable groups.** Recall that a group G is called **solvable** if there is a finite normal series for G,

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

with abelian quotients. Every abelian group is solvable. Any group of order pq, where $p < q$ are primes is solvable as the q-Sylow is always normal and the quotient is a group of order p, hence cyclic. Similarly, we have seen that groups of order p^2q and pqr, where p, q, r are distinct primes, are solvable. A theorem of Burnside states that groups of order p^aq^b are solvable.

Of course, not every group is solvable. Any non-abelian simple group (such as A_n for $n \geq 5$, and $\mathrm{PSL}_n(\mathbb{F}_q)$ for $n \geq 2$ and $(n, q) \neq (2, 2)$ or $(2, 3)$) is non solvable.

The class of solvable groups is closed under basic operations. More precisely.

Proposition 2.3.1. *A subgroup of a solvable group is solvable. A homomorphic image of a solvable group is solvable.*

Proof. Let G be a solvable group with a finite normal series,

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\},$$

with abelian quotients. Let H be a subgroup of G. One checks that

$$H = G_0 \cap H \rhd G_1 \cap H \rhd \cdots \rhd G_n \cap H = \{1\}$$

is a normal series for H with abelian quotients.

Let $f : G \to K$ be a surjective homomorphism. One checks that

$$K = f(G_0) \rhd f(G_1) \rhd \cdots \rhd f(G_n) = \{1\}$$

is a normal series for K with abelian quotients. □

Proposition 2.3.2. *Let*

$$0 \to G_1 \to G \to G_2 \to 0$$

be an exact sequence of groups. Then G is solvable if and only if both G_1 and G_2 are solvable.

This too is left as an exercise. Note that we had already shown one direction: if G is solvable so are G_1 and G_2.

3. Free groups and free products

3.1. **Categories: Definition of a category.** A **category C** consists in two things: **objects** and **morphisms**. Thus, a category $\mathbf{C}$ is a collection of objects $\mathrm{Ob}(\mathbf{C})$ and for any two objects X, Y of $\mathbf{C}$ a set $\mathrm{Mor}(X, Y)$, called the morphisms from X to Y. If we need to specify the category in our notation, we shall write $\mathrm{Mor}_C(X, Y)$. Further, for any three objects X, Y, Z there is a composition function

$$\mathrm{Mor}(Y, Z) \times \mathrm{Mor}(X, Y) \to \mathrm{Mor}(X, Z), \qquad (g, f) \mapsto g \circ f,$$

such that composition is associative: $h \circ (g \circ f) = (h \circ g) \circ f$. In addition, for every object X there is a morphism $1_X \in \mathrm{Mor}(X, X)$ such that $g \circ 1_X = g$ for all $g \in \mathrm{Mor}(X, Y)$ and $1_X \circ f = f$ for all $f \in \mathrm{Mor}(Y, X)$.

It should be stressed that there is no assumption that objects are sets, or that morphisms are actually functions. The notation $g \circ f$ is formal. Nonetheless, the notation is suggestive and by-and-large categories behave as if their objects were sets and their morphisms functions.

3.1.1. *Example:* **Sets**. The category of sets **Sets** is the category whose objects are sets and whose morphisms are functions.

3.1.2. *Example:* **Gp**. The category of groups **Gp** is the category whose objects are groups and for any two groups G, H, the morphisms $\mathrm{Mor}(G, H)$ are the group homomorphisms $f : G \to H$.

3.1.3. *Example:* **AbGp**. The category of abelian groups **AbGp** is the category whose objects are abelian groups and for any two abelian groups G, H, the morphisms $\mathrm{Mor}(G, H)$ are the group homomorphisms $f : G \to H$.

In general a category $\mathbf{D}$ is called a **subcategory** of a category $\mathbf{C}$ if $\mathrm{Ob}(\mathbf{D}) \subseteq \mathrm{Ob}(\mathbf{C})$ and for any X, Y objects of D, $\mathrm{Mor}_D(X, Y) \subseteq \mathrm{Mor}_C(X, Y)$. If, in fact, for every X, Y objects of D, $\mathrm{Mor}_D(X, Y) = \mathrm{Mor}_C(X, Y)$, one calls $\mathbf{D}$ a **full subcategory**. For example, **AbGp** is a full subcategory of **Gp**.

Here is an artificial example of a subcategory $\mathbf{E}$ of **Gp** that is not a full subcategory. The objects of $\mathbf{E}$ are groups of order, say, 32 and the morphisms are defined as $\mathrm{Mor}(G, G) = \{1_G\}$ and $\mathrm{Mor}(G, H) = \emptyset$ if $G \neq H$. (In the same vain, we could have taken as the objects of $\mathbf{E}$ the same objects of **Gp**.)

3.1.4. *Example:* $\mathbf{VSp}_k$. Let k be a field and let $\mathbf{VSp}_k$ be the category of k-vector spaces. The morphisms are k-linear maps.

3.1.5. *Example:* $\mathbf{2}^S$. Let S be a set and let $\mathbf{2}^S$ be the category whose objects are subsets of S. Further, $\mathrm{Mor}(X, Y) = \{I_{XY}\}$ (a formal symbol) if $X \subset Y$ and, whenever defined, $I_{YZ} \circ I_{XY} = I_{XZ}$. Note that I_{XX} serves as 1_X in the definition of a category.

3.2. **Categories: initial and final objects.** An **initial** object in a category $\mathbf{C}$ is an object A such that for every object X of $\mathbf{C}$ the set $\mathrm{Mor}(A, X)$ has a single element. A **final** object in a category $\mathbf{C}$ is an object Z such that for every object X of $\mathbf{C}$ the set $\mathrm{Mor}(X, Z)$ has a single element.

Two objects X, Y in a category are called **isomorphic** if there are morphisms $f \in \mathrm{Mor}(X, Y), g \in \mathrm{Mor}(Y, X)$ such that $f \circ g = 1_Y$ and $g \circ f = 1_X$. We denote this by $X \cong Y$. An initial object, if it exists, is unique up to unique isomorphism. The same holds for a final object. To see that, let A and A' be initial objects of a category $\mathbf{C}$. There is a unique morphism $f \in \mathrm{Mor}(A, A')$, because A is initial, and there is a unique morphism $g \in \mathrm{Mor}(A', A)$, because A' is initial. Then $g \circ f \in \mathrm{Mor}(A, A)$. But, since A is initial $\mathrm{Mor}(A, A)$ has a single element and so we must have $g \circ f = 1_A$. Similarly, $f \circ g = 1_{A'}$. This shows that A and A' are isomorphic. Further, since $\mathrm{Mor}(A, A')$ has a single element, this isomorphism is unique.

Example 3.2.1. The category **Sets** has an initial object - the empty set $\emptyset$. Any set of one element is a final object. The category **Gp** has an initial object - the group of one element. This element is also a final object. One calls an object which is both initial and final a zero object. The same holds for **AbGp** and $\mathbf{VSp}_k$. The category $\mathbf{2}^S$ has an initial object $\emptyset$ and a final object S. The category of fields doesn't have initial and final objects. The category of fields of characteristic zero has an initial object $\mathbb{Q}$ but doesn't have a final object. The category of fields of characteristic p, p a prime, has an initial object the field $\mathbb{Z}/p\mathbb{Z}$ but doesn't have a final object.

3.2.1. *The opposite category.* Let $\mathbf{C}$ be a category. Define the **opposite category** $\mathbf{C}^{\mathrm{op}}$ as a category with the same objects and with $\mathrm{Mor}_{C^{\mathrm{op}}}(X,Y) = \mathrm{Mor}_C(Y,X)$. In the category $\mathbf{C}^{\mathrm{op}}$ we define

$$g \circ^{\mathrm{op}} f = f \circ g, \quad g \in \mathrm{Mor}_{C^{\mathrm{op}}}(Y,Z), f \in \mathrm{Mor}_{C^{\mathrm{op}}}(X,Y).$$

This is indeed a category and $(\mathbf{C}^{\mathrm{op}})^{\mathrm{op}} = \mathbf{C}$. One can prove that if A is an initial (final) object of $\mathbf{C}$ then A is a final (reps., initial) object for $\mathbf{C}^{\mathrm{op}}$.

Exercise 3.2.2. Let G be a group. We can define a group G^{op} as the same underlying set but with $x * y = yx$, where $x * y$ denotes the product in G^{op}. Prove that this is a group, which is, in fact, isomorphic to G. At the same time, we can associate to G a category $\underline{G}$. It has a single object, say e and $\mathrm{Mor}(e,e) := G$, where $x \circ y = xy$ (the product in G). Show that there is a natural identification $(\underline{G})^{\mathrm{op}}$ with $\underline{G^{\mathrm{op}}}$.

3.3. **Free groups.** Let X be a set. Consider the category with objects being a function $f : X \to G$ from X into any group G. Morphisms in this category are commutative diagrams

$$\begin{array}{ccc} X & \xrightarrow{f_1} & G_1 \\ \| & & \downarrow g \\ X & \xrightarrow{f_2} & G_2, \end{array}$$

where g is a group homomorphism. A group G is called a **free group** on the set X if it is an initial object in this category. Since initial objects are unique up to unique isomorphism - if they exist at all - a free group is unique up to unique isomorphism (but be careful what morphisms we are talking about!).

Let $f : X \to G$ be a free group. We also say that G has the universal property: given any function $f_1 : X \to G_1$ there is a unique group homomorphism $g : G \to G_1$ such that

$$g(f(x)) = f_1(x), \qquad \forall x \in X.$$

One often uses the language of universal property, but, in fact, in all cases this amounts to saying that some related object is an initial object in an appropriate category. We shall see plenty of examples in the sequel.

Theorem 3.3.1. *Given a set X there is a free group G on X, i.e. an initial object $f : X \to G$.*

Before the proof, we develop some terminology. A **word** ω in the **alphabet** X is a finite string $\omega = \omega_1\omega_2 \dots \omega_n$, where each ω_i is equal to either $x \in X$ or x^{-1} for $x \in X$. Here x^{-1} is a formal symbol. So, for example, if $X = \{x\}$ then words in X are $x, xxx^{-1}x, \emptyset$, etc. If $X = \{x,y\}$ we have as examples $x, y, x^{-1}yyxy, x^{-1}y^{-1}y$, and so on. We say that two words ω, σ are **equivalent** if one can get from one word to the other performing the following basic operations:

Replace $\omega_1 \dots \omega_i x x^{-1} \omega_{i+1} \dots \omega_n$ and $\omega_1 \dots \omega_i x^{-1} x \omega_{i+1} \dots \omega_n$ by $\omega_1 \dots \omega_i \omega_{i+1} \dots \omega_n$, and the opposite of those operations (i.e., inserting xx^{-1} or $x^{-1}x$ at some point in the word).

We denote this equivalence relation by $\omega \sim \sigma$. For example, for $X = \{x,y\}$ we have

$$x \sim xyy^{-1} \sim xyxx^{-1}y^{-1} \sim xyy^{-1}yxx^{-1}y^{-1}.$$

A word is called **reduced** if it doesn't contain a string of the form xx^{-1} or $x^{-1}x$ for some $x \in X$. One can show that every equivalence class contains a unique reduced word and that word is the string of minimal length in the equivalence class. This is not needed for the proof of the present theorem, and we shall come back to this point after proving the Theorem.

Proof. (Theorem 3.3.1) The elements of the group G are equivalence classes

$$[\omega] = \{\sigma | \sigma \sim \omega\}$$

of words in the alphabet X. Multiplication is defined using representatives:

$$[\sigma][\tau] = \sigma\tau$$

(the two words are simply written one after the other). It is easy to see that this is well-defined on equivalence classes: the operations performed on σ to arrive at an equivalent word σ' can be performed on the initial part of $\sigma\tau$ to arrive at $\sigma'\tau$, etc. The identity element is the empty word; we also denote it 1, for convenience. The inverse of $[\omega]$ where $\omega = \omega_1 \dots \omega_n$ is the equivalence class of $\omega_n^{-1} \dots \omega_1^{-1}$ (where we define $(x^{-1})^{-1} = x$ for $x \in X$). Finally, the associative law is clear.

We have constructed a group. The function $f : X \to G$ is just $x \mapsto [x]$, where now x is considered as a word of length 1 in G and we take its equivalence class $[x]$. Given a function $f_2 : X \to G_2$ we define a function

$$g : G \to G_2, \qquad g([\omega]) = f_2(\omega_1) \cdots f_2(\omega_n),$$

where $\omega = \omega_1 \cdots \omega_n$, $\omega = x^{\pm 1}$ where $x \in X$ and by $f_2(x^{-1})$ we mean $(f_2(x))^{-1}$ which is a well defined element of G_2. We leave the verification that g is well-defined as an exercise. It is clear that this is the only possibility and that g is a group homomorphism. □

END of lecture 6 (September 24)

Theorem 3.3.2. *Any word is equivalent to a unique reduced word.*

Proof. We need to show that two reduced words that are equivalent are in fact equal. Let ω and τ be equivalent reduced words. Then, there is a sequence

$$\omega = \sigma_0 \sim \sigma_1 \sim \cdots \sim \sigma_n = \tau,$$

where at each step we either insert, or delete, one couple of the form xx^{-1} or $x^{-1}x$, $x \in X$. Let us look at the lengths of the words. The length function, evaluated along the chain, receives a relative minimum at ω and τ. Suppose it receives another relative minimum first at σ_r (so the length of σ_{r-1} is bigger than that of σ_r and the length of σ_r is smaller than that of σ_{r+1}. We can take σ_r and reduce it be erasing repeatedly pairs of the form xx^{-1}, or $x^{-1}x$, until we cannot do that any more. We get a chain of equivalences $\sigma_r = \alpha_0 \sim \alpha_1 \sim \alpha_s$, where α_s is a reduced word. We now modify our original chain to the following chain

$$\omega = \sigma_0 \sim \sigma_1 \sim \cdots \sim \sigma_r = \alpha_0 \sim \cdots \sim \alpha_{s-1} \sim \alpha_s \sim \alpha_{s-1} \sim \cdots \sim \alpha_0 = \sigma_r \sim \sigma_{r+1} \dots \sigma_n = \tau.$$

A moment reflection shows that by this device, we can reduce the original claim to the following.

Let σ and τ be two reduced words that are equivalent as follows

$$\omega = \sigma_0 \sim \sigma_1 \sim \cdots \sim \sigma_n = \tau$$

where the length increases at every step from σ_0 to σ_a and decreases from σ_a to $\sigma_n = \tau$. Then $\sigma = \tau$.

We view σ and τ as two reduced words obtained by cancellation only from the word σ_a. We argue by induction on the length of σ_a.

If σ_a is reduced, there's nothing to prove because then necessarily $0 = a = n$ and we are considering a tautology. Else, there is a pair of the form dd^{-1} or $d^{-1}d$ in σ_a. We allow ourselves

here $(d^{-1})^{-1} = d$ and then we may that there is a pair dd^{-1} where d or d^{-1} are in X. Let us highlight that pair using a yellow marker and keep track of it. If in the two cancellations processes (one leading to σ, the other to τ) the first step is to delete the highlighted pair, then using induction for the word σ_a with the highlighted pair deleted, we may conclude that $\sigma = \tau$. If in the cancellation process leading to σ at some point the highlighted pair is deleted, then we may change the order of the cancellations so that the highlighted pair is deleted first. Similarly concerning the reduction to τ. And so, in those cases we return to the previous case. Thus, we may assume that in either the reduction to σ, or the reduction to τ, the highlighted pair is not deleted. Say, in the reduction to σ. How then can σ be reduced? The only possibility is that at some point in the reduction process (not necessarily the first point at which it occurs) we arrive at a word of the form $\cdots d^{-1}\boxed{dd^{-1}}\cdots$ or $\cdots\boxed{dd^{-1}}d\cdots$ and then it is reduced to $\cdots \cancel{d}^{-1}\boxed{\cancel{d}d^{-1}}\cdots$ or $\cdots\boxed{d\cancel{d}^{-1}}\cancel{d}\cdots$. But note that the end result is the same as if we strike out the highlighted pair. So we reduce to the previous case. □

Note that as a consequence, if $\omega \in [\omega]$ is a word whose length is the minimum of the lengths of all words in $[\omega]$ then ω is the unique reduced word in the equivalence class $[\omega]$.

Corollary 3.3.3. *Let $f : X \to G$ be a free group on X then f is an injective map.*

Proof. We may assume that G is the group we have constructed. The map $f : X \to G$ is of course just the map

$$f(x) = [x]$$

(the equivalence class of the word x). If $x \neq y$ are in X, the two words x and y are reduced and different, so are not equivalent. □

3.4. **Categories: universal objects.** As we have already discussed above, a **universal object** in a category is an object defined by the fact that it has a universal property and that determines it up to a unique isomorphism. Having a universal property just means being an initial object in a related category, depending on the situation. We discussed that for free groups. Let us give a few more examples.

(1) **Free abelian groups.** Let X be a set. We consider the category of functions $f : X \to A$, where A is an abelian group and morphisms are diagrams

$$\begin{array}{ccc} X & \xrightarrow{f_1} & A_1 \\ \| & & \downarrow g \\ X & \xrightarrow{f_2} & A_2, \end{array}$$

where g is a group homomorphism. Then $f : X \to A$ is a **free abelian group** on X if it is an initial object for this category. We can prove directly that if we take for A the vectors

$$\{(n_x)_{x\in X} : n_x \in \mathbb{Z}, \text{ all but finitely many } n_x = 0\}$$

then this is a free abelian group on X. For example, if $X = \{1, 2, \ldots, n\}$ the group we construct is just $\mathbb{Z}^n$. The function $f : X \to A$ is $y \mapsto \delta(y) = (\delta(y)_x)_{x\in X}$, where

$$\delta(y)_x = \begin{cases} 1 & x = y \\ 0 & \text{otherwise.} \end{cases}$$

It is an exercise to check that this is a free abelian group on X.

(2) Let G be a fixed group. Consider the category whose objects are homomorphisms $f : G \to A$ from G to abelian groups A. The morphisms are commutative diagrams

$$\begin{array}{ccc} G & \xrightarrow{f_1} & A_1 \\ \| & & \downarrow g \\ G & \xrightarrow{f_2} & A_2. \end{array}$$

There is an initial object in this category. It is the object

$$\pi : G \to G/G',$$

where G' is the commutator subgroup of G and π the canonical map. The quotient G/G' is called the **abelianization** of G and denoted also G^{ab}.

3.5. **Free groups: further properties.**

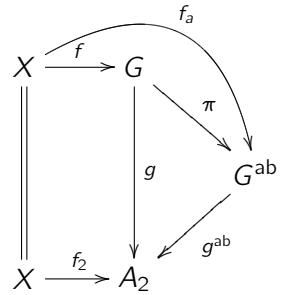
Lemma 3.5.1. *Let X be a set and G a free group on X, $f : X \to G$. Let $A = G^{\mathrm{ab}}$ and consider the composition $f_a : X \to G \to A$, where $G \to A$ is the canonical map. Then $f_a : X \to A$ is a free abelian group.*

Note this gives an alternative construction of a free abelian group.

Proof. We show $f_a : X \to A$ is an initial object in the respective category. Let $f_2 : X \to A_2$ be a function into an abelian group A_2. Then, since $f : X \to G$ is universal for groups and A_2 is a group, there is a unique homomorphism $g : G \to A_2$ making the diagram commutative:

$$\begin{array}{ccc} X & \xrightarrow{f} & G \\ \| & & \downarrow g \\ X & \xrightarrow{f_2} & A_2. \end{array}$$

Since A_2 is abelian, we have unique factorization



It remains to show that any homomorphism $h : G^{\mathrm{ab}} \to A_2$ such that $h \circ f_a = f_2$ is necessarily g^{rmab}. But this too follows from the universal property of G, because $(h \circ \pi) : G \to A_2$ is a homomorphism such that $(h \circ \pi) \circ f = f_2$ and so $(h \circ \pi) = g$ and that implies $h = g^{\mathrm{ab}}$. □

Corollary 3.5.2. *Let $f : X \to G$ and $g : Y \to H$ be free groups on X and Y, respectively. Then $G \cong H$ if and only if $|X| = |Y|$.*

Proof. If $|X| = |Y|$ then it is easy to see that $G \cong H$, for example from the explicit construction. Conversely, suppose that $G \cong H$ the also $G^{\mathrm{ab}} \cong H^{\mathrm{ab}}$; say $h : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is an isomorphism. Consider the subgroups $2G^{\mathrm{ab}}, 2H^{\mathrm{ab}}$. That is $2G^{\mathrm{ab}} = \{g + g : g \in G^{\mathrm{ab}}\}$. Then h induces an isomorphism $2G^{\mathrm{ab}} \cong 2H^{\mathrm{ab}}$ and $G^{\mathrm{ab}}/2G^{\mathrm{ab}} \cong H^{\mathrm{ab}}/2H^{\mathrm{ab}}$. Using the specific model for a free abelian group we have constructed above, we see that $G^{\mathrm{ab}}/2G^{\mathrm{ab}}$ is isomorphic to a vector space over $\mathbb{Z}/2\mathbb{Z}$ of dimension $|X|$

(for example, $\{\delta(x) : x \in X\}$ form a basis). Similarly for $H^{ab}/2H^{ab}$. Using that two vector spaces over a field k are isomorphic if and only if they have the same dimension, conclude $|X| = |Y|$. $\square$

3.5.1. *Generators and relations.* Let X be a set. Denote by $F(X)$ "the" free group on X. Let $R = \{r_\alpha\}$ a collection of words in the alphabet X. We define the group G generated by X, subject to the **relations** R as follows. Let N be the minimal normal subgroup of $F(X)$ containing $[r]$ for all $r \in R$. Define G as $F(X)/R$. Note that in G any word r becomes trivial. Note also that G is a universal object for this property. Namely, it is an initial object for the category whose objects are $f : X \to H$, H a group, f a function such that $f(r) = 1_H$ for all $r \in R$, where if $r = \omega_1 \dots \omega_n$, $\omega_i = x^{\pm 1}$ for $x \in X$, then $f(r) := f(\omega_1) \cdots f(\omega_n)$ (with $f(x^{-1}) := f(x)^{-1}$). We denote G also by

$$\langle X|R\rangle.$$

A **presentation** of a group H is an isomorphism

$$H \cong \langle X|R\rangle$$

for some X and R. A group can have many presentations. There is always the tautological presentation. Take $X = \{\underline{g} : g \in G\}$, so that we can distinguish between g as an element of the group G and $\underline{g}$ an element of X, and take

$$R = \{r = \underline{\omega_1} \dots \underline{\omega_n} : \text{in the group } G \text{ we have that the product } \omega_1 \cdots \omega_n = 1_G\}.$$

But usually there are more interesting, and certainly more economical presentations.

(1) Let $F(X)'$ be the commutator subgroup of $F(X)$ then $\langle X : F(X)'\rangle$ is a presentation of the free abelian group on X. But, for example, for $X = \{x, y\}$, we have the more economical presentation
$$\langle \{x, y\} : xyx^{-1}y^{-1}\rangle.$$
Lets prove it. First, from the universal property, since in $\mathbb{Z}^2$ all commutators are trivial, there is a unique homomorpism
$$\langle \{x, y\} : xyx^{-1}y^{-1}\rangle \ \to \ \mathbb{Z}^2, \qquad x \mapsto (1, 0), y \mapsto (0, 1).$$
Clearly this is a surjective homomorphism. Define now a homomorphism
$$\mathbb{Z}^2 \to \langle \{x, y\} : xyx^{-1}y^{-1}\rangle, \qquad f(m, n) = x^m y^n.$$
We need to show that f is a homomorphism. Namely, that in the group $\langle \{x, y\} : xyx^{-1}y^{-1}\rangle$ we have
$$x^a y^b x^c y^d = x^{a+c} y^{b+d}.$$
It's enough to show that $xy = yx$ because then we may pass the powers of x through those of y one at the time. But we have the equality $yx = (xyx^{-1}y^{-1})(yx) = xy$. It is easy to check that f is an inverse to the previous homomorphism.

(2) S_n is generated by the permutations (12) and $(12 \cdots n)$ and so it follows that it has a presentation $\langle \{x, y\} : R\rangle$ for some set of relations R; for example, R could be the kernel of the surjective homomorphism $F(\{x, y\}) \to S_n$ that takes x to (12) and y to $(12 \cdots n)$. As such, R is an infinite set. But, can we replace R be a finite list of relations. The answer is yes. It follows from the following two theorems, that we will not prove in the course, one reason being that the best proofs use the theory of covering spaces and fundamental groups that we do not assume as prerequisites.

Theorem 3.5.3. *(Nielsen-Schreier) A subgroup of a free group is free.*

Theorem 3.5.4. *Let F be a free group of rank r and let H be a subgroup of F of finite index h. The H is free of rank $h(r - 1) + 1$.*

It follows that we can determine all the relations in S_n as a consequence of certain $n!+1$ relations. However, this is far from optimal. For example, S_3 has the presentation

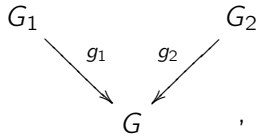
$$\langle \{x, y\} : x^2, y^3, xyxy \rangle$$

The explanation for this particular saving is that we take the minimal *normal* subgroup generated by the relations and not the minimal subgroup generated by the relations. In this example, the minimal normal subgroup has rank $7 = 3! + 1$, while the minimal subgroup has rank at most 3. We leave it as an exercise to prove that this is indeed a presentation for S_3 and to find a similar presentation for S_4.

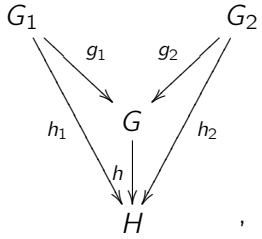
(3) After experimenting a little with examples, one easily concludes that it is in general difficult to decide whether a finitely presented group is isomorphic to a given one. In fact, a theorem (which is essentially "the word problem" for groups) says that there is no algorithm that given a finite presentation $\langle X|R\rangle$, X and R finite, will decide in finite time (that is independent of the presentation) whether this is a presentation of the finite group or not.

End of lecture 7 (October 1)

3.6. **Free products.** Let G_1, G_2 be groups. The **free product** of G_1 and G_2, denoted $G_1 * G_2$ is the initial object in the following category: the objects are diagrams



where G is a group and the g_i group homomorphisms. A morphism in this category is



where h is a homomorphism making the diagram commutative. By taking $H = G_1$, h_1 the identity homomorphism and h_2 the trivial homomorphism. We see that $G_1 * G_2$ contains G_1, and also G_2. Thus, in a sense, it is the minimal group containing G_1 and G_2 such that no further relationship between the images is assumed. The problem is to show it exists.

Let $\langle X_i|R_i\rangle$ be a presentation of G_i and, without loss of generality, $X_1 \cap X_2 = \emptyset$. We claim that

$$\langle X_1 \cup X_2 | R_1 \cup R_2 \rangle$$

is the free product $G_1 * G_2$. The proof is straightforward and is left as an exercise. Note, for example, the following examples:

(1) For disjoint sets X_1, X_2 we have $F(X_1) * F(X_2) \cong F(X_1 \cup X_2)$.
(2) $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ is an infinite group (exercise; for example, find a suitable homomorphism into a group of 2×2 matrices).

3.7. **Category theory: functors and adjoint functors.** We take this opportunity to discuss some key concepts in category theory and illustrate them using some of the material developed above. The first notion is a notion of a **functor**. There are two variants - the **covariant** and the **contravariant** functors. Both arise when one wants to define a notion of a morphism between categories. Let

$\mathbf{C}, \mathbf{D}$ be categories. What should a morphism $F : \mathbf{C} \to \mathbf{D}$ be? In some sense it should transform the category $\mathbf{C}$ into part of the category $\mathbf{D}$. Thus, it is natural to require:

(1) For every object c of $\mathbf{C}$ there is given an object $F(c)$ of $\mathbf{D}$.

Equally important is that morphisms should be transformed. F is called a covariant functor if

(2) For a morphism $f \in \mathrm{Mor}_{\mathsf{C}}(c, d)$ there is a morphism $F(f) \in \mathrm{Mor}(F(c), F(d))$. This respects composition, $F(f \circ g) = F(f) \circ F(g)$, and $F(1_c) = 1_{F(c)}$.

F is called a contravariant functor if

(2) For a morphism $f \in \mathrm{Mor}_{\mathsf{C}}(c, d)$ there is a morphism $F(f) \in \mathrm{Mor}(F(d), F(c))$. This respects composition, $F(f \circ g) = F(g) \circ F(g)$, and $F(1_c) = 1_{F(c)}$.

3.7.1. *Examples of functors.*

1. *The forgetful functor.* Let $\mathbf{C}$ be a category whose objects are, in particular, sets and whose morphisms are, in particular, functions between sets. For example, $\mathbf{C}$ could be the category of groups, the category of abelian groups, the category of topological spaces, the category of vector spaces over a field k. The **forgetful functor**

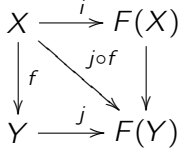
$$\Phi : \mathbf{C} \to \mathbf{Sets},$$

is the functor sending each object of $\mathbf{C}$ to its underlying set and the morphisms of $\mathbf{C}$ are viewed as functions. This is a covariant functor.

A covariant functor $F : \mathbf{C} \to \mathbf{D}$ is called **full** if for every objects c, d of $\mathbf{C}$ and any morphism $g \in \mathrm{Mor}_{\mathsf{D}}(F(c), F(d))$, there is a morphism $f \in \mathrm{Mor}_{\mathsf{C}}(c, d)$ such that $F(f) = g$. Otherwise said, $\mathrm{Mor}_{\mathsf{C}}(c, d) \to \mathrm{Mor}_{\mathsf{D}}(F(c), F(d))$ is surjective. Typically Φ is not full, because typically in categories morphisms are functions with additional properties. For example, $\Phi : \mathbf{Gps} \to \mathbf{Sets}$ is not full. Take $c = d$ to be the group $\mathbb{Z}/n\mathbb{Z}$. Then $\mathrm{Mor}_{\mathsf{Sets}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is a set of cardinality n^n, while $\mathrm{Mor}_{\mathsf{Gps}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is a set of n elements. A similar definition is made for contravariant functors.

A covariant functor $F : \mathbf{C} \to \mathbf{D}$ is called **faithful** if $\mathrm{Mor}_{\mathsf{C}}(c, d) \to \mathrm{Mor}_{\mathsf{D}}(F(c), F(d))$ is injective. Usually $\Phi : \mathbf{C} \to \mathbf{Sets}$ is faithful, because very often morphisms are determined by the map they induce on the underlying sets. This holds for groups, abelian groups, topological spaces and k-vector spaces, for instance. A similar definition is made for contravariant functors. Finally, a morphism is **fully faithful** if it is both full and faithful. That is, for any two objects in $\mathbf{c}$, the map $\mathrm{Mor}_{\mathsf{C}}(c, d) \to \mathrm{Mor}_{\mathsf{D}}(F(c), F(d))$ is bijective ($\mathrm{Mor}_{\mathsf{C}}(c, d) \to \mathrm{Mor}_{\mathsf{D}}(F(d), F(c))$, for contravariant functors). An example of a fully faithful functor are subcategories. For example, the functor $\mathbf{AbGps} \to \mathbf{Gps}$ is fully faithful. For another example, let $k = \mathbb{Z}/p\mathbb{Z}$, p prime. The functor from the category of k-vector spaces to the category of abelian groups is fully-faithfull.

2. *Free construction.* Let X be a set and $F(X)$ the free group on X. Any function $f : X \to Y$ between sets induces a homomorhism $F(f) : F(X) \to F(Y)$. This is evident from our construction of free groups. Another way to see that is that we have a diagram



The homomorphism $F(X) \to F(Y)$, denoted $F(f)$, exists by the universal property of $F(X)$. In fact, it not hard to show that

$$X \mapsto F(X), \quad f \mapsto F(f),$$

gives a functor

$$F : \mathbf{Sets} \to \mathbf{Gps}.$$

This is the **free construction functor**. There are many variants of this functor, as the category of groups is replaced by other categories (modules, for example) and one uses the same terminology.

3.7.2. *Adjoint functors.* A pair of covariant functors (F, G)

$$F : \mathbf{C} \to \mathbf{D}, \qquad G : \mathbf{D} \to \mathbf{C},$$

are called an **adjoint pair** if one is given a bijection

$$\alpha_{c,d} : \mathrm{Mor}_{\mathsf{D}}(F(c), d) \to \mathrm{Mor}_{\mathsf{C}}(c, G(d))$$

for every pair of objects c of $\mathbf{C}$ and d of $\mathbf{D}$, such that for any morphism $f : c \to c_1$ the diagram

$$\begin{array}{ccc} \mathrm{Mor}_{\mathsf{D}}(F(c), d) & \xrightarrow{\alpha_{c,d}} & \mathrm{Mor}_{\mathsf{C}}(c, G(d)) \\ {\scriptstyle (\,)\circ F(f)}\uparrow & & \uparrow{\scriptstyle (\,)\circ f} \\ \mathrm{Mor}_{\mathsf{D}}(F(c_1), d) & \xrightarrow{\alpha_{c_1,d}} & \mathrm{Mor}_{\mathsf{C}}(c_1, G(d)) \end{array}$$

is commutative, and for every morphism $f : d \to d_1$ the diagram

$$\begin{array}{ccc} \mathrm{Mor}_{\mathsf{D}}(F(c), d) & \xrightarrow{\alpha_{c,d}} & \mathrm{Mor}_{\mathsf{C}}(c, G(d)) \\ \downarrow{\scriptstyle f\circ(\,)} & & \downarrow{\scriptstyle G(f)\circ(\,)} \\ \mathrm{Mor}_{\mathsf{D}}(F(c), d_1) & \xrightarrow{\alpha_{c,d_1}} & \mathrm{Mor}_{\mathsf{C}}(c, G(d_1)) \end{array}$$

is commutative as well. One says that F is **left-adjoint** to G and G is **right-adjoint** to F. A similar definition is made for contravariant functors.

Here are some examples.

(1) Let $\Phi : \mathbf{Gps} \to \mathbf{Sets}$ be the forgetful functor and let $F : \mathbf{Sets} \to \mathbf{Gps}$ be the free construction functor. Then the pair (F, Φ) is an adjoint pair. Namely, there are natural bijections

$$\mathrm{Mor}_{\mathsf{Gps}}(F(X), G) \cong \mathrm{Mor}_{\mathsf{Sets}}(X, \Phi(G)).$$

We leave it as an exercise to supply the details.

(2) In a similar vein one constructs a free construction functor

$$G : \mathbf{Sets} \to \mathbf{AbGps}.$$

The pair (G, Φ) is an adjoint pair.

(3) Let $\mathbf{Top}$ be the category of topological spaces. Let $\Phi : \mathbf{Top} \to \mathbf{Sets}$ be the forgetful functor and define two functors $G_1, G_2 : \mathbf{Sets} \to \mathbf{Top}$. The first gives a set X the trivial topology whose open sets are only $\emptyset$ and X. The second gives a set X the discrete topology - every subset of X is open. Then each of the G_i forms an adjoint pair with Φ, but one is left-adjoint to Φ and the other is right-adjoint. We leave it as an exercise to check that G_i are functors and to find which is the left-adjoint and which is the right-adjoint.

4. Modules

4.1. **Recall.** Let R be a ring. For us, rings are always associative, with 1, and a ring homomorphism must take 1 to 1. A module R over a ring R is an abelian group M together with a function

$$R \times M \to M, \quad (r, m) \mapsto r * m$$

(although often we just write rm) such that the following holds for all $r_1, r_2 \in R, m, m' \in M$:

(1) $r_1 * (r_2 * m) = (r_1 r_2) * m$.
(2) $(r_1 + r_2) * m = r_1 * m + r_2 * m$.
(3) $1_R * m = m$
(4) $r_1 * (m + m') = r_1 * m + r_1 * m'$.

Otherwise said, since M is an abelian group $\mathrm{End}(M)$ is a ring under addition and composition of functions and to say that M is a module over R is the same thing as to give a homomorphism of rings $R \to \mathrm{End}(M)$. (Given an action define a homomorphism by $r \mapsto f_r$ where $f_r(m) := r * m$, etc.)

The notions of a submodule, a module homomorphism, quotient module, direct sum and product of modules and isomorphism are entirely as expected. The analogues of the 4 isomorphism theorems for groups hold for modules. An R-module M is called finitely generated if there is a finite set $m_1, \ldots, m_n$ of elements of M such that $M = Rm_1 + \cdots + Rm_n$. Equivalently, if there is a surjective R-module homomorphism $R^n \to M$.

For a module M we definite $\mathrm{Tor}(M)$ to be the **torsion** elements of M,

$$\mathrm{Tor}(M) = \{m \in M : \exists r \in R, r \neq 0, rm = 0\}.$$

If R is an integral domain then this is a submodule of M. It consists, in fact, of all finite sums $i_1 m_1 + \cdots + i_1 m_a$, where $i_j \in I, m_j \in M$.

If I is a left ideal of R and M is an R-module then IM denotes the submodule generated by the elements $\{im : i \in I, m \in M\}$.

4.2. **Localization of rings and modules.** Let R be a commutative ring and $S \subseteq R$ a subset. S is called **multiplicative** if:

(1) $1 \in S$, and
(2) $x, y \in S \Rightarrow xy \in S$.

Example 4.2.1. Here are some key examples of multiplicative sets.

(1) Let $f \in R$. Then $S = \{1, f, f^2, f^3, \ldots\}$ is a multiplicative set.
(2) Let $\mathfrak{p} \lhd R$ be a prime ideal. Then $S = R - \mathfrak{p}$ is a multiplicative set.
(3) Suppose that R is an integral domain. Then $S = R - \{0\}$ is a multiplicative set.

End of lecture 8 (October 3)

Our goal is to construct a ring $R[S^{-1}]$ with a ring homomorphism $R \to R[S^{-1}]$ (that will satisfy a universal property) and to construct a functor ${}_R\mathbf{Mod} \to {}_{R[S^{-1}]}\mathbf{Mod}$.

Let M be an R-module and $S \subseteq R$ a multiplicative set. Consider formal fractions $\frac{m}{s}$, where $m \in M$ and $s \in S$. Define a relation by

$$\frac{m_1}{s_1} \sim \frac{m_2}{s_2} \quad \text{if for some } s \in S, s(s_2 m_1 - s_1 m_2) = 0.$$

It is not hard to verify that this is an equivalence relation. We denote the equivalence classes by $M[S^{-1}]$ and call it the **localization** of M by S. Abuse notation and write $\frac{m}{s}$ also for the equivalence

class of $\frac{m}{s}$. Define addition by

$$\frac{m_1}{s_1}+\frac{m_2}{s_2}=\frac{s_2m_1+s_1m_2}{s_1s_2}.$$

One checks that this is well-defined and provides $M[S^{-1}]$ with a structure of an abelian group. The zero element is the equivalence class of $\frac{0}{1}$. In the particular case $M=R$ we also define multiplication by

$$\frac{m_1}{s_2}\cdot\frac{m_2}{s_2}=\frac{m_1m_2}{s_1s_2}.$$

And one checks that this gives $R[S^{-1}]$ a commutative ring structure. The identity element is the equivalence class of $\frac{1}{1}$. Further $M[S^{-1}]$ become an $R[S^{-1}]$-module where we define

$$\frac{r_1}{s_1}\cdot\frac{m}{s}=\frac{r_1m}{s_1s},\qquad \frac{r_1}{s_1}\in R[S^{-1}],\frac{m}{s}\in M[S^{-1}].$$

4.2.1. *On localization of rings.* There is a natural ring homomorphism

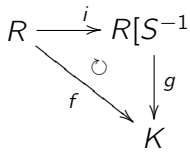
$$i:R\to R[S^{-1}],\qquad r\mapsto\frac{r}{1}.$$

One should be careful that this is not an injection in general. Indeed the kernel of i is the elements r such that $\frac{r}{1}\sim\frac{0}{1}$. That is,

$$\mathrm{Ker}(i)=\{r\in R:\exists s\in S,sr=0\}.$$

And so, in general there could be a kernel, but if R is an integral domain and $0\notin S$ then i is injective. The ring $R[S^{-1}]$ has the property that all the elements $\frac{s}{1}$ are invertible in it. In fact, this is the universal property that characterizes it.

Proposition 4.2.2. *Let K be a commutative ring and let $f:R\to K$ be a ring homomorphism such that $f(s)$ is invertible in K for all $s\in S$. Then there exists a unique ring homomorphism $g:R[S^{-1}]\to K$ such that the following diagram is commutative:*



Proof. The definion of g is straight-forward. Define

$$g(\frac{r}{s})=f(r)f(s)^{-1}.$$

First, $f(s)$ is invertible in K so the formula makes sense. Next, g is well-defined. Suppose that $\frac{r}{s}\sim\frac{r_1}{s_1}$ so for some $s_2\in S$ we have $s_2(s_1r-sr_1)=0$. Thus, $f(s_2)(f(s_1)f(r)-f(s)f(r_1))=0$. Since $f(s_2)$ is invertible, we conclude that $f(s_1)f(r)-f(s)f(r_1)=0$ and so $f(r)f(s)^{-1}=f(r_1)f(s_1)^{-1}$. The verification that g is a ring homomorphism and that $g\circ i=f$ is automatic. □

4.2.2. *The field of fractions.* Let R be an integral domain and $S=R-\{0\}$, which is a multiplicative set. The localization $R[S^{-1}]$ is a commutative ring which is in fact a field. First, $R\hookrightarrow R[S^{-1}]$ as follows from our calculation of the kernel in general and using that R is an integral domain. So, in particular, $0\neq 1$ in $R[S^{-1}]$. Finally, if $r/s\in R[S^{-1}]$ is a non-zero element then $r\in S$ and $(s/r)\cdot(r/s)=1/1$ is the unit element of $R[S^{-1}]$. Thus, every non-zero element is invertible and so $R[S^{-1}]$ is a field. By the universal property, it is the minimal field into which R embeds. We denote this localization by $\mathrm{Frac}(R)$, or $\mathrm{Quot}(R)$ and refer to it as the **field of fractions** of R.

For example, it is quite visible that $\mathrm{Frac}(\mathbb{Z})=\mathbb{Q}$ and, for a field k, $\mathrm{Frac}(k[x])=k(x)$.

4.2.3. *On localization of modules.* The next point we want to make is that in fact $M \to M[S^{-1}]$ can be made into a functor

$$_R\mathbf{Mod} \to {}_{R[S^{-1}]}\mathbf{Mod}.$$

Given an R-module homomorphism $f : M_1 \to M_2$ define a map

$$f[S^{-1}] : M_1[S^{-1}] \to M_2[S^{-1}], \qquad \frac{m}{s} \mapsto \frac{f(m)}{s}.$$

The verification that this is a well-defined homomorphism of $R[S^{-1}]$-modules is straightforward and would not be done here. Let us also remark that the localization of the zero module of R is the zero module of $R[S^{-1}]$ and both are denoted 0.

Theorem 4.2.3. *The localization functor is* **exact**. *That is, if*

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

is an exact sequence of R-modules and S is a multiplicative set in R, then the sequence

$$0 \longrightarrow M_1[S^{-1}] \xrightarrow{f[S^{-1}]} M_2[S^{-1}] \xrightarrow{g[S^{-1}]} M_3[S^{-1}] \longrightarrow 0$$

is an exact sequence of $R[S^{-1}]$-modules.

Proof. To simplify notation and write f for $f[S^{-1}]$, etc. Let $m_1/s \in M_1$ such that $f(m_1/s) = f(m_1)/s = 0$. Then, for some $s' \in S$ we have $s'f(m_1) = 0$. But, $s'f(m_1) = f(s'm_1) = 0$. Since f is injective $s'm_1 = 0$ and so $m_1/s = 0$.

Since $g(f(m_1/s)) = g(f(m_1))/s = 0/s = 0$, $\mathrm{Ker}(g) \supseteq \mathrm{Im}(f)$. Let $m_2/s \in \mathrm{Ker}(g)$. Then, for some $s' \in S$ we have $s'g(m_2) = 0$. That is, $g(s'm_2) = 0$. Let $m_1 \in M_1$ be such that $f(m_1) = s'm_2$. Then, $f(m_1/ss') = m_2/s$ and so $\mathrm{Im}(f) \supseteq \mathrm{Ker}(g)$.

Finally, given $m_3/s \in M_3[S^{-1}]$ choose $m_2 \in M_2$ such that $g(m_2) = m_3$. Then $g(m_2/s) = m_3/s$ and so $g : M_2[S^{-1}] \to M_3[S^{-1}]$ is surjective. □

4.2.4. *Ideals under localization.*

Theorem 4.2.4. *Let S be a multiplicative set in R and let $f : R \to R[S^{-1}]$ be the canonical homomorphism of rings.*

1. *Let $J \lhd R[S^{-1}]$ be an ideal and let $J^c := f^{-1}(I)$. Then J^c is an ideal of R. If J is prime then J^c is prime.*
2. *Let I be an ideal of R. Then $I[S^{-1}]$ can be identified with $f(I)R[S^{-1}]$ and is an ideal of $R[S^{-1}]$, denoted I^e. If I is prime and $I \cap S = \emptyset$ then I^e is prime.*
3. *Let J be an ideal of $R[S^{-1}]$. Then $J^{ce} = J$.*
4. *Let I be a prime ideal of R such that $I \cap S = \emptyset$ then $I^{ec} = I$.*
5. *The functions $I \mapsto I^e$, $I \lhd R$, $J \mapsto J^c$, $J \lhd R[S^{-1}]$, give a bijection between prime ideals of R that are disjoint from S and prime ideals of $R[S^{-1}]$.*
6. *Let $\mathfrak{p}$ be a prime ideal of R and $S = R - \mathfrak{p}$. The ring $R[S^{-1}]$, which is denoted in this case $R_{\mathfrak{p}}$, is a local ring with a maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.*

Proof. To prove (1) we first recall that the pre-image of an ideal J under a ring homomorphism $f : R \to T$ is always an ideal. Since $R/f^{-1}(J) \hookrightarrow T/J$ and the latter is an integral domain, also $R/f^{-1}(J)$ is an integral domain. That is, $f^{-1}(J)$ is a prime ideal of R.

The exact sequence of R modules, $0 \to I \to R$, gives an exact sequence of $R[S^{-1}]$-modules,

$$0 \to I[S^{-1}] \to R[S^{-1}].$$

That is, $I[S^{-1}]$ can be viewed as a submodule of $R[S^{-1}]$, that is to say, an ideal. It is clear from the definitions that $I[S^{-1}]$ is the ideal generated by $f(I)$ in $R[S^{-1}]$. Thus, (2) follows (we check that I^e is prime below).

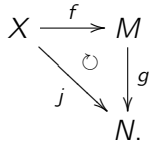
To show (3) we first note that from the definitions $J^{ce} \subseteq J$. Let $j/s \in J$. Then also $j/1 = s/1 \cdot j/s \in J$ and so $j \in J^c$ and hence $j/1 \in J^{ce}$. Thus, also $1/s \cdot j/1 = j/s \in J^{ce}$ and we have proven $J \subseteq J^{ce}$.

We now prove (4). Let $I \lhd R$ be a prime ideal disjoint from S. Then $I^e = \{i/e : i \in I\}$ and so I^{ec} are the elements $t \in R$ such that $t/1 = i/s$ for some $i \in I, s \in S$. Equivalently, the elements t such that for some $s' \in S$, $s'st = s'i$. We see that if $t \in I$ this is always satisfied (take $s = s' = 1$). Conversely, for such t, we have $(s's)t \in I$. Since S is multiplicative $s's \in S$. Since I is prime, either $s's \in I$ or $t \in I$. But, $S \cap I = \emptyset$ and so $t \in I$. We also check that I^e is prime. Suppose that $r_1/s_1 \cdot r_2/s_2 \in I^e$. Thus, for some $i \in I$ and $s \in S$, $(r_1r_2)/(s_1s_2) = i/s$. So, for some $s_3 \in S$ we have equality $s_3sr_1r_2 = s_3s_1s_2i \in I$. Once more, using that I is prime and $s_3s \in S, S \cap I = \emptyset$, we find that either r_1 or r_2 belong to I. Then, either $r_1/s_1 = 1/s_1 \cdot r_1/1$, or $r_2/s_2 = 1/s_2 \cdot r_2/1$ belong to I^e, and we are done.

Part (5) is a direct consequence of the results we have just proven. For (6), note that the set of prime ideals $I \lhd R$ that are disjoint from S has a maximal ideal, i.e., $\mathfrak{p}$. Since $I \mapsto I^e$ preserves inclusion, we conclude that $R_{\mathfrak{p}}$ has a unique maximal ideal, which is $\mathfrak{p}R_{\mathfrak{p}}$. □

End of lecture 9 (October 10)

4.3. **Free modules and rank.** Let R be a ring. We may as well assume R is not the zero ring (equivalently, $0 \neq 1$ in R) because every module over the zero ring is the zero module and there is nothing of interest there. Let X be a set. A **free module on** X is an R-module M together with a function $f : X \to M$ that has the following universal property. For every R-module N and a function $j : X \to N$ there is a unique R-module homomorphism $g : M \to N$ such that the following diagram commutes:



At this point, it should not be hard to prove that M exists, for example by defining M as the module of all vectors

$$\{(r_x)_{x\in X} : r_x \in R, r_x = 0 \text{ for all but finitely many } x\}.$$

(The operations are of course $(r_x)_{x\in X} + (r'_x)_{x\in X} = (r_x + r'_x)_{x\in X}$ and $r \cdot (r_x)_{x\in X} = (rr_x)_{x\in X}$.) The map $f : X \to M$ takes $t \in X$ to the vector e_t all whose coordinates are zero, except for the t coordinate which is 1. This module is also denoted $\oplus_{x\in X} R$

If we let $\Phi : {}_R\mathbf{Mod} \to \mathbf{Sets}$ be the forgetful functor from the category of left R-modules to the category of sets and we let $F : \mathbf{Sets} \to {}_R\mathbf{Mod}$ be the free-construction functor associating to a set X the free module on X, then (F, Φ) is an adjoint pair.

Lemma 4.3.1. *A module M is isomorphic to a free module on a set X if and only if there are elements $\{m_x : x \in X\}$ of M such that every element in M can be written as a unique linear combination of the elements $\{m_x\}$. Namely, given $m \in M$ there are unique elements $r_x \in R$, all but finitely many of which are zero, such that $m = \sum_{x\in X} r_x m_x$. We shall also say that M* **is free on the elements** *$\{m_x : x \in X\}$.*

Proof. Indeed, if $f: X \to M$ is a free module then $M \cong \oplus_{x\in X} R$ and the set $\{m_x : x \in X\}$ can be taken to be the set $\{e_x : x \in X\}$ appearing above. Conversely, given such a set of elements, we find that the map

$$\oplus_{x\in X} R \to M, \qquad (r_x)_{x\in X} \mapsto \sum_{x\in X} r_x \cdot m_x,$$

is an isomorphism. □

Assume henceforth that R be a commutative ring.

Lemma 4.3.2. *Let X, Y be sets and M, N free modules on X, Y. Then $M \cong N$ (as an R-module) if and only if $|X| \cong |Y|$ (as sets).*

Proof. We may assume $M = \oplus_{x\in X} R$ and $N = \oplus_{y\in Y} R$. Clearly a bijection $\varphi: X \to Y$ induces an isomorphism $M \cong N$ by $(r_x)_{x\in X} \mapsto (c_y)_{y\in Y}$, where $c_y = r_{\varphi^{-1}(y)}$. Conversely, if $M \cong N$, choose a maximal ideal $\mathfrak{p}$ of R, which exists by Zorn's lemma. Let $k = R/\mathfrak{p}$, which is a field. Since $M \cong N$, $\mathfrak{p}M \cong \mathfrak{p}N$ and so $M/\mathfrak{p}M \cong N/\mathfrak{p}N$. But $M/\mathfrak{p}M$ is a module over $R/\mathfrak{p}$; that is, a k-vector space and it is easy to see that $\{e_x : x \in X\}$ is a basis. Similarly $\{e_y : y \in Y\}$ is a basis for $N/\mathfrak{p}N$. Thus, $|X| = |Y|$. □

In general, a subset $\{m_\alpha : \alpha \in A\}$ of a module M is called **linearly independent** if a finite linear combination $\sum r_\alpha m_\alpha = 0$ ($r_\alpha \in R$, all but finitely many are zero) implies all $r_\alpha = 0$. It is a **spanning set** or a **generating set** if every element of M is of the form $\sum r_\alpha m_\alpha$ for some $r_\alpha \in R$, all but finitely many are zero. It is a **basis** if every element of M is of the form $\sum r_\alpha m_\alpha$ for unique $r_\alpha \in R$, all but finitely many are zero. A set is a basis if and only if it is spanning and linearly independent. But, unlike in the situation of vector spaces (that is, modules over a field) a maximal independent set is not necessarily a basis. For example, for $R = \mathbb{Z} = M$, the set $\{2\}$ is maximal independent but is not a basis. We define the **rank** of a module M to be the maximal cardinality of a linearly independent subset of M.

From this point on we assume R is an integral domain

Proposition 4.3.3. *Let M be a free module on $\{m_\alpha : \alpha \in A\}$. Then the rank of M is $|A|$. In particular, the rank of R^n is n.*

Proof. Let $F = \mathrm{Frac}(R)$ be the quotient field. We have $M = \oplus_{\alpha\in A} R \subseteq \oplus_{\alpha\in A} F$, a vector space of dimension $|A|$. The set $\{e_\alpha : \alpha \in A\}$ clearly becomes a basis of $\oplus_{\alpha\in A} F$. If $\{n_\beta : \beta \in B\}$ is any other linearly independent set in M then viewed in $\oplus_{\alpha\in A} F$ it is still linearly independent. Indeed, given a finite linear combination $\sum_{i=1}^n \frac{r_i}{s_i}\frac{m_{\alpha_i}}{1} = 0$, by passing to a common denominator $s = s_1 \cdots s_n$ and $r_i' = \frac{s_1 \cdots \hat{s_i} \cdots s_n r_i}{s}$ we get $\sum_{i=1}^n \frac{r_i'}{s}\frac{m_{\alpha_i}}{1} = 0$. Therefore, $\sum_{i=1}^n r_i' \cdot m_{\alpha_i} = 0$ and, since $\{m_\alpha\}$ is independent, all $r_i' = 0$ and also all $r_i = 0$. Therefore $|B| \leq |A|$. □

The proof suggests that a stronger statement is true:

Proposition 4.3.4. *Let R be an integral domain and let $S = R - \{0\}$. M is of rank α if and only if $M[S^{-1}]$ has dimension α over $F = \mathrm{Frac}(R)$.*

Proof. As above (but without needing to assume M is free), let $\{n_\beta : \beta \in B\}$ be a linearly independent set in M then $\{\frac{n_\beta}{1} : \beta \in B\}$ viewed in $M[S^{-1}]$ is still linearly independent. Indeed, give a finite linear combination $\sum_{i=1}^n \frac{r_i}{s_i} \cdot \frac{m_{\alpha_i}}{1} = 0$, by passing to a common denominator $s = s_1 \cdots s_n$ and $r_i' = \frac{s_1 \cdots \hat{s_i} \cdots s_n r_i}{s}$ we get $\sum_{i=1}^n \frac{r_i'}{s}\frac{m_{\alpha_i}}{1} = 0$. Therefore, $\sum_{i=1}^n \frac{r_i'}{s} \cdot m_{\alpha_i} =$ and, since $\{m_\alpha\}$ is independent, all $r_i' = 0$ and also all $r_i = 0$.

Now, suppose that $\{n_\beta : \beta \in B\}$ is a maximal linearly independent set in M. Let $\frac{m}{s} \in M[S^{-1}]$. The set $\{m\} \cup \{n_\beta : \beta \in B\}$ is a subset of M that must be linearly dependent and a non-trivial linear dependence involving m must exist, say, $rm + \sum_{i=1}^n r_i m_{\alpha_i} = 0$. Then also $\frac{r}{1}\frac{m}{s} + \sum_{i=1}^n \frac{r_i}{s}\frac{m_{\alpha_i}}{1} = 0$. That is, $\{\frac{n_\beta}{1} : \beta \in B\}$ is a maximal linearly independent set in $M[S^{-1}]$ and so $|B|$ is the dimension of $M[S^{-1}]$. □

Corollary 4.3.5. *Let R be an integral domain. Let*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be an exact sequence of R-modules. Then

$$\mathrm{rk}(M_2) = \mathrm{rk}(M_1) + \mathrm{rk}(M_3).$$

Proof. Indeed, $\mathrm{rk}(M_i) = \dim_F(M_i[S^{-1}])$ and the sequence

$$0 \to M_1[S^{-1}] \to M_2[S^{-1}] \to M_3[S^{-1}] \to 0$$

is an exact sequence of vector spaces. The theorem of the kernel and image in linear algebra says exactly that

$$\dim_F(M_2[S^{-1}]) = \dim_F(M_1[S^{-1}]) + \dim_F(M_3[S^{-1}]),$$

and we are done. □

Since R is an integral domain, $\mathrm{tor}(M)$ is a submodule of M. One checks that $\mathrm{tor}(M/\mathrm{tor}(M)) = 0$.

Corollary 4.3.6. *Let R be an integral domain.* $\mathrm{rk}(M) = \mathrm{rk}(M/\mathrm{tor}(M))$. *In particular, a module has rank* 0 *if and only if it is torsion.*

Proof. We have an exact sequence

$$0 \to \mathrm{tor}(M) \to M \to M/\mathrm{tor}(M) \to 0.$$

Since $\mathrm{rk}(M) = \mathrm{rk}(\mathrm{tor}(M)) + \mathrm{rk}(M/\mathrm{tor}(M))$, it is enough to show that $\mathrm{rk}(\mathrm{tor}(M)) = 0$. Given $m \in \mathrm{tor}(M)$ there is $s \in R, s \neq 0$ such that $sm = 0$. This shows that the $\frac{m}{1}$ of $M[S^{-1}]$ is equal to 0. Therefore, any element $\frac{m}{s}$ of $M[S^{-1}]$ is equal to zero. That is, if M is a torsion module then $M[S^{-1}] = 0$ and so of dimension 0.

If a module M is torsion then $\mathrm{rk}(M) = \mathrm{rk}(M/\mathrm{tor}(M) = \mathrm{rk}(0) = 0$. If a module M has rank 0 then $M[S^{-1}]$ has dimension 0 and so is 0. If $M[S^{-1}] = 0$ then for every $m \in M$, $\frac{m}{1} = 0$ and so there is some $s \neq 0$ such that $sm = 0$. This shows that M is torsion. □

Consider a multiplicative set S in a ring R and an R-module M. There is a map

$$M \to M[S^{-1}], \qquad m \mapsto \frac{m}{1}.$$

This map is a homomorphism of R-modules (when we view $M[S^{-1}]$ as an R-module via $i : R \to R[S^{-1}]$). The map is injective if $sm = 0$ for $s \in S$ and $m \in M$ implies $m = 0$. For example, if R is an integral domain, this is so when $\mathrm{tor}(M) = 0$. The map is surjective if M is divisible by s. Namely, if given $s \in S$ and $m \in M$ there is an $m_1 \in M$ such that $sm_1 = m$. Then we get the following consequence.

Proposition 4.3.7. *Let R be an integral domain and $F = \mathrm{Frac}(R)$. Let $M \subset V$ be an R-module contained in an F-vector space V of finite dimension d. Then* $\mathrm{rk}(R) \leq d$, *with equality if and only if R contains a basis for V.*

Proof. Indeed, we have an exact sequence $0 \to M \to V$ of R-modules that yields an exact sequence $0 \to M[S^{-1}] \to V[S^{-1}]$, where $S = R - \{0\}$. Since V is divisible by S and is torsion-free, we have $V[S^{-1}] = V$ and so $M[S^{-1}] \subset V$, with equality if and only if M contains a basis for V. Since $\mathrm{rk}(M) = \dim_F(M[S^{-1}])$, we are done. □

Finally, the following property of free modules (that one proves directly from the definition) is left as an exercise.

Proposition 4.3.8. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of R-modules. Then, if M_1 and M_3 are free also M_2 is free.*

4.4. **Local properties.** As previously, let R be a commutative ring. A property of modules is called a **local property** if an R-module M has that property if and only if the $R_{\mathfrak{p}}$-modules $M_{\mathfrak{p}} := M[(R-\mathfrak{p})^{-1}]$ have that property for all prime ideals $\mathfrak{p}$ of R.

Proposition 4.4.1. *"Being zero" is a local property.*

Proof. Certainly, if M is the zero R-module, then $M_{\mathfrak{p}}$ is the zero $R_{\mathfrak{p}}$-module for any prime ideal $\mathfrak{p}$. Conversely, suppose that $M \neq 0$. Let $m \in M$ be a non-zero element and consider

$$\mathrm{Ann}(m) = \{r \in R : rm = 0\}.$$

This is an ideal of R, which is proper as $1 \notin \mathrm{Ann}(m)$. Let $\mathfrak{p}$ be a maximal ideal containing $\mathrm{Ann}(m)$. It is a prime ideal too. Consider $\frac{m}{1} \in M_{\mathfrak{p}}$. If $\frac{m}{1} = \frac{0}{1}$ then for some $s \in R - \mathfrak{p}, sm = 0$. But then $s \in \mathrm{Ann}(m)$ and that is a contradiction. □

The following would appear on the exercise list.

Proposition 4.4.2. *"Being equal" is a local property. Suppose that A, B are two submodules of a module M then $A = B$ if and only if for all $\mathfrak{p}$ prime $A_{\mathfrak{p}} = B_{\mathfrak{p}}$.*

Proposition 4.4.3. *A morphism $f : M \to N$ of R-modules is the zero morphism if and only if $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is the zero morphism for all prime ideals $\mathfrak{p}$.*

End of lecture 10 (October 17)

4.5. **Equivalence of categories.**

4.5.1. *Definition of a natural transformation.* Let $F, G : \mathbf{C} \to \mathbf{D}$ be two covariant functors from the category $\mathbf{C}$ to the category $\mathbf{D}$ (similar definitions are made for a pair of contravariant functors; this is left to the reader). A **natural transformation** or a **morphism of functors** α from F to G is a map associating to every object A of $\mathbf{C}$ a morphism $\alpha_A : F(A) \to G(A)$, such that for every arrow $f : A \to B$ in $\mathbf{C}$ we have a commutative diagram:

$$\begin{array}{ccc} A & & F(A) \xrightarrow{\alpha_A} G(A) \\ \downarrow f & & \downarrow F(f) \qquad \downarrow G(f) \\ B & & F(B) \xrightarrow{\alpha_B} G(B). \end{array}$$

If each α_A is an isomorphism, we say that F and G are **naturally equivalent**, or **isomorphic**. Note that in that case, we get isomorphisms

$$\mathrm{Mor}(F(A), F(B)) \cong \mathrm{Mor}(G(A), G(B)), \quad h \mapsto \alpha_B \circ h \circ \alpha_A^{-1}.$$

We only give a few examples at this point. Given a set S there are two trivial topologies on it: the topology $\mathscr{T}_{\mathrm{disc}}$ consisting of all subsets of S, and the topology $\mathscr{T}_{\mathrm{triv}}$ consisting of the empty set and the total space alone. We get two functors $F, G : \mathbf{Sets} \to \mathbf{TopSp}$:

$$F(S) = (S, \mathscr{T}_{\mathrm{disc}}), \quad F(f) = f,$$

and

$$G(S) = (S, \mathscr{T}_{\mathrm{triv}}), \quad G(f) = f.$$

There is natural transformation $\alpha : F \to G$ given by $\alpha_A = 1_A$. Note, though, that there is no natural transformation $G \to F$.

Here is a another example. Consider the abelianization functor $\Gamma \mapsto \Gamma/\Gamma'$, now as a functor from the category of groups **Gps** to itself (and not to the category **AbGps** of abelian groups). The natural homomorphism $\alpha_\Gamma : \Gamma \to \Gamma/\Gamma'$ defines a natural transformation from the identity functor to the abelianization functor. There is a natural transformation in the other direction, but it is not really interesting. It assigns the trivial homomorphism $\Gamma/\Gamma' \to \Gamma$ (taking every element of Γ/Γ' to 1_Γ).

As a final example, consider the double-dual functor on the category of k-vector spaces $V \mapsto V^{**}$. The natural map $V \to V^{**}$, mapping a vector v to the function sending a functional ϕ on V to $\phi(v)$, defines a natural transformation of the identity functor to the functor $(\cdot)^{**}$.

4.5.2. *Definition of equivalence.* Using the concept of a natural transformation between functors we can define the notion of equivalence of categories. It is a relaxation of the natural impulse to define two categories **C** and **D** as equivalent if there are functors $F : \mathbf{C} \to \mathbf{D}, G : \mathbf{D} \to \mathbf{C}$ such that $F \circ G$ and $G \circ F$ are the identity functors. Indeed, what we want to capture in the definition to be given is that a category **C** "much smaller" than a category **D** may still capture "everything that is going on in **D**" and so should be considered as equivalent to it. For example, the whole theory of finite dimensional k-vector spaces can be captured through the category whose objects are just $\{0\}, k, k^2, k^3, \ldots$ with linear transformations between them, while the objects of the category of finite dimensional k-vector spaces are so numerous that they can't even be assigned a cardinality.

Let **C** and **D** be categories. We say that they are **equivalent** if there are functors $F : \mathbf{C} \to \mathbf{D}$ and $G : \mathbf{D} \to \mathbf{C}$ such that the compositions satisfy $GF \cong 1_\mathsf{C}$ (the identity functor of **C**) and $FG \cong 1_\mathsf{D}$ (the identity functor of **D**).

We have similarly the notion of **antiequivalence**. The definition is the same, only that both F and G are assumed to be contravariant (note that the compositions are still covariant, so the requirements $GF \cong 1_\mathsf{C}$, $FG \cong 1_\mathsf{D}$ make sense).

4.5.3. *Some examples.* Here are some important examples.

(1) The categories of subfields of a Galois extension and subgroups of the Galois group, cf. § **??** are antiequivalent.

(2) The functor $*$ on the category of k-vector spaces ${}_k\mathbf{Mod}$ is not an antiequivalence; in general, we only have a natural transformation $1 \mapsto **$ which is not an equivalence. The problem being that for infinite dimensional vector spaces the map $V \to V^{**}$ is only an inclusion.

Let **D** be a category. Recall that a subcategory **C** of **D** is a category whose objects are a subcollection of those of **D** and such that for every $A, B \in \mathbf{Ob}\ \mathbf{C}$ we have $\mathrm{Mor}_\mathsf{C}(A, B) \subseteq \mathrm{Mor}_\mathsf{D}(A, B)$. For example, the category of finite sets is a subcategory of the category of sets. A subcategory is called full if in fact we have $\mathrm{Mor}_\mathsf{C}(A, B) = \mathrm{Mor}_\mathsf{D}(A, B)$ for any $A, B \in \mathbf{Ob}\ \mathbf{C}$. Thus, the category of finite sets is a full subcategory of the category of sets. The category of abelian groups is a full subcategory of the category of groups. The category of finite dimensional vector spaces over k, $\mathbf{fVSp}_k$ is a full subcategory of the category of vector spaces over k, $\mathbf{VSp}_k = {}_k\mathbf{Mod}$. On the category $\mathbf{fVSp}_k$ the duality functor $*$ is an anti-equivalence.

Consider now another category, say **B**. The objects of **B** are the vector spaces

$$k^0, k, k^2, k^3, \ldots,$$

one for each non-negative integer. The morphisms are just linear maps. There is an obvious functor $F : \mathbf{B} \to \mathbf{fVSp}_k$, realizing **B** as a full subcategory. Define a functor $G : \mathbf{fVSp}_k \to \mathbf{B}$. Given an object A in $\mathbf{fVSp}_k$, *choose* an isomorphism $\eta_A : A \to k^{\dim(A)}$; if $A = k^n$ then we

may choose η_A to be the identity. Define now $G(A) = k^{\dim(A)}$ and for $f \in \mathrm{Mor}(A, B)$ the map $G(f) = \eta_B f \eta_A^{-1}$.

4.5.4. *A criterion for equivalence.* There is a general criteria for a functor F to be a natural equivalence of categories.

Theorem 4.5.1. *Let $F : \mathbf{C} \to \mathbf{D}$ be a covariant (respectively, contravariant) functor. There exists a covariant (respectively, contravariant) functor $G : \mathbf{D} \to \mathbf{C}$ such that (F, G) is an (respectively, anti-) equivalence of categories if and only if:*

(1) *F is full and faithful;*
(2) *F is essentially surjective, namely, for every object D of $\mathbf{D}$ there is an object C of $\mathbf{C}$ such that $F(C)$ is isomorphic to D.*

Proof. We consider the covariant case. The argument in the contravariant case is the same.

Suppose that there exists such a functor G and let

$$\gamma \colon GF \to 1_{\mathsf{C}}, \quad \delta \colon FG \to 1_{\mathsf{D}},$$

be isomorphisms. Consider $\mathrm{Mor}_{\mathsf{C}}(A, B)$ and $\mathrm{Mor}_{\mathsf{D}}(F(A), F(B))$. It is easy to check that the isomorphism $\gamma \colon GF \to 1_{\mathsf{C}}$ induces an isomorphism

$$\mathrm{Mor}_{\mathsf{C}}(GF(A), GF(B)) \xrightarrow{\simeq} \mathrm{Mor}_{\mathsf{C}}(A, B),$$

for every $A, B \in \mathbf{Ob}\ \mathbf{C}$.

Since the inverse of this map, namely the isomorphism

$$\mathrm{Mor}_{\mathsf{C}}(A, B) \to \mathrm{Mor}_{\mathsf{C}}(GF(A), GF(B))$$

factors through the map $\mathrm{Mor}_{\mathsf{C}}(A, B) \to \mathrm{Mor}_{\mathsf{D}}(F(A), F(B))$ induced by the functor F, this map too is injective. That is, F is faithful. There is a little point to worry about in this argument. For the argument to work, we need that the isomorphism $\mathrm{Mor}_{\mathsf{C}}(GF(A), GF(B)) \cong \mathrm{Mor}_{\mathsf{C}}(A, B)$, or rather its inverse $\mathrm{Mor}_{\mathsf{C}}(A, B) \to \mathrm{Mor}_{\mathsf{C}}(GF(A), GF(B))$, agrees with the composition of the functor maps

$$\mathrm{Mor}_{\mathsf{C}}(A, B) \xrightarrow{F} \mathrm{Mor}_{\mathsf{D}}(F(A), F(B)) \xrightarrow{G} \mathrm{Mor}_{\mathsf{C}}(GF(A), GF(B)).$$

Well, the isomorphisms $\gamma_A : GF(A) \to A, \gamma_B : GF(B) \to B$ satisfy, by definition, $GF(h) = \gamma_B^{-1} h \gamma_A$, for $h \in \mathrm{Mor}_{\mathsf{C}}(A, B)$, and that is exactly the compatibility we are looking for.

Likewise, the isomorphism,

$$FG : \mathrm{Mor}_{\mathsf{D}}(F(A), F(B)) \to \mathrm{Mor}_{\mathsf{D}}(FGF(A), FG(B)),$$

factors through $F : \mathrm{Mor}_{\mathsf{C}}(GF(A), GF(B)) \to \mathrm{Mor}_{\mathsf{D}}(FGF(A), FGF(B))$ and so this map F is surjective too. Since $GF \xrightarrow{\sim} 1_{\mathsf{C}}$ we get

$$\mathrm{Mor}_{\mathsf{C}}(A, B) \cong \mathrm{Mor}_{\mathsf{C}}(GF(A), GF(B)) \to \mathrm{Mor}_{\mathsf{D}}(FGF(A), FGF(B)) \cong \mathrm{Mor}_{\mathsf{D}}(F(A), F(B))$$

is surjective, too. This shows that F is full. Furthermore, let D be an object of $\mathbf{D}$ then $C = G(D)$ is an object of $\mathbf{C}$ and we have an isomorphism $\delta_{FG(D)} : FG(D) \to D$, and so the last condition is also satisfied.

We now prove the converse. Let F be a functor that is fully-faithful and essentially surjective. To define G first choose in an arbitrary fashion an isomorphism

$$\delta_D : D \to F(c_D),$$

for every object D in $\mathbf{D}$, where c_D is a suitable object of $\mathbf{C}$. Such exists by the "essentially surjective" property. Define G on objects by

$$G(D) = c_D$$

and on morphisms as follows. Given a morphism $g \in \mathrm{Mor}_{\mathsf{D}}(D, E)$ we get a morphism $g' = \delta_E g \delta_D^{-1} \in \mathrm{Mor}(F(C_D), F(C_E))$. There is a unique morphism $f \in \mathrm{Mor}(C_D, C_E) = \mathrm{Mor}(G(D), G(E))$ such that $F(f) = g'$. We let

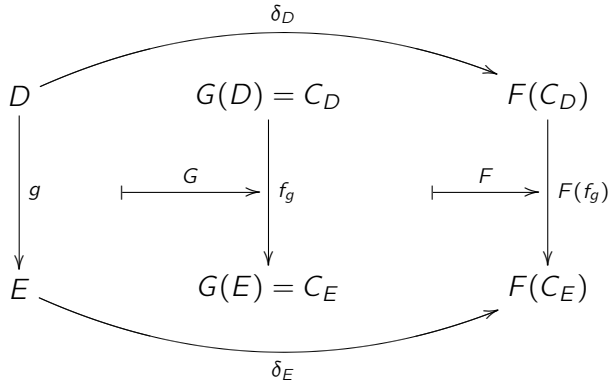
$$G(g) = f.$$

We denote this f also by f_g. To rephrase, for a morphism $g \in \mathrm{Mor}_{\mathsf{D}}(D, E)$, $G(g)$ is the unique morphism $f_g \in \mathrm{Mor}(C_D, C_E)$ such that the diagram

$$\begin{array}{ccc} D & \xrightarrow{\delta_D} & F(C_D) \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle F(f_g)} \\ E & \xrightarrow{\delta_E} & F(C_E) \end{array}$$

is a commutative diagram.

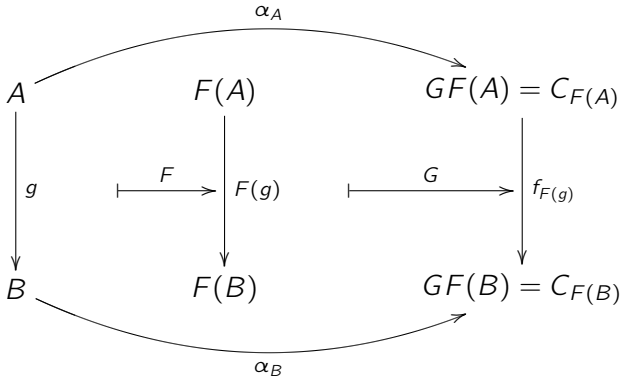
The following diagram shows that $\delta : 1_{\mathsf{D}} \to FG$ is an isomorphism.



To construct an isomorphism $\alpha : 1_{\mathsf{C}} \to GF$ we proceed as follows. Given an object A of $\mathbf{C}$ we have an isomorphism $\delta_{F(A)} : F(A) \to F(C_{F(A)}) = F(G(A))$. Since F is fully faithful, there is an isomorphism

$$\alpha_A : A \to G(A), \quad F(\alpha_A) = \delta_{F(A)}.$$

We now find the diagram



To check that the outer square commutes (and hence that $\alpha : 1_C \to GF$ is an isomorphism), it is enough to check that after apply F, because F is faithful. That is, we need to check that

$$\begin{array}{ccc} F(A) & \xrightarrow{F(\alpha_A)=\delta_{F(A)}} & F(C_{F(A)}) \\ \downarrow{\scriptstyle F(g)} & & \downarrow{\scriptstyle F(f_{F(g)})} \\ F(B) & \xrightarrow{F(\alpha_B)=\delta_{F(B)}} & F(C_{F(B)}) \end{array}$$

□

End of lecture 11 (October 22)

4.6. **Modules over a PID.** Let R be a **PID** (principal ideal domain). That is, R is an integral domain and every ideal of R is principal, meaning of the form Rr for some $r \in R$. Two of the main examples are $\mathbb{Z}$ - the ring of integers - and $k[x]$ - the ring of polynomials in one variable over a field k. The structure theorem for finitely generated modules over R has two spectacular applications: the classification of finitely generated abelian groups and the Jordan canonical form (and a more general structure theorem for linear transformations). We recall that theorem, but do not prove it here. It was proven in the previous course MATH 370 and a proof can also be found in Dummit & Foote, and in many algebra books. It rests of the following extremely useful theorem.

Theorem 4.6.1. *(***Elementary divisors theorem***) Let M be a free module of rank n over a PID R. Let $N < M$ be a submodule. There exists a basis $\{x_1, \ldots, x_n\}$ of M and non-zero elements $r_1, \ldots, r_m$ of R such that:*

(1) *$r_1 | r_2 | \cdots | r_m$.*
(2) *The set $\{r_1 x_1, r_2 x_2, \ldots, r_m x_m\}$ is a basis of N.*

In particular, N is free. Furthermore, m and the ideals (r_i), $i = 1, \ldots, m$, are uniquely determined.

One common application is the following. Let M, N be free modules of finite rank over a PID R and let $f : M \to N$ be a homomorphism of R-modules. There are bases of M and N in which f is represented by a diagonal matrix

$$\begin{pmatrix} r_1 & 0 & & \ldots & & 0 \\ 0 & r_2 & & & & \\ & & \ddots & & & \\ & & & r_n & & \\ & & & & 0 & \\ & & & & & \ddots \\ 0 & & & \ldots & & 0 \end{pmatrix},$$

where $r_1 | r_2 | \cdots | r_n$ are non-zero elements of R.

Theorem 4.6.2. *(***Structure theorem** *for modules over a PID) Let R be a PID and M a finitely generated R-module. There exists an integer $n \geq 0$ and non-zero, non-unit, elements $r_1, \ldots, r_m$ of R such that $r_1 | r_2 | \cdots | r_m$ and*

$$M \cong R^n \oplus \bigoplus_{i=1}^{m} R/(r_i).$$

As the proof of the existence part of the structure theorem is easy given the elementary divisors theorem we give it here.

Suppose that M is generated by t elements $y_1, \dots, y_t$. The R-module homomorphism $R^t \to M$, $(a_1, \dots, a_t) \mapsto \sum_{i=1}^t a_i y_i$ is surjective. Let K be the kernel. We may assume then that $M = R^t/K$. We apply the elementary divisors theorem for $K < R^t$ and find a basis $x_1, \dots, x_t$ for R^t and elements $r_1 | \cdots | r_{m'}$, $r_i \neq 0$, such that K has a basis $r_1 x_1, \dots, r_{m'} x_{m'}$. It follows that

$$M \cong R^{t-m'} \oplus \oplus_{i=1}^{m'} R/(r_i).$$

If any of the r_i are units, we may omit them and remain with $r_a | r_{a+1} | \cdots | r_{m'}$, non-zero and non-unit elements. And,

$$M \cong R^{t-m'} \oplus \oplus_{i=a}^{m'} R/(r_i).$$

It only remains to denote $t - m'$ by n and rename the r_i to get the statement as it appears in the theorem.

The uniqueness requires some argument. First note that n can be characterized as $\mathrm{rk}(M)$ and so is an invariant of M itself and not of the presentation. The submodule $\oplus_{i=1}^m R/(r_i)$ is characterized as $\mathrm{tor}(M)$ and so is an invariant of M as well. This allows to reducing the proof of uniqueness to proving that if $M \cong \oplus_{i=1}^m R/(r_i) = \oplus_{i=1}^a R/(r_i')$ where the r_i' satisfy the same properties as the r_i, then $a = m$ and $(r_i) = (r_i')$. This is a bit of combinatorics and we refer for details to Dummit and Foote.

This theorem has beautiful applications to the theory of abelian groups and to the theory of vector spaces. Before giving them, we develop a bit of language concerning categories.

4.7. **Applications of the Structure theorem for modules over PID.** There are two important applications that we discuss in turn.

4.7.1. *Finitely generated abelian groups.* In this case the PID is the ring of integers $\mathbb{Z}$. Every abelian group can be viewed as a $\mathbb{Z}$-module and vice-versa. (We could have said that the category of abelian groups is equivalent to the category of $\mathbb{Z}$-modules, but that would be an abuse of power.) Thus, the structure theorem gives the following result:

Theorem 4.7.1. *Every finitely generated abelian group M is isomorphic to an abelian group of the form $\mathbb{Z}^n \oplus \oplus_{i=1}^m \mathbb{Z}/r_i\mathbb{Z}$ where $1 < r_1 | \cdots | r_m$, for a unique n, which is the rank of M, and unique elements r_i. The torsion subgroup of M is precisely the subgroup mapping to $\oplus_{i=1}^m \mathbb{Z}/r_i\mathbb{Z}$.*

4.7.2. *Vector spaces.* Let k be a field. We claim that the category ${}_{k[x]}\mathbf{Mod}$ of $k[x]$-modules is equivalent to the following category $\mathbf{C}$. The objects of $\mathbf{C}$ are pairs (V, T) consisting of a k-vector space V and a linear transformation $T : V \to V$. A morphism $f : (V_1, T_1) \to (V_2, T_2)$ is a linear map $f : V_1 \to V_2$ such that $f \circ T_1 = T_2 \circ f$.

Indeed, given a $k[x]$-module V, view V as a k-vector space and define a transformation $T : V are V$ by the formula

$$T(v) = x \cdot v,$$

where the multiplication is the module multiplication between the element x of the ring $k[x]$ and the element v of the $k[x]$-module V. A $k[x]$-module homomophism $f : V_1 \to V_2$ is naturally a k-linear map $f : V_1 \to V_2$ and since $f(x \cdot v) = x \cdot f(v)$ it is a morphism $(V_1, T_1) \to (V_2, T_2)$.

Conversely, given a pair (V, T) define a $k[x]$-module structure by

$$g(x) \cdot v = g(T)(v).$$

Since $(g + h)(T) = g(T) + h(T)$, $(gh)(T) = g(T)h(T)$, etc. this a module structure. A morphism $f : (V_1, T_1) \to (V_2, T_2)$ satisfies $f \circ T_1 = T_2 \circ f$ and so it satisfies for any polynomial expression g in T_1 that $f \circ g(T_1) = g(T_2) \circ f$. Therefore, f becomes a morphism of $k[x]$-modules.

In this case, the composition of the functors in either order are the identity maps, so the equivalence of categories is straightforward. We shall often refer to the module associated to (V, T) as the $k[x]$-module V, leaving T to be understood from the context.

It is now interesting to see what module theory says about vector spaces and vice-versa. Some very simple observations are:

(1) T invariant subspaces of (V, T) correspond to sub $k[x]$-modules of V. And then, quotients correspond to quotients.
(2) For a polynomial $f(x) \in k[x]$, $f(T)$ is the zero linear map if and only if $f(x) \in \mathrm{Ann}_{k[x]}(V)$.
(3) $(V, T) \cong (V_1, T_1) \oplus (V_2, T_2)$ if and only if $V \cong V_1 \oplus V_2$ as $k[x]$-modules.

Proposition 4.7.2. *Let V be a k-vector space of finite dimension. Let $T : V \to V$ be a linear map. Then the $k[x]$-module V is a torsion module. Conversely, every finitely-generated torsion module arises this way.*

Proof. Write V as a sum of $k[x]$-modules.

$$V \cong (k[x])^n \oplus \oplus_{i=1}^m k[x]/(f_i(x)),$$

where we may choose the f_i to be monic and $f_1(x)|\cdots|f_m(x)$, and that determines these polynomials uniquely. The dimension of $k[x]$ as a k-module is infinite, because $1, x, x^2, x^3, \ldots$ are independent over k. Thus, our assumption forces $n = 0$ and so V is torsion.

Conversely, given a finitely generated torsion $k[x]$-module, we may write it as

$$\oplus_{i=1}^m k[x]/(f_i(x)).$$

Since the equivalence of categories commutes with direct sums, it is enough to whose that $k[x]/(f_i)$ arises from a finite dimensional vector space, but this is clear; in fact, the dimension of this vector space is precisely the degree of f_i. □

Applying the Proposition and the observations above we find the following.

Theorem 4.7.3. *Let (V, T) be a finite-dimensional k-vector space with a linear transformation T and decompose it as a $k[x]$-module:*

$$V \cong \oplus_{i=1}^m k[x]/(c_i(x)),$$

where the c_i are monic polynomials satisfying $c_1(x)|c_2(x)|\cdots|c_m(x)$. Let

$$(V, T) = \oplus_{i=1}^m (V_i, T_i)$$

be the corresponding decomposition of V into T-invariant subspaces. Then,

(1) $\dim_k(V_i) = \deg(c_i(x))$.
(2) *The minimal polynomial of T_i is equal to its characteristic polynomial and both are equal to $c_i(x)$.*
(3) *Fix i and write $c_i(x) = x^d + \alpha_{d-1}x^{d-1} + \cdots + \alpha_0$. There is a basis for V_i in which T_i is given by the matrix*

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & -\alpha_0 \\ 1 & 0 & 0 & \cdots & -\alpha_1 \\ 0 & 1 & 0 & \cdots & -\alpha_2 \\ \vdots & & & \vdots & \\ 0 & 0 & 0 & \cdots & -\alpha_{d-1} \end{pmatrix}.$$

(4) *We have* $\dim_k(V) = \sum_{i=1}^m \deg(c_i(x))$.
(5) *The minimal polynomial of T on V is $c_m(x)$, while its characteristic polynomial is given by $c_1(x)c_2(x)\cdots c_m(x)$.*

(6) *T is diagonalizable over some extension field of k if and only if $c_m(x)$ has no repeated roots, that is,* $\gcd(c_m(x), c_m'(x)) = 1$. *It is diagonalizable over k if and only if $c_m(x)$ factors into linear terms over k.*

End of lecture 12 (October 24)

4.7.3. *The Jordan canonical form.* We assume here that the characteristic polynomial of T, and hence the invariant factors $c_i(x)$, factors into linear terms over the field k. That would be the case if k is algebraically closed, which is often the setting in which one develops the theory of Jordan canonical form, but in fact this is not necessary. The weaker assumption we make suffices.

Let us focus on one invariant factor $c(x) = c_i(x)$. It factors as $c(x) = \prod_{i=1}^{a}(x-\lambda_i)^{b_i}$. Here the λ_i are some of the eigenvalues of T and the $b_i > 0$ are multiplicities bounded by the multiplicities in the characteristic polynomial of T. We apply the Chinese Remainder theory and get

$$k[x]/(c(x)) \cong \oplus_{i=1}^{b_i} k[x]/((x-\lambda_i)^{a_i}).$$

And, so, it behooves us to analyze modules of the form $k[x]/((x-\lambda)^a)$. A change of variable $x \mapsto y = x - \lambda$ allows us to study $k[y]/(y^a)$, which corresponds to a vector space of dimension a and a linear transformation with a matrix of the form

$$\begin{pmatrix} 0 & 1 & & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ & & & \cdots & 1 \\ 0 & & & \cdots & 0 \end{pmatrix}.$$

(The corresponding basis for the polynomials is $x^{a-1}, x^a, \ldots, x, 1$.) Therefore, $k[x]/((x-\lambda)^a)$ corresponds to a vector space of dimension a and a linear transformation with a matrix of the form

$$\begin{pmatrix} \lambda & 1 & & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ & & & \cdots & 1 \\ 0 & & & \cdots & \lambda \end{pmatrix}.$$

We call such a matrix a **Jordan block** and denote it $J(\lambda, a)$. Putting it all together, we find the following.

Theorem 4.7.4. *(***Jordan canonical form***) Every matrix T whose characteristic polynomial factors into linear terms over k is conjugate to a block diagonal matrix of the form*

$$\operatorname{diag}(J(\lambda_1, a_1), \ldots, J(\lambda_b, a_b))$$

of Jordan blocks. The λ_i (that need not be distinct) are the eigenvalues of T. Each eigenvalue λ of T appears and $\sum_{\{i:\lambda_i=\lambda\}} a_i$ is the algebraic multiplicity of λ in the characteristic polynomial of T. Furthermore, the set of Jordan blocks is uniquely determined by T.

4.8. **Morita equivalence.**

Morita Equivalence

Theorem (Special case of Morita's theory)
Let R be a ring. The categories ${}_R\mathrm{Mod}$ and ${}_{M_n(R)}\mathrm{Mod}$ are equivalent.

Proof: Define a functor

$$F: {}_R\mathrm{Mod} \longrightarrow {}_{M_n(R)}\mathrm{Mod}$$

$F(M) = M^n$, M an R-module. (column vectors)
$F(f) = {}^t(f,\dots,f)$ for $f: M \to N$ in ${}_R\mathrm{Mod}$.

It is easy to check F is a functor. Clearly, F is faithful ($F(f)=F(g) \Rightarrow f=g$). Further, F is additive. We next check F is full.

Any morphism $\varphi: M^n \to N^n$ is of the form $\varphi(\underline{m}) = {}^t(\varphi_1(\underline{m}),\dots,\varphi_n(\underline{m}))$
Now, $\varphi({}^t(m,0,\dots,0)) = \varphi(E_{11}\,{}^t(m,0,\dots,0)) = E_{11}\varphi({}^t(m,0,\dots,0)) = ({}^t\varphi_1(m,0,\dots,0),0,\dots,0)$
(E_{ij} are the elementary matrices; E_{ij} has 1 at the ij place and else 0). We therefore conclude that for $i\neq 1$, φ_i vanishes on $(m,0,\dots,0)$. By symmetry, φ_i vanishes on $m\cdot e_j$, $\forall j\neq i$, $m\in M$.
Thus, using linearity,

$$\varphi({}^t(m_1,\dots,m_n)) = {}^t(\varphi_1(m_1),\dots,\varphi_n(m_n))$$

(where $\varphi_i(m_i) := \varphi_i({}^t(0,\dots,0,\overset{i}{m_i},0,\dots,0))$)
Further, given $\sigma\in S_n$ let $E(\sigma)$ be the permutation matrix associated to σ^{-1}, so that

$$E(\sigma)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} m_{\sigma(1)} \\ \vdots \\ m_{\sigma(n)} \end{pmatrix}.$$

Then,

$$\varphi(E(\sigma)\,{}^t(m_1,\dots,m_n)) = \varphi\left({}^t(m_{\sigma(1)},\dots,m_{\sigma(n)})\right) = {}^t(\varphi_1(m_{\sigma(1)}),\dots,\varphi_n(m_{\sigma(n)})).$$

OTOH, $\varphi(E(\sigma)\,{}^t(m_1,\dots,m_n)) = E(\sigma)\,{}^t\varphi(m_1,\dots,m_n)$, because φ is a homom. of $M_n(R)$-modules. Thus,

$${}^t(\varphi_1(m_{\sigma(1)}),\dots,\varphi_n(m_{\sigma(n)})) = E(\sigma)\,{}^t(\varphi_1(m_1),\dots,\varphi_n(m_n)) = {}^t(\varphi_{\sigma(1)}(m_{\sigma(1)}),\dots,\varphi_{\sigma(n)}(m_{\sigma(n)}))$$

This implies,

$$\varphi_i = \varphi_{\sigma(i)},\ \forall i,\ \forall \sigma \in S_n.$$

Thus, $\varphi = (\varphi_1,\dots,\varphi_1) = F(\varphi_1)$, and F is full.

Since a functor is an equivalence of categories if and only if it's faithfull, full, and essentially surjective, we need only prove the latter property. Namely, that every $M_n(R)$-module is isomorphic to $F(N)$ for some R-module N.

Let M be an $M_n(R)$-module. We shall make use of the identities: $E_{lk}E_{ij} = \delta_{ki}E_{lj}$.

First, we claim that

$$M \cong E_{11}M \oplus \cdots \oplus E_{nn}M \quad \text{as } R\text{-modules.}$$

This is easy to verify using $I_n = E_{11}+\cdots+E_{nn}$. The maps being

$$m \longmapsto (E_{11}m,\dots,E_{nn}m),\quad \sum a_i \longleftarrow (a_1,\dots,a_n).$$

Claim: $E_{l1}M = E_{ll}M$. (Equality, not just $\cong$).

Indeed, $E_{l1}M = E_{ll}E_{l1}M$ so we get $\subseteq$. OTOH, $E_{ll}M = E_{l1}E_{1l}M$ and we get $\supseteq$.

Therefore,

$M \cong E_{11}M \oplus E_{21}M \oplus \cdots \oplus E_{n1}M$, where, still, $\sum a_i \longleftrightarrow (a_1, a_n)$

Claim: $E_{11}M \xrightarrow{\sim} E_{\ell 1}M$ by $a \longmapsto E_{\ell 1}a$ (restriction of $M \to E_{\ell 1}M$).

The inverse is $E_{1\ell}b \longleftarrow b$.

(This is easy to verify after noting that E_{11} acts as the identity on $E_{11}M$ and $E_{\ell\ell} = E_{\ell 1}E_{1\ell}$ acts as the identity on $E_{\ell 1}M$).

We conclude that

$$M \cong E_{11}M \oplus \cdots \oplus E_{11}M, \qquad (*)$$

where the map r.h.s. $\to$ l.h.s. is $(a_1, \ldots, a_n) \longmapsto (E_{11}a_1, E_{21}a_2, \ldots, E_{n1}a_n) = \sum_{\ell=1}^{n} E_{\ell 1}a_\ell$.

We let $N = E_{11}M$, an R-module. As R-modules $F(N) \cong M$, but we need to check this is an isomorphism of $M_n(R)$-modules, and it is enough to check it commutes with the matrices $E_{\ell k}$. By linearity, we need only deal with $E_{\ell k}\,{}^t(0, \ldots, \overset{k}{a}, 0, \ldots, 0)$, where $a \in E_{11}M$.

If $i \neq k$ this is zero. If $i = k$ this is ${}^t(0, \ldots, \overset{\ell}{a}, \ldots 0)$. This element is sent to $E_{\ell 1}a$ under $(*)$. OTOH, ${}^t(0, \ldots, a, \ldots, 0)$ is sent to $E_{i1}a$ under $(*)$ and $E_{\ell k}E_{i1}a = \begin{cases} 0 & i \neq k \\ E_{\ell 1}a & i = k \end{cases}$.

So it checks! $\square$

Suppose that $R = D$ is a division ring. The only maximal left ideal is $\{0\}$ and so D is the unique simple D-module.

Clearly D is semisimple and so every D-module is isomorphic to D^α for some cardinality α, i.e. $\cong \bigoplus_{i \in I} D$, for some index set I of cardinality α.

We conclude that $M_n(D)$ has a unique simple module D^n and $M_n(D) \cong \underbrace{D^n \oplus \cdots \oplus D^n}_{n}$ (as $M_n(D)$-modules) is semisimple. Further,

$$\mathrm{Hom}_{M_n(D)}(D^n, D^n) \cong \mathrm{Hom}_D(D, D) \cong D^{op} \quad (\text{under } f \mapsto f(1).$$

Note: $gf \mapsto (gf)(1) = g(f(1)) = f(1) \cdot g(1)$, thus the "op".)

Applying this to irreducible repn's of a finite group, as we had done, one finds that if (V, ρ) is an irred. repn of G then any auto of (V, ρ) is a scalar.

End of lecture 13 (October 29)

4.9. **Injective and projective limits.**

Injective and projective limits

* Index sets.

By an index set I we mean a partially ordered set (poset). That is, there's a relation $\leq$ holding b/w some elements of I s.t.: (i) $x \leq x$, $\forall x \in I$. (ii) $x \leq y$ and $y \leq x \Rightarrow x = y$. (iii) $x \leq y$ and $y \leq z \Rightarrow x \leq z$.

A poset may be viewed as a category whose objects are the elements $x \in I$ and $\mathrm{Mor}(x,y) = \begin{cases} i_{xy} & \text{if } x \leq y \\ \phi & \text{else} \end{cases}$

(Check the category axioms. Formulate a converse.)

Let $\underline{C}$ be a category. A direct system in $\underline{C}$ (indexed by I) is a covariant functor $I \longrightarrow \underline{C}$. An inverse system in $\underline{C}$ is a contravariant functor $I \longrightarrow \underline{C}$.

Examples:

(1) Direct / inverse systems in Ab.Gps.

* $I = \mathbb{Z}_{>0}$. Say $n \leq m$ if $n \mid m$.

$C_n := \frac{1}{n}\mathbb{Z} \xhookrightarrow[i_{nm}]{} \frac{1}{m}\mathbb{Z}$ if $n \mid m$.

$(\{C_n\}, \{i_{nm}\})$ is a direct system.

* Same I, but now let $C_n := \mathbb{Z}/n\mathbb{Z}$.

$C_n \xleftarrow[p_{nm}]{} C_m$ if $n \mid m$ by $x \pmod n \longleftarrow x \pmod m$

$(\{C_n\}, \{p_{nm}\})$ = inverse system.

* $I = \mathbb{Z}_{\geq 0}$ where $n \leq m$ is the usual order. p = fixed prime number.

$\mathbb{Z}/p^n\mathbb{Z} \xleftarrow[\pi_{nm}]{} \mathbb{Z}/p^m\mathbb{Z}$. $(\{C_n\}, \{p_{nm}\})$ = inverse system.

(2) I = any set. Only $x \leq x$ (if $x \neq y$ the relation $x \leq y$ doesn't hold). $\underline{C}$ any category. Giving an object C_x for all $x \in I$ gives both a direct system and an inverse system.

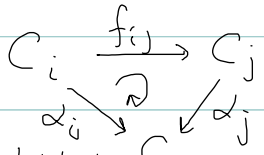
(3) Given a simple graph whose vertices are objects of $\underline{C}$ and each arrow b/w vertices corresponds to a morphism, such that the the condition on triangles holds  then + composition identity

we get a direct/inverse system.

Definition (direct limit): Let $(\{C_i\}, \{f_{ij}\})$ be a direct system in a category $\underline{C}$. The direct (or injective) limit $\varinjlim_{i \in I} C_i$, if it exists, is an object C in $\underline{C}$, with morphisms

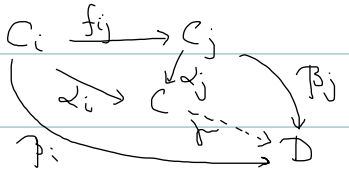
$$\alpha_i : C_i \longrightarrow C$$

such that for all $i \leq j$



and so that the universal property holds:

Given an object D in $\underline{C}$, $\beta_i : C_i \to D$, $\beta_j \circ f_{ij} = \beta_i$, there exists a unique morphism $\gamma : C \to D$ s.t.

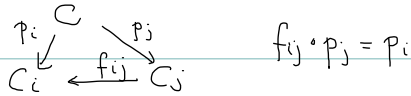


commutative, $\forall\, i \leq j$.

Remark: Let $I^+ = I \cup \{\infty\}$ and extend the order to I^+ by $x \leq \infty$ for all $x \in I$. Then we can phrase everything in terms of functors $I^+ \longrightarrow \underline{C}$, extending the functor $I \to \underline{C}$ that defines the direct system. (Work that out!).

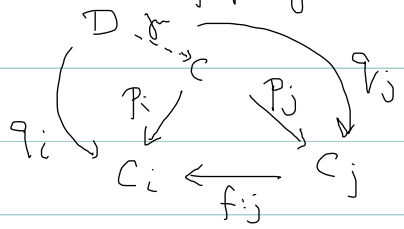
Definition (projective limit):

Let $(\{C_i\}, \{f_{ij}\})$ be an inverse system. It's inverse (or projective) limit of it, $\varprojlim_{i \in I} C_i$, if it exists, is an object $C \in \mathcal{C}$ with morphisms $p_i : C \to C_i$ s.t.



$f_{ij} \circ p_j = p_i, \quad \forall i \leq j$

that has the universal property ....



As usual, the universal property implies that direct/inverse limits are unique, up to unique isomorphism, if they exist. In general, they need not exist (or one may exist and the other not). The main theorem is:

Theorem: Let R be a ring. Direct and inverse limits exist in R-Mod.

Proof:

Let I be an index set and $(M_i, \{f_{ij}\})$ a direct system in R-Mod. Let

$$\bigoplus_{i \in I} M_i = \left\{ (m_i)_{i \in I} : m_i \in M_i,\ m_i = 0 \text{ for almost all } i \right\}$$

It's an R-module under coordinate-wise addition and $r(m_i)_i = (rm_i)_i$.

Let $\lambda_i : M_i \longrightarrow \bigoplus_i M_i$ be the inclusion at the i-th component. Let $W \subseteq \bigoplus_i M_i$ be the submodule generated by all elements of the form

$$\lambda_i(a) - \lambda_j(f_{ij}(a)) \quad i \leq j, a \in M_i$$

Let

$$C = \bigoplus_{i \in I} M_i / W$$

and

$\alpha_i : M_i \longrightarrow C$ is the composition

$$M_i \xrightarrow{\lambda_i} \bigoplus_i M_i \longrightarrow C$$

We claim that $(C, \{\alpha_i\})$ is a direct limit. First, in C we have

$$\alpha_j(f_{ij}(a)) = \lambda_j(f_{ij}(a)) = \lambda_i(a)$$

Thus the commutativity

$$\begin{array}{ccc} M_i & \xrightarrow{f_{ij}} & M_j \\ & \searrow^{\alpha_i} \quad \swarrow_{\alpha_j} & \\ & C & \end{array}$$

Next, given $(D, \{\beta_i : M_i \longrightarrow D\})$, $\beta_j \circ f_{ij} = \beta_i$ we define a homomorphism

$$\tilde{\beta} : \bigoplus_i M_i \longrightarrow D, \quad \tilde{\beta}((m_i)) = \sum_i \beta_i(m_i).$$

Note that

$$\tilde{\gamma}(\lambda_i(a) - \lambda_j(f_{ij}(a))) = \beta_i(a) - \beta_j(f_{ij}(a)) = \beta_i(a) - \beta_i(a) = 0$$

Thus $\tilde{\gamma}$ induces a well-defined homom.

$$\gamma : C = \left(\bigoplus_i M_i\right)/W \longrightarrow D$$

and $\gamma \circ \alpha_i = \beta_i$.

The uniqueness of γ is clear from the fact that C is generated by the images $\alpha_i(M_i)$.

Existence of projective limits:

We let $\prod_{i \in I} M_i = \{(m_i)_i : m_i \in M_i\}$. It is an R-module under component-wise addition with $r(m_i)_i := (rm_i)_i$.

We define $C \subseteq \prod_i M_i$ to consist of the "compatible" sequences:

$$C = \{(m_i)_i : f_{ij}(m_j) = m_i, \forall i \leq j\}.$$

It's an R-module and the projection maps

$$p_i : C \longrightarrow M_i, \quad p_i((m_j)_j) = m_i,$$

satisfy $f_{ij} \circ p_j = p_i$.

Given D with maps $q_j : D \to M_j$ s.t. $f_{ij} \circ q_j = q_i$, define a map

$$\varphi : D \to C, \quad \varphi(d) = (q_i(d))_i.$$

It's well-defined — we leave that and the rest of the proof as an exercise. □

Important examples:

(1) Take I to have the discrete order $x \leq x$ only.

In this case, the direct limit is called the direct sum and is just $\bigoplus_{i \in I} M_i$.

The inverse limit is called the direct product and is just $\prod_i M_i$.

It is easy to see that the direct limit of $A \to B$ is B and the projective limit is A. Similarly for $A \to B \to C$.

slightly more complicated diagrams

$$\begin{array}{ccc} A & \to & B \\ \downarrow & & \\ C & & \end{array} \qquad \begin{array}{ccc} & & C \\ & & \downarrow \\ A & \to & B \end{array}$$

lead to interesting constructions called pushout and pullback. They are treated in the exercises.

(2) Again I is discrete but now the category is Sets. Direct and inverse limits exist (in general). For such I

$$\varinjlim C_i = \coprod C_i \quad \text{(disjoint union)}$$

and

$$\varprojlim C_i = \prod C_i \quad \text{(cartesian product)}$$

(3) Consider the category of groups and the set $I = \{1, 2\}$ with discrete order. A direct system is just 2 groups G_1, G_2.

Claim: The direct limit is $G_1 * G_2$, the free product of G_1, G_2. It's the group whose elements are equivalence class of words $x_1 x_2 \cdots x_n$ where $x_i \in G_1 \cup G_2$ (we assume G_1, G_2 are disjoint). We allow the relations

$$x_1 \cdots x_i x_{i+1} \cdots x_n \sim x_1 \cdots x_{i-1} (x_i x_{i+1}) \cdots x_n$$

if x_i, x_{i+1} are in the same group, and

$$x_1 \cdots x_{i-1} e x_{i+1} \cdots x_n \sim x_1 \cdots x_{i-1} x_{i+1} \cdots x_n$$

if e is the identity of either G_1 or G_2.
The multiplication is just

$$x_1 \cdots x_n * y_1 \cdots y_m = x_1 \cdots x_n y_1 \cdots y_m$$

It's well-defined. The identity is the empty word and $(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1}$.

We have homom. $G_i \longrightarrow G_1 * G_2$, by $x \longmapsto x$. Given homom. $f_i : G_i \longrightarrow H$, we may define $h : G_1 * G_2 \longrightarrow H$ by

$$h(x_1 \cdots x_n) = h(x_1) \cdots h(x_n)$$

where $h(x) = f_i(x)$ if $x \in G_i$. This is well-defined. So $G_1 * G_2$ is the direct limit.

Proposition: If $G_i = \langle X_i \mid R_i \rangle$ then

$$G_1 * G_2 \cong \langle X_1 \amalg X_2 \mid R_1 \amalg R_2 \rangle.$$

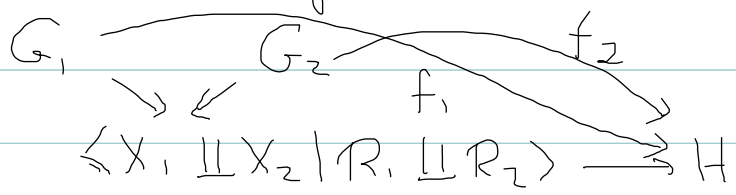
Proof:
We have natural homom.

$$G_i \longrightarrow \langle X_1 \amalg X_2 \mid R_1 \amalg R_2 \rangle$$

Given homom. $f_i : G_i \longrightarrow H$ we define a homom. $\mathcal{F}(X_1 \amalg X_2) \longrightarrow H$ s.t.

$$a \longmapsto f_i(a) \text{ if } a \in X_i.$$

This homom. factors through $\langle X_1 \amalg X_2 \mid R_1 \amalg R_2 \rangle$ and we get a comm. diagram



The uniqueness of such a homom. is clear and so $\langle X_1 \amalg X_2 \mid R_1 \amalg R_2 \rangle \cong G_1 * G_2$. $\square$

It is easier to prove that the inverse limit of $\{G_1, G_2\}$ is simply $G_1 \times G_2$.

(4) I-adic completions.

Let R be a commutative ring and I an ideal of R. Consider the inverse system

$$\cdots \to R/I^3 \longrightarrow R/I^2 \longrightarrow R/I$$

It is a system of R-modules and so the projective limit $\varprojlim_n R/I^n$ exists and is equal to

$$\{(\cdots, m_3, m_2, m_1) : m_i \in R/I^i,\ m_i \equiv m_{i-1} \bmod I^{(i-1)}\}$$

One easily checks that this is in fact a ring under coordinate-wise multiplication. It's called the I-adic completion of R.

The natural map

$$R \longrightarrow \varprojlim R/I^n$$

$$r \longmapsto (\cdots, r, r, r)$$

is a ring homom. with kernel $\bigcap_n I^n = \{0\}$.

After this intersection is trivial and then

$$R \hookrightarrow \varprojlim R/I^n =: \hat{R}$$

A theorem of Krull says that if R is noetherian (any increasing chain of ideals becomes stationary) then the kernel are the elements of R killed by some element of $1+I$. So, if R is an integral domain, $R \hookrightarrow \hat{R}$.

Let $R = \mathbb{F}[X_1, \dots, X_n]$ and $I = (X_1, \dots, X_n)$ then $\hat{R} \cong \mathbb{F}[\![X_1, \dots, X_n]\!]$ (power series in n variables). To see that note that $I^a = \langle m(X_1, \dots, X_n) : m \text{ monomial of deg. } a \rangle$

We define

$$\mathbb{F}[\![X_1, \dots, X_n]\!] \longrightarrow \hat{R}$$
$$f(X_1, \dots, X_n) \longmapsto (f_i)_i, \quad f_i = f \bmod I^i$$

This is clearly a well-defined ring homom. If $f_i = 0$ then $f = \sum_J a(J) X^J$ (multi index notation: $J = (j_1, \dots, j_n)$, $X^J = X_1^{j_1} \cdots X_n^{j_n}$) has only monomials of degree $> i$. Thus one concludes the homomorphism is injective. Now given $(f_i)_i \in \hat{R}$, we may represent

each f_i uniquely as $\sum_{|J|<i} a(J) x^J$
$(|J| = j_1 + \cdots + j_n)$.

The congruences $f_{i+1} \equiv f_i \bmod I^i$ show that $a(J)$ doesn't depend on i.

Therefore, $f = \sum_J a(J) x^J$ maps to $(f_i)_i$.

End of lecture 14 (October 31)

4.9.1. *More Examples: injective limits.*

Examples of injective limits

Directed index sets: Suppose I is a poset. We call I directed if for any $x, y \in I$ there is $z \in I$ s.t. $x \leq z$ and $y \leq z$.

Proposition: Let $(\{M_i\}, \{f_{ij}\})$ be a direct system of R-modules indexed by a directed poset I. Put a relation on $\coprod M_i$ (disjoint union) by saying that $m_x \in M_x$, $m_y \in M_y$ are related, $x \sim y$, if for some $z \in I$ s.t. $x \leq z$, $y \leq z$, we have $f_{xz}(m_x) = f_{yz}(m_y)$.

(i) This is an equivalence relation. Let $[x]$ denote the equv. class.

(ii) Define $[x_1] + [x_2] = [x_3]$ for $x_1 \in M_a$, $x_2 \in M_b$ as follows. Pick $c \in I$ s.t. $a \leq c$, $b \leq c$ and let $x_3 = f_{ac}(x_1) + f_{bc}(x_2)$. Further, for $r \in R$ let $r[x] = [rx]$. This makes the equivalence classes into an R-module.

(iii) $\varinjlim M_i \cong M$.

Remark: The particular case where I has a maximal element i_∞ is worth noting:

$\varinjlim M_i \cong M_{i_\infty}$.

Example: Let R be an integral domain and $s \in R$, $s \neq 0$. Denote by $R[1/s]$ the localization of R at $\{1, s, s^2, \ldots\}$. Note that for $s \mid t$ we have $R[1/s] \to R[1/t]$. $I = R \setminus \{0\}$ is a directed poset where $s \leq t$ if $s \mid t$ (given s_1, s_2 we let $s_3 = s_1 s_2$ and $s_1 \mid s_3$, $s_2 \mid s_3$). We have the injective system $\{R[1/s] : s \in R \setminus \{0\}\}$. It is easy to see that $\varinjlim R[1/s] =$ Frac. field of R.

4.9.2. *More Examples: projective limits.* For the discussion of infinite Galois groups we will need to consider projective limits of groups. We consider here the general problem, leaving the more thorough discussion of projective limits of finite groups to the chapter on Galois theory.

Proposition 4.9.1. *Projective limits exist in the category of groups.*

Proof. The proof is verbatim the proof for R-modules. Therefore, we will be brief. Given an index set I and an inverse system $(\{G_i\}_{i\in I}, \{f_{ij} : G_j \to G_i\}_{i\leq j})$ of groups, let

$$\prod_{i\in I} G_i = \{(g_i)_{i\in I} : g_i \in G_i\},$$

be the direct product of the underlying sets. We make it into a group by

$$(g_i)_i \cdot (h_i)_i := (g_i h_i)_i.$$

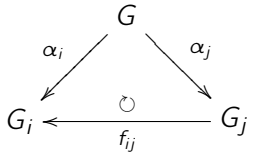
Consider now the subset

$$G = \{(g_i)_i : f_{ij}(g_j) = g_i, \forall i \leq j\}.$$

One easily checks it is a subgroup of G, using that all f_{ij} are group homomorphisms. The projections $p_i : \prod_{i\in I} G_i \to G_i$ induce by restriction group homomorphisms

$$\alpha_i : G \to G_i, \qquad \alpha_i((g_j)_j) = g_i.$$

The homomorphisms α_i satisfy $\alpha_i \circ f_{ij} = \alpha_j$:



Given a group D and homomorphisms $\beta_i : D \to G_i$ such that $\beta_i \circ f_{ij} = \beta_j$ define a group homomorphism $h : D \to G$ by $h = (\beta_i)_i$. Clearly h satisfies $\alpha_i \circ h = \beta_i$ and, in fact, this property determines h uniquely. □

Proposition 4.9.2. *Projective limits exist in the category of topological spaces.*

Proof. Let $(\{X_i\}, \{f_{ij} : X_j \to X_i\}_{i\leq j})$ be an inverse system of sets indexed by an index set I. Let

$$X = \{(x_i)_{i\in I} : f_{ij}(x_j) = x_i, \forall i \leq j\}.$$

We consider X as a subspace of $\prod_{i\in I} X_i$. The proof is as for the case of groups. □

Proposition 4.9.3. *Projective limits exist in the category of sets.*

Proof. Let $(\{X_i\}, \{f_{ij} : X_j \to X_i\}_{i\leq j})$ be an inverse system of topological spaces indexed by an index set I. Let

$$X = \{(x_i)_{i\in I} : f_{ij}(x_j) = x_i, \forall i \leq j\}.$$

We consider X as a subspace of $\prod_{i\in I} X_i$, where the latter is equipped with the product topology. Then

$$X = \lim_{i\in I} X_i.$$

The proof is as in the case of groups, only that one needs to justify that the "obvious" maps are continuous. □

A group G, whose multiplication map and inverse map are denoted, respectively,

$$m : G \times G \to G, \qquad \iota : G \to G,$$

is called a **topological group** if there is a topology given on G such that the functions m and ι are continuous, where we provide $G \times G$ with the product topology.

Proposition 4.9.4. *Projective limits exist in the category of topological groups.*

Proof. Let $(\{G_i\}, \{f_{ij} : G_j \to G_i\}_{i \leq j})$ be an inverse system of topological groups indexed by an index set I. Let

$$G = \{(g_i)_{i \in I} : f_{ij}(g_j) = g_i, \forall i \leq j\}.$$

We consider G as a subgroup of $\prod_{i \in I} G_i$, where the latter is equipped with the product topology and with coordinate-wise multiplication and that makes the product a topological group and makes G into a sub topological group relative to the subspace topology (this requires verification that is omitted here). Then

$$G = \lim_{i \in I} G_i.$$

The proof proceeds as in the case of groups and topological spaces combined, only that one needs to justify that the "obvious" maps are continuous and are homomorphisms. □

A topological group is a **homogenous space**; namely, for every $x, y \in G$ there is an homeomorphism φ of the topological space underlying G such $\varphi(x) = y$. Thus, G - as a topological space - "looks the same from every point". Indeed, given an element $g \in G$ denote by $[g]$ the function

$$[g] : G \to G, \quad [g](x) = gx.$$

It is easy to check that $[g]$ is a continuous map with inverse given by $[g^{-1}]$, hence a homeomorphism. Given x, y as above take the homeomorphism $[yx^{-1}]$. Let X be a homogenous topological space and $x \in X$ a point. The topology of X is completely determined by the knowledge of the open sets of X that contain x. Indeed, if U is an open set containing x, $y \in X$ and $\varphi(x) = y$ then $\varphi(U)$ is an open set containing y. If U is any open set, choose for every $y \in U$ a homeomorphism φ_{xy} of X such that $\varphi_{xy}(x) = y$ then $\varphi_{xy}^{-1}(U)$ is an open set containing x.

In particular, the topology of a topological group is completely determined by the knowledge of open sets containing the identity. Further, suppose that we have a collection $\mathscr{C}$ of open sets of G such that each $U \in \mathscr{C}$ contains the identity and every open set containing the identity contains some $U \in \mathscr{C}$. Then the collection $\mathscr{C}$ determines the topology of G. Indeed, given an open set V and $y \in V$ choose an open set $U_y \subset \varphi_{1,y}^{-1}(V)$ such that $U_y \in \mathscr{C}$. Then $V = \cup_{y \in V} \varphi_{1,y}(U_y)$.

Proposition 4.9.5. *Let $(\{G_i\}, \{f_{ij} : G_j \to G_i\}_{i \leq j})$ be an inverse system of topological groups such that each G_i is a Hausdorff topological group. Then $\varprojlim_{i \in I} G_i$ is a closed subgroup of $\prod_{i \in I} G_i$.*

Proof. We have defined $G = \varprojlim_{i \in I} G_i$ as

$$G = \{(g_r)_{r \in I} \in \prod_{r \in I} G_r : f_{ij}(g_j) = g_i, \forall i \leq j\}.$$

We may write then

$$G = \cap_{i \leq j} \{(g_r) \in \prod_{r \in I} G_r : f_{ij}(g_j) = g_i\},$$

and so it is enough to prove that for every i, j the set $\{(g_r) \in \prod_{r \in I} G_r : f_{ij}(g_j) = g_i\}$ is closed. This set is equal to $\prod_{r \notin \{i,j\}} G_r \times \{(g_i, g_j) \in G_i \times G_j : f_{ij}(g_j) = g_i\}$. The complement of this set is $\prod_{r \notin \{i,j\}} G_r \times (G_i \times G_j \setminus \{(g_i, g_j) \in G_i \times G_j : f_{ij}(g_j) = g_i\}$, and so it is enough to prove that $\{(g_i, g_j) \in G_i \times G_j : f_{ij}(g_j) = g_i\}$ is a closed subset of $G_i \times G_j$.

Let $\Delta = \{(x, x) : x \in G_i\}$ be the diagonal of $G_i \times G_i$. Let $Id \times f_{ji} : G_i \times G_j \to G_i \times G_i$ be the continuous map taking (g_i, g_j) to $(g_i, f_{ij}(g_j))$. Then,

$$\{(g_i, g_j) \in G_i \times G_j : f_{ij}(g_j) = g_i\} = (Id \times f_{ji})^{-1}(\Delta).$$

Since G_i is Hausdorff Δ is closed in $G_i \times G_i$ and thus so is $\{(g_i, g_j) \in G_i \times G_j : f_{ij}(g_j) = g_i\}$. □

Corollary 4.9.6. *Let $(\{G_i\}, \{f_{ij} : G_j \to G_i\}_{i \leq j})$ be an inverse system of finite groups, made into topological groups by the discrete topology on each G_i. Then $G = \varprojlim_{i \in I} G_i$ is a compact Hausdorff topological group. G has a local basis of open sets at the identity consisting of normal open subgroups of finite index in G.*

Proof. Since the product of Hausdorff spaces is Hausdorff and a subspace of a Hausdorff space is Hausdoff, G is Hausdorff. By Tychonoff's theorem $\prod G_i$ is a compact Hausdorff space. Since G is a closed subset of a compact space, G is compact too. Finally, any open subset of $\prod G_i$ containing the identity contains an open set V of the form

$$V = \prod_{i \in I_0} U_i \times \prod_{i \notin I_0} G_i,$$

for some finite subset I_0 of I and where the U_i are open in G_i. Note that $1_{G_i} \in U_i$. Since $\{1_{G_i}\}$ is itself on open subset of G_i, we see that this set contains the open set

$$U = \prod_{i \in I_0} \{1_{G_i}\} \times \prod_{i \notin I_0} G_i,$$

which is a normal subgroup of $\prod G_i$ of finite index $\prod_{i \in I_0} |G_i|$. As the open sets in G are of the form $V \cap G$ and this contains $U \cap G$, which is a normal subgroup of G of finite index, the proof is complete. □

5. Infinite Galois theory

5.1. **A quick review of Galois theorey of finite extensions.**

§ Recall

A polynomial $f(x) \in \mathbb{F}[x]$ is separable if it has distinct roots, equivalently $(f(x), f'(x)) = 1$.

A field $\mathbb{F}$ is perfect if it either has char. 0, or it has char. p and $x \to x^p$ is surjective.

An irreducible polynomial over a perfect field is separable.

Splitting fields: Let $f(x) \in \mathbb{F}[x]$. A splitting field for f is a field $L \supseteq \mathbb{F}$ in which $f(x) = c \cdot \prod_{i=1}^{n} (x - \alpha_i)$, $\alpha_i \in L$ and $L = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$. A basic result is that any two splitting fields for f are isomorphic. In fact, if $\sigma : \mathbb{F} \xrightarrow{\sim} \mathbb{F}'$ taking f to $\tilde{f}$ and L (resp. $\tilde{L}$) is a splitting field for f (resp. $\tilde{f}$) then there's an isomorphism

$$L \xrightarrow{\tilde{\sigma}}_{\sim} \tilde{L}$$

s.t. $\tilde{\sigma}\big|_{\mathbb{F}} = \sigma$. The key is the following: if f is irreducible, $\alpha \in L$ is a root then $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/(f(x))$. The proof of (*) is done inductively and is useful for calculating Galois groups.

An algebraic extension $K/\mathbb{F}$ (every elt of K solves some non-zero $f(x) \in \mathbb{F}[x]$) is called a normal extension if it's the splitting field for a collection of polynomials $\{f(x)\} \subseteq \mathbb{F}[x]$. (They split in K and the roots generate K over $\mathbb{F}$).

It's a theorem that if $K/\mathbb{F}$ is normal, $f(x) \in \mathbb{F}[x]$ is irreducible and has a root in K then it splits in K.

An algebraic extension $K/\mathbb{F}$ is called separable if every element of K is a root of a separable polynomial in $\mathbb{F}[x]$.

Automorphisms:

Let K/F be a field extension. We define

$$\mathrm{Aut}(K/F) = \{\sigma : K \to K \text{ a field automor. s.t. } \sigma|_F = id\}.$$

Assume until further notice that K/F is a finite extension. We have the basic

Theorem: $|\mathrm{Aut}(K/F)| \leq [K:F]$ with equality iff K is the splitting field of a separable polynomial (equiv., a collection of separable polynomials).

We call such an extension a Galois extension and use $\mathrm{Gal}(K/F)$ for $\mathrm{Aut}(K/F)$.

Theorem: TFAE for K/F a finite extension.

(i) K/F is Galois, i.e., $\#\mathrm{Aut}(K/F) = [K:F]$;

(ii) $F = K^{\mathrm{Aut}(K/F)} = \{k \in K : \sigma(k) = k, \ \forall \sigma \in \mathrm{Aut}(K/F)\}$.

(iii) K = splitting field of a separable polynomial $f(x) \in F[x]$.

(iv) K/F is a normal, separable extension.

A key example: Let K/F be any extension of fields and $G \subseteq \mathrm{Aut}(K/F)$ a finite group. Then K/K^G is a Galois extension with Galois group G.

In general, we have two maps for an extension K/F:

$$G \subseteq \mathrm{Aut}(K/F) \longmapsto K^G = \{k \in K : \sigma(k) = k, \ \forall \sigma \in G\}$$

$$K \supseteq L \supseteq F \longmapsto G_L = \{\sigma \in \mathrm{Aut}(K/F) : \sigma|_L = id\}$$

We have $G_{K^G} \supseteq G$, $K^{G_L} \supseteq L$, but only for K/F Galois these are inverse correspondences.

The main theorem of Galois theory:

Let K/F be a finite Galois extension, $G = \mathrm{Gal}(K/F)$. There's a bijection

$$\{\text{subfields } K \supset L \supset F\} \longleftrightarrow \{\text{subgroups } H \subseteq G\}$$

$L \longmapsto \mathrm{Aut}(K/L)$

$K^H \longleftarrow H$

These maps are mutual inverses.

(1) $H_1 \subseteq H_2 \longrightarrow K^{H_1} \supseteq K^{H_2}$, $K_1 \supseteq K_2 \Longrightarrow \mathrm{Aut}(K/K_1) \subseteq \mathrm{Aut}(K/K_2)$.

(2) $[K:K^H] = \#H$, $[K^H : F] = [G:H]$.

(3) K/L is Galois with Galois group H if $L = K^H$.

(4) $L = K^H$ is Galois over F if and only if H is normal in G. Then $\mathrm{Gal}(L/F) = G/H$.

(5) $K^{H_1} \cap K^{H_2} = K^{\langle H_1, H_2 \rangle}$, $K^{H_1} \cdot K^{H_2} = K^{H_1 \cap H_2}$.

Some very useful propositions:

* Let K_i/F be Galois extensions (with $G_i = \mathrm{Gal}(K_i/F)$) contained in some extension L/F. Then $K_1 \cap K_2$ and $K_1 K_2$ are Galois extensions and

$$\mathrm{Gal}(K_1K_2/F) = \left\{ (\sigma, \tau) \in G_1 \times G_2 : \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2} \right\}$$

* Let K/F be Galois and F'/F (s.t. $K, F' \subseteq L$ any extension!) Then KF'/F' is Galois and $\mathrm{Gal}(KF'/F') = \mathrm{Gal}(K/K \cap F')$.

5.2. **First definitions.** Let $K/\mathbb{F}$ be an algebraic extension. We that that $K/\mathbb{F}$ is **Galois** if it is a separable and normal extension. That is, every $k \in K$ solves a separable non-zero polynomial $f(x) \in \mathbb{F}[x]$ and any irreducible polynomial $f(x) \in \mathbb{F}[x]$ that has a root in K splits over K.

Lemma 5.2.1. *$K/\mathbb{F}$ is Galois if and only if $K = \cup L$, the union being over all finite Galois extensions $L/\mathbb{F}$ contained in K.*

Proof. Suppose that $K = \cup L$, the union being over all finite Galois extensions $L/\mathbb{F}$ contained in K. Let $k \in K$. Then $k \in L$ for some $L/\mathbb{F}$ a finite Galois sub extension of K. Thus, k solves a separable non-zero polynomial over $\mathbb{F}$. That shows that $K/\mathbb{F}$ is separable. Given $f(x) \in \mathbb{F}[x]$ an irreducible polynomial that has a root $k \in K$. Take again $L/\mathbb{F}$ finite Galois sub extension such that $k \in L$. Then $f(x)$ splits over L, hence over K.

Conversely, let $K/\mathbb{F}$ be Galois. For each $k \in K$ choose a separable polynomial $f_k(x)$ that k satisfies. Since a factor of a separable polynomial is separable and k is a root of one of the factors of $f_k(x)$ we may as well assume that $f(x)$ is irreducible. Let L_k be the splitting field of $f(x)$ in K. Then $k \in L_k$, $L_k/\mathbb{F}$ is a Galois extension and so $K = \cup_{k \in K} L_k$, which gives $K = \cup L$, the union being over all finite Galois extensions $L/\mathbb{F}$ contained in K. □

Corollary 5.2.2. *$K/\mathbb{F}$ is Galois if and only if K is the splitting field of a collection of separable polynomials $\{f_\alpha(x) : \alpha \in I\}$ of $\mathbb{F}[x]$.*

Proof. Suppose that $k/\mathbb{F}$ is Galois. For every $k \in K$ choose an irreducible polynomial that k solves. Then, as we saw, K is the union of the splitting fields of the polynomials $\{f_k(x) : k \in K\}$, which is a collection of separable polynomials over $\mathbb{F}[x]$.

Conversely, suppose that K is the splitting field of a collection of separable polynomials $\{f_\alpha(x) : \alpha \in I\}$ of $\mathbb{F}[x]$. For every finite subset $J \subset I$ let L_J be the splitting field in K of the polynomials $\{f_j(x) : j \in J\}$. Then $L_J/\mathbb{F}$ is a finite Galois extension and $K = \cup_{J \subset I, J \text{ finite}} L_J$, hence $K/\mathbb{F}$ is Galois. □

Let $K/\mathbb{F}$ be a Galois extension. Let

$$I = \{L : K \supseteq L \supseteq \mathbb{F}, L/\mathbb{F} \text{ finite Galois}\}.$$

Then I is a poset where we say that $L \leq L'$ if $L \subseteq L'$. Further, I is *directed*, because given L_1, L_2 in I, the compositum $L1L_2$ is a subfield of K which is also a finite Galois extension of $\mathbb{F}$. Thus, $L_1L_2 \in I$ and $L_i \leq L_1L_2$. We note that

$$K = \varinjlim_{L \in I} L.$$

If $L_{\supseteq} L_2 \supseteq \mathbb{F}$ are Galois, we know from Galois theory that we have surjective group homomorphism

$$\text{res}_{L_1,L_2} : \text{Gal}(L_1/\mathbb{F}) \to \text{Gal}(L_2/\mathbb{F}), \qquad \sigma \mapsto \sigma|_{L_2},$$

the kernel of which is $\text{Gal}(L_1/L_2)$. Let

$$G = \varprojlim_{L \in I} \text{Gal}(L/\mathbb{F}),$$

the limit taken over all finite Galois extensions $L/\mathbb{F}$ relative to the homomorphisms res_{L_1,L_2}.

Theorem 5.2.3. $G \cong \text{Aut}(K/\mathbb{F})$.

Proof. Recall that G was defined as a subgroup of $\prod_{L \in I} \text{Gal}(L/\mathbb{F})$,

$$G = \{(\sigma_L)_L : L_1 \supseteq L_1 \Rightarrow \sigma_{L_1}|_{L_2} = \sigma_{L_2}\}.$$

Given $\sigma \in K$, σ induces an automorphism of every finite Galois extension $L/\mathbb{F}$. Indeed, if $L/\mathbb{F}$ is the splitting field of a polynomial $f(x) \in \mathbb{F}[x]$ then $\sigma(L)$ is the splitting field of the polynomial $\sigma(f)$, obtained from f by applying σ to its coefficients. But, $\sigma(f) = f$ and so $\sigma(L) = L$. Therefore,

we have $\sigma_L := \sigma|_L \in \mathrm{Gal}(L/\mathbb{F})$ for all $L/\mathbb{F}$ finite Galois. Clearly $\sigma_{L_1}|_{L_2} = \sigma_{L_2}$. This gives a group homomorphism $\mathrm{Aut}(K/\mathbb{F}) \to G$.

Conversely, let $(\sigma_L)_L \in G$. Define $\sigma \in \mathrm{Aut}(K/\mathbb{F})$ as follows. Given $k \in K$ choose a finite Galois extension L such that $k \in L$. Let

$$\sigma(k) := \sigma_L(k).$$

This is well-defined. If $k \in L_1 \cap L_2$ then

$$\sigma_{L_1}(k) = \sigma_{L_1 \cap L_2}(k) = \sigma_{L_2}(k).$$

Finally, given $k_1, k_2 \in K$, there are Galois extensions L_i such that $k_i \in L_i$. Then k_1, k_2 are both in $L = L_1 L_2$. We then calculate that $\sigma(k_1 * k_2) = \sigma_L(k_1 * k_2) = \sigma_L(k_1) * \sigma_L(k_2) = \sigma(k_1) * \sigma(k_2)$, where $*$ stands for either $+$ or $\times$. Thus, σ is a homomorphism of fields. Finally, since $K = \cup_{L \in I} L$, $\sigma(K) = \cup_{L \in I} \sigma(L) = \cup_{L \in I} L = K$, where we have used that for every $L/\mathbb{F}$ finite Galois $\sigma(L) = L$. Thus, $\sigma \in \mathrm{Aut}(K/\mathbb{F})$. It is also easily checked that this is the inverse function to the homomorphism constructed in the first part of the proof. Thus, we have constructed an isomorphism between the groups. □

As usual, if $K/\mathbb{F}$ is a Galois extension, we shall denote

$$\mathrm{Gal}(K/\mathbb{F}) := \mathrm{Aut}(K/\mathbb{F}).$$

A group G is called a **profinite group** if $G \cong \varprojlim_{i \in I} (\{G_i\}_{i \in I}, \{f_{ij} : G_j \to G_i\})$, where

(1) I is a directed index set;
(2) G_i if a finite group;
(3) all given group homomorphisms f_{ij} are surjective.

The group $\mathrm{Gal}(K/\mathbb{F})$ is a profinite group. If G is a profinite group then, since each G_i is compact Hausdorff, G is a closed subset of the compact topological space $\prod_{i \in I} G_i$ and so G is compact Hausdorff as well (Corollary 4.9.6). The following proposition shows that pro finite groups have a topology which is very well controlled and that will be very useful in our discussion of infinite Galois extensions.

Before that, we discuss some properties of general topological groups G. For such a group, and an element $g \in G$ we have a function

$$[g] : G \to G, \qquad [g](x) = gx.$$

This is a continuous function: let $m : G \to G$ be the multiplication map and $U \subset G$ an open subset, then $\{g\} \times [g]^{-1}(U) \cong m^{-1}(U) \cap \{g\} \times G$. Since $\{g\} \times G$ is homeomorphic to G, we get that $[g]^{-1}(U)$ is open.

Further, $[g]$ is a homeomorphism because $[g^{-1}]$ is its inverse. We see that a topological group is a **homogenous space** - for every $x, y \in G$ there is a homeomorphism $\varphi : G \to G$ such that $\varphi(x) = y$ (indeed, take $\varphi = [yx^{-1}]$).

Proposition 5.2.4. *Let $G = \varprojlim_{i \in I} (\{G_i\}_{i \in I}, \{f_{ij} : G_j \to G_i\})$ be a profinite group.*

(1) *For every finite subset $J \subset I$ define*

$$G_J = \left(\prod_{j \in J} \{1_{G_j}\} \times \prod_{i \notin J} G_i \right) \cap G.$$

Then G_j is a normal subgroup of G of finite index. Further, G_J is open.

(2) *Let U be an open subset of G containing the identity element 1_G. Then $U \supset G_J$ for some J. Every open subset of G is a union of cosets of the subgroups G_J. If U is a subgroup then U has finite index.*
(3) *Every open subgroup of G has finite index and is closed.*
(4) *Every closed subgroup of G of finite index is open.*
(5) *The intersection of open subgroups is a closed subgroup. Every closed subgroup is the intersection of open subgroups.*
(6) *G is totally disconnected. Namely, every set with more than 1 element is not connected.*

Proof. We observe that $\prod_{j\in J}\{1_{G_j}\}\times\prod_{i\notin J}G_i$ is a normal subgroup of G. It is open, because, due to the discrete topology on each G_j, $\{1_{G_j}\}$ is an open subset of G_j. It is of finite index, equals in fact to $\prod_{j\in J}|G_j|$. Thus, G_J is a normal open subgroup of G of finite index.

Let U be now an open subset of G such that $1_G\in U$. Write $U=V\cap G$ where V is open in $\prod_{i\in I}G_i$. We have $1_G\in V$ and so, since V is open, by the definition of the product topology, for some finite subset $J\subset I$ we have

$$1\in\prod_{j\in J}V_j\times\prod_{i\notin J}G_i\subseteq V.$$

Necessarily, $1_{G_j}\in V_j$ and so

$$\prod_{j\in J}\{1_{G_j}\}\times\prod_{i\notin J}G_i\subseteq V,$$

and it follows that $G_J\subset U$.

Let U be any open subset of G. For every $x\in U$ choose a group $G_{J(x)}\subset[x^{-1}](U)$, where $J(x)\subset I$ is a suitable finite subset. Then $U=\cup_{x\in U}[x](G_{J(x)})=\cup_{x\in U}x\cdot G_{J(x)}$ is a union of cosets of groups G_J.

Finally, if U is an open subgroup then $U\supseteq G_J$ for some J. Since G_J has finite index in G, so does U. That concludes the proof of (2).

For (3), we have just seen that U has finite index. Since $G-U=\cup_{x\notin U}xU$ and each xU is open, it follows that $G-U$ is open and so U is closed. Similarly, if U is a closed subgroup of finite index, the union $\cup_{x\notin U}xU$ is really a union of finitely many closed subsets and so is closed; it follows that U is open. This proves (4).

Let U_α be a collection of open subgroups. Then, each U_a is closed and so the subgroup $\cap_\alpha U_\alpha$ is closed. Conversely, let H be a closed subgroup. Consider the sets HG_J. Since G_J is a normal subgroup of G, HG_J is a subgroup of G. Since $HG_J=\cup_{h\in H}hG_J$, it follows that HG_J is an open subgroup. We claim that

$$H=\cap_{J\subset I,\ \text{finite}}HG_J.$$

The inclusion $\subseteq$ is clear. Suppose then that $x\notin H$. We shall show x is not in the right hand side. Since $x\notin H$, $1_G\notin Hx=H^{-1}x$. Since Hx is closed, $G-Hx$ is open and so there is some finite set $J\subset I$ such that

$$1_G\in G_J,\qquad G_J\cap H^{-1}x=\emptyset.$$

It follows that $x\notin HG_J$. Indeed, if $x=hg$ then $h^{-1}x=g\in H^{-1}x\cap G$, which is contradiction.

Finally, to prove (6) let U be an open set and $x\neq y$ elements of U. Let $G_J\subset x^{-1}U$. By adding to J an index j for which that j-th component of $x^{-1}y$ is not 1_{G_j}, we may assume $x^{-1}y\notin G_J$. And so xG_J is an open subset of U to which y does not belong. But xG_J is also open. It follows that U is disconnected. □

5.3. **The main theorem of Galois theory.**

Theorem 5.3.1. *Let $K/\mathbb{F}$ be a Galois extension, $G = \mathrm{Gal}(K/\mathbb{F})$. There is an inclusion-reversing bijection*

$$\left\{ \begin{matrix} K \supseteq M \supseteq \mathbb{F} \\ M \text{ any subfield} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} H \subseteq G \\ H \text{ a closed subgroup} \end{matrix} \right\},$$

under which

$$M \mapsto H_M := \{\sigma \in G : \sigma|_M = \mathrm{Id}\}$$

and

$$H \mapsto K^H = \{k \in K : \sigma(k) = k, \forall \sigma \in H\}.$$

Furthermore:

(1) *M is a finite extension of $\mathbb{F}$ if and only if H_M is an open subgroup.*
(2) *K/M is a Galois extension with Galois group H_M.*
(3) *$M/\mathbb{F}$ is Galois if and only if $H_M \lhd G$, in which case $\mathrm{Gal}(M/\mathbb{F}) = G/H_M$.*
(4) *Let M_1, M_2 be subfields. Then $M_1 \cap M_2$ corresponds to $\langle H_{M_1}, H_{M_2}\rangle^c$ and $M_1 M_2$ corresponds to $H_{M_1} \cap H_{M_2}$, where here ^{c} stands for taking the closure.*

Before the proof proper, let us make a remark about the topology of G. By the general theory a basis at the identity for the topology of G is given as follows: pick $L_1, \ldots, L_r$ finite Galois extensions of $\mathbb{F}$ and let

$$G_{\{L_1,\ldots,L_r\}} = \{(\sigma_L)_L : \sigma_{L_i} = \mathrm{Id}, i = 1, \ldots, r\} = \{\sigma \in \mathrm{Aut}(K/F) : \sigma|_{L_i} = \mathrm{Id}, i = 1, \ldots, r\}.$$

Then $G_{L_1,\ldots,L_r}$ is an open subgroup and these subgroups form a local basis at 1. But, let $L = L_1 L_2 \ldots L_r$, the compositum of the fields L_i. Then $L/\mathbb{F}$ is a Galois extension and the condition $\sigma|_{L_i} = \mathrm{Id}, i = 1, \ldots,$ is equivalent to the condition $\sigma|_L = \mathrm{Id}$. Thus, we have a simplified description of a local basis at the identity. It consists of all subgroups of the form

$$G_{\{L\}} = \{\sigma \in \mathrm{Aut}(K/F) : \sigma|_L\},$$

where L runs over all *finite, Galois* extensions of $\mathbb{F}$ contained in K.

Proof. We first check that the correspondence is well-defined. Clearly, K^H is a subfield of K that contains $\mathbb{F}$ and H_M a subgroup of G.. We need to show that H_M is a *closed* subgroup of G. Before that, note that K/M is the splitting field of the same collection of separable polynomials of $\mathbb{F}[x]$ that shows $K/\mathbb{F}$ is Galois. Thus, K/M is Galois and

$$\begin{aligned} \mathrm{Gal}(K/M) &= \{\sigma \in Aut(K) : \sigma|_M = \mathrm{Id}\} \\ &= \{\sigma \in \mathrm{Aut}(K/\mathbb{F}); \sigma|_m = \mathrm{Id}\} \\ &= H_M. \end{aligned}$$

Let $\sigma \in G - H_M = G - \mathrm{Gal}(K/M)$. We need to show that there is an open set $U \subset G$ such that $\sigma \in U$ and $U \cap \mathrm{Gal}(K/M) = \emptyset$. It is enough (and, essentially, necessary) to find some finite Galois extension $L/\mathbb{F}$ such that

$$\sigma \cdot G_{\{L\}} \cap \mathrm{Gal}(K/M) = \sigma \cdot \mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/M) = \emptyset.$$

Now, since $\sigma \notin \mathrm{Gal}(K/M)$, there is an element $m \in M$ such that $\sigma(m) \neq m$. Let $f_m(x)$ be the minimal polynomial of m over $\mathbb{F}$. It is a separable polynomial and its splitting field L over $\mathbb{F}$ is a finite Galois extension, and $m \in L$. Let $\tau \in \mathrm{Gal}(K/L)$ then

$$\sigma\tau(m) = \sigma(m) \neq m.$$

That shows that $\sigma \cdot \mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/M) = \emptyset$. Thus, we have proved the the correspondence is well-defined. It is also clear from the definition that it is inclusion reversing. The next step is to check that the maps

$$M \mapsto H_M, \quad H \mapsto K^H,$$

are mutual inverses.

Clearly $M \subseteq K^{H_M}$. To show they are equal we will show that if $k \notin M$ then $\exists \sigma \in \mathrm{Aut}(K/M)$ such that $\sigma(k) \neq k$. That implies $k \notin K^H$.

First, let L be the splitting field over M of the minimal polynomial of k over $\mathbb{F}$. Then $L \supsetneqq M$, L/M is Galois and by finite Galois theory, $\exists \sigma \in \mathrm{Gal}(L/M)$ such that $\sigma(k) \neq k$. If we can extend σ to an automorphism $\tilde{\sigma} : K \to K$, we are done. This follows immediately from the following Lemma.

Lemma 5.3.2. *Let L be a subfield of K and $\sigma : L \to L$ a field automorphism, then $\exists \sigma \in \mathrm{Aut}(K)$ such that the following diagram commutes*

$$\begin{array}{ccc} K & \xrightarrow{\tilde{\sigma}} & K \\ \uparrow & & \uparrow \\ L & \xrightarrow{\sigma} & L \end{array}$$

Proof. (of Lemma) Let

$$\Sigma = \{(L_1, \sigma_1) : \sigma_1 : L_1 \to L_1 \text{ an automorphism}, L_1 \supseteq L, \sigma_1|_L = \sigma\}.$$

Note that Σ is not empty, because $(L, \sigma) \in \Sigma$, and is partially ordered under the relation

$$(L_1, \sigma_1) \leq (L_2, \sigma_2) \iff L_1 \subseteq L_2 \text{ and } \sigma_2|_{L_1} = \sigma_1.$$

Every chain $\{(L_\alpha, \sigma_\alpha)\}$ has a supremum in Σ. Indeed, let $L_0 = \cup_\alpha L_\alpha$. It is a field. One defines $\sigma_0; L_0 \to L_0$, by $\sigma_0(a) = \sigma_\alpha(a)$ if $a \in L_\alpha$. It is easy to check that σ_0 is a well defined field homomorphism. We have $\sigma_0(L_0) = \sigma_0(\cup_\alpha L_\alpha) = \cup_\alpha \sigma_0(L_\alpha) = \cup_\alpha \sigma_\alpha(L_\alpha) = \cup_\alpha L_\alpha = L_0$.

By Zorn's lemma, Σ has a maximal element (L_1, σ_1). We claim that $L_1 = K$ (and so the lemma is proved). If not, let $k \in K - L_1$. Let L_2 be the splitting field over L_1 of the minimal polynomial f of k over $\mathbb{F}$. Then, by finite Galois theory (using that σ_1 acts trivially on the coefficients of f), there is an automorphism $\sigma_2 : L_2 \to L_2$ such that the diagram is commutative:

$$\begin{array}{ccc} L_2 & \xrightarrow{\sigma_2} & L_2 \\ \uparrow & & \uparrow \\ L_1 & \xrightarrow{\sigma_1} & L_1 \end{array}$$

Thus,

$$(L_1, \sigma_1) \lneqq (L_2, \sigma_2),$$

and that is a contradiction. □

Having proven that $M = K^{H_M}$, let's prove that

$$H_{K^H} = H.$$

Again, one inclusion is clear: $H_{K^H} \supseteq H$. Let L/K^H be a finite Galois extension. The restriction map

$$\mathrm{Gal}(K/K^H) \to \mathrm{Gal}(L/K^H), \sigma \mapsto \sigma|_L,$$

is a well-defined homomorphism (surjective, by the Lemma). Also, for every such L, the restriction map

$$H \to \mathrm{Gal}(L/K^H), \qquad \sigma \mapsto \sigma|_L,$$

is a well-defined homomorphism. As $L^{\mathrm{Im}(H)} = L \cap K^H = K^H$, by finite Galois theory $\mathrm{Im}(H) = \mathrm{Gal}(L/K^H)$. That is, $H \to \mathrm{Gal}(L/K^H)$ is surjective homomorphism, too.

Suppose that there is an automorphism $\sigma \in \mathrm{Gal}(K/K^H)$ and $\sigma \notin H$. Since H is closed, there exists a finite Galois extension $L_1/\mathbb{F}$ such that $\sigma \cdot \mathrm{Gal}(K/L_1) \cap H = \emptyset$. The extension L/K^H, where $L = L_1K^H$ is a finite Galois extension, and σ being an automorphism of K/K^H induces an automorphism $\sigma|_L$ of L/K^H. By what we had shown above, there is $\tau \in H$ such that

$$\sigma|_L = \tau|_L.$$

But this implies that $\sigma^{-1}\tau|_L = \mathrm{Id}$, so $\sigma^{-1}\tau \in \mathrm{Gal}(K/L_1)$ and so $\tau \in \sigma\mathrm{Gal}(K/L_1)$. Contradiction.

At this point in the proof we have established that $M \mapsto H_M$ and $H \mapsto K^H$ are well-defined mutual inverses. We know that K/M is Galois and $H_M = \mathrm{Gal}(K/M)$.

Suppose that $M/\mathbb{F}$ is a finite extension. Let L be the normal closure of M in K. Then $L/\mathbb{F}$ is a finite Galois extension and $H_M \supseteq H_L = G_{\{L\}}$, which is an open subgroup. It follows that H_M is open too. Conversely, suppose that K is an open subgroup. Say $H = H_M$. Then $H_M \supseteq G_{\{L\}}$ for some $L/\mathbb{F}$ finite Galois extension. Then, $L \supseteq M \supseteq \mathbb{F}$ and so $M/\mathbb{F}$ is a finite extension.

Next, we note that the statement about $H_1 \cap H_2$ and $\langle H_1, H_2\rangle^c$f are a formal consequence, as $H_1 \cap H_2$ is the maximal subgroup contained in both in H_1 and H_2 and so $K^{H_1 \cap H_2}$ is the minimal field containing both K^{H_1} and K^{H_2}, etc.

We note that the Galois correspondence is equivariant in the following sense. G acts both on the set of subfields by $M \mapsto \sigma(M)$, which is another subfield of K containing $\mathbb{F}$. It acts on subgroups by $H \mapsto \sigma H \sigma^{-1}$, which is another closed subgroup of G. The equivariance property is

$$H_{\sigma(M)} = \sigma H_M \sigma^{-1}.$$

It follows that the fixed points of the action must correspondence under the Galois correspondence. On the level of subgroups, this is the collection of normal subgroups of G. On the level of subfields, we prove the following statement.[6]

Lemma 5.3.3. *Let M, $K \supseteq M \supseteq \mathbb{F}$, be a subfield. Then $M/\mathbb{F}$ is Galois if and only if $\sigma(M) = M$ for all $\sigma \in G$.*

Proof. (Of lemma) Suppose that $M/\mathbb{F}$ is Galois; say, M is the splitting field of a collection of separable polynomials $\{f_\alpha(x) \in \mathbb{F}[x]\}$. Let R be the set of roots of $\{f_\alpha(x)\}$ in K. Then, $M = \mathbb{F}(R)$. If $\sigma \in G$ then $\sigma(R) = R$ and so $\sigma(M) = M$.

Suppose, conversely, that $\sigma(M) = M$ for all $\sigma \in G$. Let $m \in M$ and let $f_m(x)$ be the minimal polynomial of m over $\mathbb{F}[x]$. Let m' be another root of $f_m(x)$. We have the following diagram for some field isomorphism $\sigma : \mathbb{F}(m) \to \mathbb{F}(m')$, such that $\sigma(m) = m'$.

$$\begin{array}{ccc} \mathbb{F}(m) & \xrightarrow{\sigma} & \mathbb{F}(m') \\ \uparrow & & \uparrow \\ \mathbb{F} & \xrightarrow{\mathrm{Id}} & \mathbb{F} \end{array}$$

Extend σ to an element (still denoted σ) of G, using Lemma 5.3.2. As $\sigma(M) = M$ it follows that $\sigma(m) = m'$, $m' \in M$ too. If follows that M is the splitting field of the collection of separable polynomials $\{f_m(x) : m \in M\}$ of $\mathbb{F}[x]$ and so $M/\mathbb{F}$ is Galois. □

[6] We have in fact used this lemma above more than once of finite Galois extensions, since we allowed ourselves to assume finite Galois theory. But, in fact, the proof here is self-contained and proves the case of finite Galois extensions as well.

Finally, suppose that $M/\mathbb{F}$ is Galois. There is a injective homomorphism

$$G/H_M \to \mathrm{Gal}(M/\mathbb{F}), \qquad \sigma \mapsto \sigma|_M.$$

Lemma 5.3.2 shows this is a surjective homomorphism. The proof of the theorem is complete. □

5.4. $\mathbb{Z}_p$**.** The ring of p-**adic integers** $\mathbb{Z}_p$ can be defined in several ways. We first approach it as an inverse limit, in concert with the construction of infinite Galois extensions. Thus, for us,

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z},$$

relative to the transition maps

$$\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}, \quad x \pmod{p^n} \mapsto x \pmod{p^m}, \qquad m \leq n.$$

Thus $\mathbb{Z}_p$ is a profinite group, compact and Hausdorf in particular. In fact, since the transition maps are ring homomorphisms (continuous for the discrete topology, of course), $\mathbb{Z}_p$ is a **topological ring**. Namely, the multiplication map is continuous too. We have a hands-on description of $\mathbb{Z}_p$ as

$$\{(,\dots,x_3,x_2,x_1) : x_i \in \mathbb{Z}/p^i\mathbb{Z}, x_{i+1} \equiv x_i \pmod{p^i}, i = 1,2,3,\dots\}.$$

In this notation, addition and multiplication are done component-wise. Recalling the basis for the topology of a profinite group at the identity, we see that for $\mathbb{Z}_p$ a basis for the topology at 0 are the subgroups of finite index

$$\begin{aligned} I_n &= \{(x_i)_i \in \mathbb{Z}_p : x_n \equiv 0 \pmod{p^n}\} \\ &= \{(\dots,x_{n+1},0,\dots,0,0) : x_{i+1} \equiv x_i \pmod{p^i}\}. \end{aligned}$$

Lemma 5.4.1. *The map*

$$\mathbb{Z} \to \mathbb{Z}_p, \qquad a \mapsto \underline{a} = (\dots,a,a,a),$$

is an injective ring homomorphism. The image of $\mathbb{Z}$ is dense. $\mathbb{Z}_p$ is an integral domain.

Proof. First, note that $\underline{a}$ is indeed in $\mathbb{Z}_p$. The definitions give immediately that this is a ring homomorphism. If a is in the kernel then $\underline{a} = 0$, which means that the n coordinate is zero for every n, that is, $a \equiv 0 \pmod{p^n}$ for every n and so $a = 0$.

To show the image is dense, we need to show that given $x = (\dots,x_2,x_1) \in \mathbb{Z}_p$ and n, there is $a \in \mathbb{Z}$ such that $\underline{a} \in x + I_n$. But that just means that $\underline{a} - x = (\dots,a-x_3,a-x_2,a-x_1) \in I_n$. Therefore, we only need to choose some $a \in \mathbb{Z}$ such that $a \equiv x_n \pmod{p^n}$.

If $x,y \in \mathbb{Z}_p$ and $xy = 0$ and, say $x \neq 0$, then for some n, $x_n \not\equiv 0 \mod p^n$. For every N then $x_{n+N} \not\equiv 0 \mod p^n$. Since $x_{n+N}y_{n+N} \equiv 0 \pmod{p^{n+N}}$ we get that $y_{n+N} \equiv 0 \pmod{p)^{N+1}}$. Given now any i, choose $N \geq i-1$ to get $y_{n+N} \equiv 0 \pmod{p^i}$ and so that $y_i \equiv 0 \pmod{p^i}$. It follows that $y = 0$. □

Proposition 5.4.2. *The subgroups I_n are principal ideals and*

$$I_n = p^n\mathbb{Z}_p.$$

We have

$$\mathbb{Z}_p/I_n \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Every closed subgroup of $\mathbb{Z}_p$ is equal to some I_n and, in particular, open of finite index.

Proof. Suppose S is a dense set of a topological space X and U is a subset of X which is open and close, then U is equal to the closure C of $U \cap S$. Indeed, C is contained in U because U is closed. On the other hand, if there is an element $x \in U - C$, then in the open subset $U - C$ there is no element of S, and that contradicts the fact that S is dense. Thus, $U = C$.

Apply that to I_n which is open, hence closed, and to the set $\mathbb{Z}$. The intersection $\mathbb{Z} \cap I_n = p^n\mathbb{Z}$, clearly. Its closure is $p^n\mathbb{Z}_p$: on the one hand, because multiplication by p^n is continuous and $\mathbb{Z}_p$ is compact Hausdorff, $p^n\mathbb{Z}_p$ is closed. On the other hand, if $C \subset p^n\mathbb{Z}_p$ is closed and contains $\mathbb{Z}$ then $p^{-n}C$ is well defined, closed and contains $\mathbb{Z}$. Thus, $p^{-n}C = \mathbb{Z}_p$.

We can also show more directly that I_n is equal to $p^n\mathbb{Z}_p$. On the one hand, it is clear from the definition that I_n is an ideal and that $p^n \in I_n$ and so that $I_n \supseteq p^n\mathbb{Z}_p$. On the other hand,

let $x = (\dots, x_{n+1}, 0, \dots, 0, 0) \in I_n$. For every m define an element y_m as follows. The element $x_{n+m} \in \mathbb{Z}/p^{m+n}\mathbb{Z}$ is congruent to zero modulo p^n and so, there is an element $\tilde{y}_m \in \mathbb{Z}/p^{m+n}\mathbb{Z}$ such that $p^n\tilde{y}_m = x_{n+m}$. Let

$$y_m = \tilde{y}_m \pmod{p^m}.$$

We claim that $y = (\dots, y_2, y_1) \in \mathbb{Z}_p$ and $p^n y = x$.

First, $y_{m+1} \pmod{p^m} = \tilde{y}_{m+1} \pmod{p^m}$ and $y_m \pmod{p^m} = \tilde{y}_m \pmod{p^m}$, so it's enough to show $\tilde{y}_{m+1} - \tilde{y}_m \equiv 0 \mod p^m$. Now, because $p^n\tilde{y}_{m+1} \equiv x_{n+m+1} \equiv x_{n+m} \equiv p^n\tilde{y}_m \pmod{p^{n+m}}$, it follows that $p^n(\tilde{y}_{m+1} - \tilde{y}_m) \equiv 0 \mod p^{m+n}$ and so that $\tilde{y}_{m+1} - \tilde{y}_m \equiv 0 \mod p^m$.

Secondly, the equation $p^n\tilde{y}_m \equiv x_{n+m} \pmod{p^{n+m}}$ gives upon reduction modulo p^m, $p^n y_m \equiv x_m \pmod{p^m}$, so $p^n y = x$.

We have a ring homomorphism

$$\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}, \quad x \mapsto x_n.$$

The kernel is clearly I_n. The map is surjective, because the composition $\mathbb{Z} \to \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ is surjective. Thus,

$$\mathbb{Z}_p/I_n \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Lemma 5.4.3. *The units of $\mathbb{Z}_p$ consist of the elements $x = (\dots, x_2, x_1)$ such that $x_1 \neq 0 \pmod p$.*

Proof. Clearly, if $xy = 1$ then $x_1y_1 = 1 \pmod p$ and so $x_1 \neq 0 \pmod p$. Conversely, suppose that $x_1 \neq 0 \pmod p$. Then, for every n, x_n is a unit in $\mathbb{Z}/p^n\mathbb{Z}$ (the non-units are $p\mathbb{Z}/p^n\mathbb{Z}$) because it is not zero modulo p. Thus, for every n there is a y_n such that $x_ny_n = 1 \pmod{p^n}$. We need only to check that $y_{n+1} \equiv y_n \pmod{p^n}$. But, $x_{n+1}y_{n+1} \equiv x_ny_{n+1} \equiv 1 \pmod{p^n}$ and so $y_{n+1} \equiv y_n \pmod{p^n}$ □

Let I be any closed subgroup of $\mathbb{Z}_p$. If $x \in I$ then $\mathbb{Z}x \subset I$ and so $\mathbb{Z}_px \subset I$, as I is closed. That is, I is an ideal. Suppose I is not zero and let $x = (\dots, x_2, x_1) \in I$ be a non-zero element. Let n be the maximal such that $x_n \equiv 0 \pmod{p^n}$. Then, as we saw, there is $y \in \mathbb{Z}_p$ such that $x_n = p^ny$. Since $x_{n+1} \not\equiv 0 \pmod{p^n+1}$, $y_{n+1} \not\equiv 0 \pmod p$, but $y_{n+1} \equiv y_1 \pmod p$. Therefore y is a unit. It follows that $xy^{-1} = p^n \in I$ and so $I \supseteq I_n$. However, the only ideals of $\mathbb{Z}_p/I_n = \mathbb{Z}/p^n\mathbb{Z}$ are the images of I_i for $i = 0, 1, \dots, n$ and so $I = I_n$ for some n. □

Corollary 5.4.4. *$\mathbb{Z}_p$ is a principal ideal domain which is a local ring. It has, up to a unit, a unique prime element, which is p.*

Proof. Let I be any non-zero ideal. As the proof above shows, if $x \in I$ and n is the maximum so that $x_n \equiv 0 \pmod{p^n}$ then we may write $x = p^ny$. Further, since $x_{n+1} \not\equiv 0 \pmod{p^{n+1}}$ it follows $p \nmid y_{n+1}$ and so $y_1 \not\equiv 0 \pmod p$. That is, y is a unit and hence $I \supseteq (x) = (p^n) = I_n$. It follows that $I = I_m$ for some $m \leq n$ (because I/I_n is an ideal of $\mathbb{Z}/p^n\mathbb{Z}$, as above). Thus, we have shown that every ideal of $\mathbb{Z}_p$ is one of the ideal I_n. Clearly $I = (p)$ is maximal. For $m > 1$, I_m is not prime because $\mathbb{Z}_p/I_m = \mathbb{Z}/p^m\mathbb{Z}$ is not an integral domain. If $x \neq 0$ then $(x) = I_m$ for some m and is not a prime element if $m > 1$. So it follows that there is a unique, up to a unit irreducible element, which we can choose to be p. □

Here is another approach to understanding $\mathbb{Z}_p$. Define a function

$$v : \mathbb{Z}_p \to \mathbb{Z}, \qquad v(x) = \max\{n : x_n \equiv 0 \pmod{p^n}\}.$$

(We formally put $v(0) = +\infty$.) This function is an example of a **discrete valuation** which means that it satisfies:

(1) $v(xy) = v(x)v(y)$;
(2) $v(x + y) \geq \min\{v(x), v(y)\}$.

Note that an equivalent way to define v is to use unique factorization and define

$$v(x) = n \quad \text{if} \quad x = p^n u, u \in \mathbb{Z}_p^\times.$$

At any rate, with this information it is easy to check that v has the said properties. Define now

$$d(x, y) = p^{-v(x-y)}.$$

One can then check that d is a metric. The topology d induces on $\mathbb{Z}_p$ agrees with the given topology. Indeed, the ideals I_n are none other then the closed balls of radius p^{-n}, which are the open balls of radius $p^{-(n-1)}$, around the origin. $\mathbb{Z}_p$ is thus a compact metric space, containing $\mathbb{Z}$ as a dense subset. It follows that $\mathbb{Z}_p$ can be viewed as the metric completion of $\mathbb{Z}$. Note that a sequence of integers $a(i)$ of $\mathbb{Z}$ converges to zero in $\mathbb{Z}_p$,

$$\underline{a}(i) \to 0 \ \Leftrightarrow \ v(\underline{a}(i)) \to +\infty,$$

that is if and only if the integers $a(i)$ become more and more divisibly by p. A concrete example is

$$p, p^2, p^3, \ldots \to 0.$$

Finally, let $\mathbb{Q}_p$ be the fraction field of $\mathbb{Z}_p$; it is called the field of p-adic numbers. We can extend v to $\mathbb{Q}_p$ by defining

$$v(a/b) = v(a) - v(b).$$

Properties (1), (2) above still hold and $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v(x) \geq 0\}$.

5.5. **Hensel's lemma.** Rings such as $\mathbb{Z}_p$ play a very important role in number theory. If a polynomial with integer coefficients has a solution in integers, then it has a solution in $\mathbb{Z}_p$ for every prime p (and in $\mathbb{R}$). The converse need not be true. Yet, a good first step is to examine whether that polynomial has indeed a solution in $\mathbb{Z}_p$ for all p and in $\mathbb{R}$. Although at first sight the ring $\mathbb{Z}_p$ looks much more complicated than $\mathbb{Z}$, it is in fact much easier to work with. A case in point in Hensel's lemma that goes a long way towards giving a definite answer as to when a polynomial has a solution in $\mathbb{Z}_p$.

Recall that we can identify the quotient $\mathbb{Z}_p/p\mathbb{Z}_p$ with $\mathbb{Z}/p\mathbb{Z}$. Given a polynomial $f(x) \in \mathbb{Z}_p[x]$ we can look at its reduction $\bar{f}(x)$ modulo p, namely, we reduce all the coefficients modulo p and so at the value $\bar{f}(a)$ for $a \in \mathbb{Z}_p$. However, to simplify notation we will simply write $f(a)$. Same for $a \in \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p/p^n\mathbb{Z}_p$.

Theorem 5.5.1. *(***Hensel's lemma***) Let $f(x) \in \mathbb{Z}_p[x]$ be a monic, non constant polynomial. Let $\alpha_1 \in \mathbb{Z}/p\mathbb{Z}$ be a simple root of $f(x)$, namely*

(1) $f(\alpha_1) = 0$;
(2) $f'(\alpha_1) \neq 0$.

(Both statement hold in $\mathbb{Z}/p\mathbb{Z}$.) Then, there exists a unique $\alpha \in \mathbb{Z}_p$ such that

(1) $f(\alpha) = 0$ *(in $\mathbb{Z}_p$);*
(2) $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$.

Proof. We prove by induction on n that for all n there exists $\alpha_n \in \mathbb{Z}/p^n\mathbb{Z}$ such that

$$f(\alpha_n) = 0 \pmod{p^n}, \qquad \alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}.$$

It then follows that $\alpha = (\ldots, \alpha_n, \ldots, \alpha_2, \alpha_1) \in \mathbb{Z}_p$ and $f(\alpha) = 0$.

For $n = 1$, α_1 is given. Assume that we have already constructed α_n with the desired properties. The binomial formula $(x + y)^n = x^n + nx^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + y^n$ gives

$$f(x + y) = f(x) + f'(x)y + g(x, y)y^2,$$

for some polynomial $g(x, y)$ with coefficients in $\mathbb{Z}_p$ if $f(x) \in \mathbb{Z}_p[x]$.

Now, choose any $\beta \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ such that $\beta \equiv \alpha_n \pmod{p^n}$. Any other choice is of the form $\beta+\gamma$, where $\gamma \in p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$. We have

$$f(\beta+\gamma) = f(\beta) + f'(\beta)\gamma + \gamma^2 g(\beta,\gamma).$$

As $\gamma^2 \equiv 0 \pmod{p^{2n}}$ and $g(\beta,\gamma) \in \mathbb{Z}_p$, we have

$$f(\beta+\gamma) = f(\beta) + f'(\beta)\gamma \pmod{p^{n+1}}.$$

Write $f(\beta) = p^n B, \gamma = p^n C$. We can choose γ so that $B + f'(\beta)C \equiv 0 \pmod{p}$, because modulo p we have $f'(\beta) \equiv f'(\alpha_1) \not\equiv 0 \pmod{p}$. For such γ we have $f(\beta+\gamma) \equiv 0 \pmod{p^{n+1}}$ and we let

$$\alpha_{n+1} = \beta + \gamma.$$

Examining the proof shows that γ is uniquely determined, because $f'(\beta) \not\equiv 0 \pmod{p}$. Thus, α_{n+1} is uniquely determined, and thus so is α. Arguing differently, we can say that if $f(x) = (x-\alpha)(x-\alpha')h(x)$, where $\alpha, \alpha' \in \mathbb{Z}_p$ and $\alpha \equiv \alpha' \pmod{p}$ then $f'(\alpha) \equiv 0 \pmod{p}$, that is $f'(\alpha_1) = 0 \pmod{p}$ and that's a contradiction. □

Example 5.5.2. $\mathbb{Z}_p$ contains the $p-1$-st roots of unity. Indeed, the polynomial $f(x) = x^p - x$ is separable modulo p. Pick any non-zero α_1 modulo p. Then $f(\alpha_1) = 0, f'(\alpha_1) \neq 0$. Let μ_1 be the solution of f in $\mathbb{Z}_p$ such that $\mu_1 \equiv \alpha_1 \pmod{p}$, as guaranteed by Hensel's lemma. We find that $f(x) = x\prod_{i=1}^{p-1}(x-\mu_i$ and the μ_i are $p-1$-st roots of unity that are distance (even after reduction modulo p).

It is difficult, perhaps impossible, to write these roots explicitly. Take for example α_2, the mod p^2 approximation to the modulo p root given by 2 to the polynomial $x^p - x$, where $p > 2$ is a prime. We know that $\alpha_2 = 2 + kp$. We also need that $(2+kp)^p \equiv 2 + kp \pmod{p^2}$ and this is equivalent to $k = \frac{2^p-2}{p}$. Here is a table of k that shows that its behaviour is erratic. The first prime for which $k = 0$ is 1093. This is relevant to Fermat's last theorem through the "Wieferich criterion".

prime	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
k	2	1	4	10	6	9	6	11	2	12	2	5	7	41	19	16

5.6. **Finite fields.** We summarize here the main facts about finite fields. Let $\mathbb{F} = \mathbb{F}_p$ be a finite field of p elements, where p is a prime. Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$.

Theorem 5.6.1. (1) *For every integer m, $\overline{\mathbb{F}}_p$ contains a unique subfield having p^m elements. We denote it by $\mathbb{F}_p^m$. The field $\mathbb{F}_{p^m}$ is the solutions in $\overline{\mathbb{F}}_p$ to the equation $x^{p^m} - x = 0$ and is therefore Galois over $\mathbb{F}_p$.*

(2) *We have $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^n}$ if and only if $m|n$. Every finite subfield of $\overline{\mathbb{F}}_p$ is $\mathbb{F}_{p^m}$ for some m. We have:*

$$\mathbb{F}_{p^{\gcd(m,n)}} = \mathbb{F}_{p^m} \cap \mathbb{F}_{p^n}, \qquad \mathbb{F}_{p^{\mathrm{lcm}(m,n)}} = \mathbb{F}_{p^m} \cdot \mathbb{F}_{p^n}.$$

(3) *Let $f(x) \in \mathbb{F}_{p^m}[x]$ be an irreducible polynomial of degree n and α a root of f in $\overline{\mathbb{F}}_p$ then*

$$\mathbb{F}_{p^m}(\alpha) = \mathbb{F}_{p^{nm}},$$

and it is the splitting field of f.

(4) *Let L be any field (not necessarily a subfield of $\overline{\mathbb{F}}_p$) with p^m elements, then $L \cong \mathbb{F}_{p^m}$.*

(5) *$\overline{\mathbb{F}}_p$ is the algebraic closure of any of the fields $\mathbb{F}_{p^m}$.*

(6) *Define the Frobenius map*

$$\mathrm{Fr}_p : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p, \qquad \mathrm{Fr}_p(x) = x^p.$$

Let

$$\mathrm{Fr}_{p^m} = \mathrm{Fr}_p \circ \cdots \circ \mathrm{Fr}_p \quad (m \text{ times}).$$

Then $\mathrm{Fr}_{p^m}(x) = x^{p^m}$ *and it is a field automorphism whose fixed points are the field* $\mathbb{F}_{p^m}$.

(7) $\overline{\mathbb{F}}_p = \cup_{m=1}^{\infty} \mathbb{F}_{p^m}$.

Let us now consider the situation from the point of view of infinite Galois theory. $\overline{\mathbb{F}}_p$ is an infinite Galois extension of $\mathbb{F}_p$. Its Galois group is

$$\varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

Where the order is $m \leq n$ if $m|n$, the identification $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$ is such that $\mathrm{Fr}_p \mapsto 1$, and the homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ are just $x \pmod n \mapsto x \pmod n$. This inverse limit is denoted $\hat{\mathbb{Z}}$. It is a compact Hausdorff topological ring and

$$\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}, \quad m \mapsto \mathrm{Fr}_{p^m}.$$

In fact, the image of $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$. We also have

$$\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p.$$

In particular, there is a surjection $\hat{\mathbb{Z}} \to \mathbb{Z}_p$ that shows that there is a Galois sub extension $K/\mathbb{F}_p$ of $\overline{\mathbb{F}}_p$ whose Galois group $\mathrm{Gal}(K/\mathbb{F}_p) \cong \mathbb{Z}_p$. It is not hard to construct this extension by hand.

For every n consider the Galois extension $\mathbb{F}_{p^{p^m}}/\mathbb{F}_p$ with Galois group $\mathbb{Z}/p^m\mathbb{Z}$. Let

$$k = \cup_{n=1}^{\infty} \mathbb{F}_{p^{p^m}}.$$

Then

$$\mathrm{Gal}(K/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/p^m\mathbb{Z} = \mathbb{Z}_p.$$

Since we know that closed subgroups of $\mathbb{Z}_p$ we see that the only proper subfields of K are the fields $\mathbb{F}_{p^{p^m}}$ and those are finite field extensions of $\mathbb{F}_p$.

One can prove that every closed subgroup of $\hat{\mathbb{Z}}$ is equal to a product $\prod_p H_p$, where H_p is a closed subgroup of $\mathbb{Z}_p$ (it is easy to show these are closed subgroups; for the converse one proves first that every closed subgroup is a product by showing first that every closed subgroup is an ideal and then making use of idempotents). Thus, with our knowledge of $\mathbb{Z}_p$ we can write down all the closed subgroups of $\hat{\mathbb{Z}}$ and hence all the subfields of $\overline{\mathbb{F}}_p$. Here is one concrete conclusion. There is no proper subfield L of $\overline{\mathbb{F}}_p$ such that $\overline{\mathbb{F}}_p/L$ is a finite extension.

5.7. **Cyclotomic fields.** Once more, since we assume that the reader had seen the example of cyclotomic fields before, we only summarize some of their key aspects.

Let μ_n denote that n-th roots of unity in $\mathbb{C}$.

$$\mu_n = \{\alpha \in \mathbb{C} : \alpha^n = 1\} = \{e^{a \cdot \frac{2\pi i}{n}} : a = 0, 1, \ldots, n-1\}.$$

The field $\mathbb{Q}(\mu_n)$ is the splitting field of $x^n - 1$. It is called a **cyclotomic field**. Note that $\mathbb{Z}/n\mathbb{Z} \cong \mu_n$ by $a \mapsto e^{a \cdot \frac{2\pi i}{n}}$. Consequently, an element $e^{a \cdot \frac{2\pi i}{n}}$ generates μ_n if and only if $(a, n) = 1$. Therefore μ_n has $\varphi(n)$ generators, where φ is **Euler's φ-function**. They are called **primitive roots** of order n. We also note that $\mu_d \subseteq \mu_n$ if and only if $d|n$. As a matter of notation, define

$$\zeta_n = e^{\frac{2\pi i}{n}}.$$

Define the n-th **cyclotomic polynomial** Φ_n by

$$\Phi_n(x) = \prod_{\zeta \in \mu_n \text{ primitive}} (x - \zeta).$$

Note that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

One proves that $\Phi_n(x) \in \mathbb{Z}[x]$ and is, of course, a monic polynomial of degree $\varphi(n)$.

A key fact is that $\Phi_n(x)$ is an irreducible polynomial over $\mathbb{Q}$, from that we deduce that $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is a Galois extension with Galois group of order $\varphi(n)$. Such an automorphism is determined by its action of ζ_n and must take it to ζ_n^a for some $(a, n) = 1$. This allows us to deduce that

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}), \qquad a \mapsto \{\zeta \mapsto \zeta^a\}.$$

Namely, the automorphism corresponding to a congruence class a is the one uniquely determined by the property that it acts on the n-th roots of unity by raising to a-th power.

Furthermore,

$$\mathbb{Q}(\mu_n) \cap \mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_{\gcd(m,n)}), \qquad \mathbb{Q}(\mu_n) \cdot \mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_{\mathrm{lcm}(m,n)}).$$

Let $K = \cup_n \mathbb{Q}(\mu_n)$. Then $K/\mathbb{Q}$ is a Galois extension and

$$\mathrm{Gal}(K/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times,$$

where the identification takes the element $a \in \mathbb{Z}/n\mathbb{Z}$ to the automorphism determined by $\zeta_n \mapsto \zeta_n^a$. This implies that the transition maps are

$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times, \quad x \pmod n \mapsto x \pmod m, \quad m|n.$$

This inverse limit is a bit complicated. Let $p > 2$ be a prime; we shall consider a sub Galois extension L of K,

$$L = \cup_n \mathbb{Q}(\mu_{p^n}).$$

We have

$$\mathrm{Gal}(L/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Now, at each level n we have an isomorphism

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

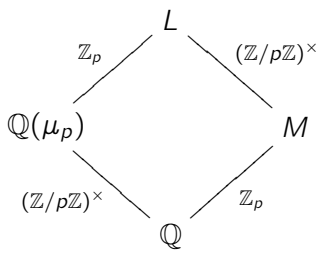
What matters to us is that the inclusion $\mathbb{Z}/p^{n-1}\mathbb{Z} \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is given by $a \mapsto (1+p)^a \pmod{p^n}$. Using this, one deduces that the transition maps induce maps

$$\alpha_n \times \beta_n : \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z},$$

where α_n is an isomorphism and $\beta_n(a \pmod{p^n}) = a \pmod{p^{n-1}}$. Consequently,

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

We deduce the following diagram



where $M \cap \mathbb{Q}(\mu_p) = \mathbb{Q}$ and $L = M\mathbb{Q}(\mu_p)$. In particular, we have contracted a $\mathbb{Z}_p$ Galois extension of $\mathbb{Q}$, which is a non-trivial task. This extension is not easily described using polynomials. To convince yourself of that, try writing the $\mathbb{Z}/p\mathbb{Z}$ Galois extension of $\mathbb{Q}$ one gets from M. It is the subfield of $\mathbb{Q}(\mu_{p^2})$ that has degree p over $\mathbb{Q}$.

6. Kummer Theory

6.1. **Cyclic Galois extensions.** Let $\mathbb{F}$ be a field and n a positive integer not divisible by the characteristic of $\mathbb{F}$. Assume that $\mathbb{F}$ contains the n-th roots of unity: the polynomial x^n-1 is separable and its roots are in $\mathbb{F}$. We denote the roots by μ_n, of $\mu_n(\mathbb{F})$ if we need to clarify the field involved; it is a cyclic group of order n under multiplication. Given an element $a\in\mathbb{F}$ we denote by $\sqrt[n]{a}$ any fixed solution of the polynomial x^n-a. Recall that a cyclic Galois extension, or simply a **cyclic extension** of fields is a finite Galois extension of fields with cyclic Galois group. In the same vain, one talks about **abelian extension**, **solvable extension**, etc.

Theorem 6.1.1. *Let $a\in\mathbb{F}^*$ then $\mathbb{F}(\sqrt[n]{a})/\mathbb{F}$ is a cyclic Galois extension of order dividing n. Conversely, if $L/\mathbb{F}$ is a cyclic Galois extension of order m, $m|n$, then $L=\mathbb{F}(\sqrt[m]{a})$ for some $a\in\mathbb{F}^*$.*

Proof. $\mathbb{F}(\sqrt[n]{a})$ is the splitting field of the polynomial x^n-a, because the roots of this polynomial are precisely $\{\zeta\cdot\sqrt[n]{a}:\zeta\in\mu_n\}$. Moreover, there are n elements in μ_n, so x^n-a is a separable polynomial and so $\mathbb{F}(\sqrt[n]{a})/\mathbb{F}$ is a Galois extension.

Let $\sigma\in\mathrm{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$, then

$$\sigma(\sqrt[n]{a})=\zeta_\sigma\cdot\sqrt[n]{a},$$

for some $\zeta_\sigma\in\mu_n$. Note that $\sigma=\mathrm{Id}$ if and only if $\zeta_\sigma=1$. Further,

$$\begin{aligned}\zeta_{\sigma\tau}\cdot\sqrt[n]{a}&=(\sigma\tau)(\sqrt[n]{a})\\&=\sigma(\zeta_\tau\sqrt[n]{a})\\&=\zeta_\tau\sigma(\sqrt[n]{a})\\&=\zeta_\tau\zeta_\sigma\cdot\sqrt[n]{a}\\&=\zeta_\sigma\zeta_\tau\cdot\sqrt[n]{a}.\end{aligned}$$

Therefore,

$$\sigma\mapsto\zeta_\sigma,$$

is an injective homomorphism $\mathrm{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})\to\mu_n$. Since μ_n is a cyclic group, so is $\mathrm{Gal}(\mathbb{F}(\sqrt[n]{a})/\mathbb{F})$.

Conversely, let $L/\mathbb{F}$ be a cyclic Galois extension of order $m|n$; say, $\mathrm{Gal}(L/\mathbb{F})=\langle\sigma\rangle$. Given $\alpha\in L$ and $\zeta\in\mu_m$, define the **Lagrange resolvent**:

$$[\alpha,\zeta]=\alpha+\zeta\sigma(\alpha)+\cdots+\zeta^{m-1}\sigma^{m-1}(\alpha). \tag{4}$$

This is an element of L and the action of σ on it is given by $\sigma([\alpha,\zeta])=\sigma(\alpha)+\zeta\sigma^2(\alpha)+\cdots+\zeta^{m-1}\sigma^m(\alpha)$. Using that $\sigma^m=\mathrm{Id}$, we find that

$$\sigma([\alpha,\zeta])=\zeta^{-1}\cdot[\alpha,\zeta].$$

It follows that $[\alpha,\zeta]^m=(\sigma([\alpha,\zeta]))^m=\sigma([\alpha,\zeta]^m)$ and so that

$$[\alpha,\zeta]^m\in\mathbb{F}.$$

By independence of characters, for every ζ there is an $\alpha\in L$ such that $[\alpha,\zeta]\neq0$. Let ζ be a primitive m-th root of unity. Then $\mathbb{F}\subseteq\mathbb{F}([\alpha,\zeta])\subseteq L$ and $\sigma^i([\alpha,\zeta])=\zeta^{-i}\cdot[\alpha,\zeta]$ implies that σ^i is not the identity on $\mathbb{F}([\alpha,\zeta])$. Thus, by the Galois correspondence,

$$L=\mathbb{F}([\alpha,\zeta]).$$

□

Remark 6.1.2. Let $L/\mathbb{F}$ be a cyclic Galois extension of order $m|$n, where $\mathbb{F}$ is as above. Let $G=\langle\sigma\rangle$ be the Galois group, a cyclic group of order m. Given an element γ of L whose m-th power is in $\mathbb{F}^\times$, we get a map

$$G\to\mu_n\subseteq\mathbb{F}^\times,\qquad\sigma^i\mapsto\sigma^i(\gamma)/\gamma.$$

This map is a homomorphism. The set of such homomorphisms forms a group under multiplication of functions and the Lagrange resolvent allows us to show that there is such a homomorphism, obtained from taking $\gamma = [\zeta, \alpha[$ for ζ a primitive m-th root of unity, whose order is m.

6.2. **Kummer extensions.** Let $\mathbb{F}$ be a field and n a positive integer not divisible by the characteristic of $\mathbb{F}$. Assume that $\mathbb{F}$ contains the n-th roots of unity. Recall that the **exponent** of a group G is the minimal integer n such that every element of G has order divisibly by n. If G is finite abelian, there is then an element of order n in G. A **Kummer n-extension** of $\mathbb{F}$ is an abelian Galois extension $L/\mathbb{F}$ of finite order such that the Galois group has exponent $m|n$. In this section we shall describe all such Galois extensions. Note that the case of G is cyclic is precisely the case we have dealt with above. We shall need some basic facts about character group of a finite abelian group.

6.2.1. *Characters of finite groups.* Let G be a finite abelian group. A **character** χ of G is a group homomorphism

$$\chi : G \to \mathbb{C}^\times.$$

We denote the set of all characters of G by $\hat{G}$. They form a group under multiplication of functions

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g).$$

$\hat{G}$ is called the **character group** of G. If G is of exponent n and we are given a field $\mathbb{F}$ as above, we can and often identify the n-th roots of unity in $\mathbb{C}^\times$ with the n-th roots of unity μ_n in $\mathbb{F}$, $\mu_n(\mathbb{C}) \cong \mu_n(\mathbb{F})$, and view $\hat{G}$ is the group of homomorphisms

$$G \to \mu_n(\mathbb{F}).$$

Suppose that G is cyclic of order $m|n$, say $G = \langle\sigma\rangle$. Then, to give a homomorphism $\chi : G \to \mathbb{C}^\times$ is equivalent to choosing an m-th root of unity ζ and defining

$$\chi_\zeta(\sigma^i) = \zeta^i.$$

And, conversely, every character arises this way. That is, we find that $G \cong \hat{G}$, but the isomorphism is not canonical, it depends on the choice of ζ. More generally, writing $G = G_1 \times \cdots \times G_a$, a product of cyclic groups, we have canonically, $\hat{G} = \hat{G}_1 \times \cdots \times \hat{G}_a$ and so $\hat{G} \cong G$ for any finite abelian group. Using this it is not hard to show the following statements.

Let G be a finite abelian group of exponent n:

(1) Let $g \in G$, $g \neq 1$. There exists $\chi \in \hat{G}$ such that $\chi(g) \neq 1$.
(2) The pairing $G \times \hat{G} \to \mu_n, (a, \chi) \mapsto \chi(a)$ is a bi-additive perfect pairing. It identifies G with $\hat{\hat{G}}$ in a canonical way.
(3) A set $\{\chi_1, \ldots, \chi_r\}$ of characters generated G if and only if $\chi_i(g) = 1$ for all i implies that $g = 1$.

6.2.2. *Kummer extensions.* Let $L/\mathbb{F}$ be a finite abelian Galois extension of exponent $m|n$. Let

$$M(L) = \{\ell \in L : \ell^n \in \mathbb{F}^\times\}, \quad N(L) = \{\ell^n : \ell \in M(L)\}.$$

$M(L)$ is a subgroup of $L^\times$ and $N(L)$ is a subgroup of $\mathbb{F}^\times$. Of course, $M(L) \supseteq \mathbb{F}^\times, N(L) \supseteq \mathbb{F}^{\times n} = N(F)$.

Theorem 6.2.1. *Let $G = \mathrm{Gal}(L/\mathbb{F})$. There is an exact sequence of groups*

$$1 \to \mathbb{F}^\times \to M(L^\times) \xrightarrow{\lambda} \hat{G} \to 1,$$

where the first map is just the inclusion. The map λ is the following. Let $\ell \in M(L)$ and $\sigma \in G$, then $\sigma(\ell) = \zeta_{\sigma,\ell} \cdot \ell$, for some root of unity $\zeta_{\sigma,\ell} \in \mu_m$, depending on σ and ℓ, because $\mathbb{F}(\ell)/\mathbb{F}$ is a cyclic Galois extension of order $m|n$. We let

$$\lambda(\ell) \in \hat{G}, \qquad \lambda(\ell)(\sigma) = \zeta_{\sigma,\ell}.$$

We have $L = \mathbb{F}(M(L))$ and $L = \mathbb{F}(\ell_1, \dots, \ell_r)$ for elements $\ell_1, \dots, \ell_r \in M(L)$ if and only if the cosets $\ell_i \mathbb{F}^*$ generate $M(L)/\mathbb{F}^\times$.

Proof. We first check that $\chi := \lambda(\ell)$ is a character. Indeed $\chi(\sigma) = \frac{\sigma(\ell)}{\ell}$ and so

$$\chi(\sigma\tau) = \frac{\sigma\tau(\ell)}{\ell} = \frac{\sigma(\chi(\tau)\ell)}{\ell} = \chi(\tau) \cdot \frac{\sigma(\ell)}{\ell} = \chi(\sigma)\chi(\tau).$$

Further, λ is a homomorphism. Let $\ell, k \in M(L)$. Then

$$\frac{\sigma(\ell k)}{\ell k} = \frac{\sigma(\ell)}{\ell} \cdot \frac{\sigma(k)}{k},$$

and so $\lambda(\ell k) = \lambda(\ell) \cdot \lambda(k)$.

It follows easily from the definitions, and Galois theory, that $\mathbb{F}^\times = \mathrm{Ker}(\lambda)$.

To show that λ is surjective, decompose G is a product of cyclic groups $G_1 \times \cdots \times G_a$. Fix $r, 1 \le r \le a$. Note that we can identify $G_r = \langle \sigma \rangle$ with the Galois group of a cyclic Galois extension $L_r/\mathbb{F}$ of order $m|n$ contained in L. Suppose that $\chi \in \hat{G}_r$. In (4) we constructed a non-zero element $[\alpha, \zeta]$ that generated $L_r/\mathbb{F}$, $\frac{\sigma([\alpha,\zeta])}{[\alpha,\zeta]} = \zeta^{-1}$ and $[\alpha, \zeta]^m \in \mathbb{F}^*$ (and so $[\alpha, \zeta]^n \in \mathbb{F}^*$). That is, we see now that if we choose ζ to a primitive m-th of unity, then $[\alpha, \zeta] \in M(L_r) \subset M(L)$ and

$$\lambda([\alpha, \zeta])(\sigma^i) = \zeta^{-i}.$$

It follows that $\lambda([\alpha, \zeta])$ is an element of $\hat{G}_r$ of order m and so the map λ is surjective onto $\hat{G}_r$ (cf. Remark 6.1.2). Doing it separately for each of the extensions $L_i/\mathbb{F}$ we find that λ is surjective onto $\hat{G}$.

Now, we clearly have $L \supseteq \mathbb{F}(M(L))$. Suppose that $\sigma \in G$ acts trivially on $\mathbb{F}(M(L))$. Then $\lambda(\ell)(\sigma) = 1$ for all $\ell \in M(L)$ and so $\chi(\sigma) = 1$ for all $\chi \in \hat{G}$. That implies that $\sigma = 1$ and so, by the Galois correspondence, that $L = \mathbb{F}(M(L))$. Now, by the same argument, $L = \mathbb{F}(\ell_1, \dots, \ell_r)$ if and only if $\{\lambda(\ell_i)\}$ generate $\hat{G}$, if and only if $\{\ell_i\}$ generate the quotient group $M(L)/\mathbb{F}^\times$; that is, if and only if $\{\ell_i \mathbb{F}^\times\}$ generate $M(L)/\mathbb{F}^\times$. □

Remark 6.2.2. The significance of the last part of the theorem is that if $\mathbb{F}$ is an infinite field, the set $M(L)$ is infinite. It is therefore useful to know when we can choose finitely many elements $\ell_i \in M(L)$ such that $L = \mathbb{F}(\ell_1, \dots, \ell_r)$.

Noting that raising to n-th power provides an isomorphism $M(L)/\mathbb{F}^\times \cong N(L)/\mathbb{F}^{\times n}$, we conclude the following.

Corollary 6.2.3. *There is an isomorphism*

$$N(L)/\mathbb{F}^{\times n} \cong \hat{G}.$$

Here $N(L)/\mathbb{F}^{\times n}$ is a finite subgroup of $F^\times/\mathbb{F}^{\times n}$. Let $a_1, \dots, a_r$ be elements of $\mathbb{F}^\times$ that generate $N(L)/\mathbb{F}^{\times n}$, then $L = \mathbb{F}(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$.

We wish now to complete our discussion by showing that every finite subgroup H of $\mathbb{F}^\times/\mathbb{F}^{\times n}$ arises as $N(L)/\mathbb{F}^{\times n}$ for a finite abelian extension of $\mathbb{F}$ or exponent n. It is quite clear what to do. Choose finitely many elements $a_1, \dots, a_r$ of $\mathbb{F}^\times$ that generate H modulo $\mathbb{F}^{\times n}$. Let

$$L = \mathbb{F}(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r}).$$

Clearly L, being the compositum of the cyclic extensions $\mathbb{F}(\sqrt[n]{a_r})$, is a finite Galois extension with abelian Galois group of exponent dividing N. Moreover, $N(L) \supseteq H$. Now, we proved in Theorem 6.2.1 that if $L = \mathbb{F}(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ then $\{\sqrt[n]{a_1} \cdot \mathbb{F}^\times, \ldots, \sqrt[n]{a_r} \cdot \mathbb{F}^\times\}$ generate $M(L)/\mathbb{F}^\times$ and so we obtain that $\{a_1 \cdot \mathbb{F}^{\times n}, \ldots, a_r \cdot \mathbb{F}^{\times n}\}$ generate $N(L)/\mathbb{F}^{\times n}$. But, they also generate H. Therefore, $H = N(L)/\mathbb{F}^{\times n}$.

Theorem 6.2.4. *Let $\mathbb{F}$ be a field containing the n-th roots of unity where n is not divisible by the characteristic of $\mathbb{F}$.*

There is a bijection between the lattice of finite abelian Galois extensions $L/\mathbb{F}$ of exponent $m|n$ and finite subgroups H of $\mathbb{F}^\times/\mathbb{F}^{\times,n}$. To a Galois extension one associates $H = N(L)/\mathbb{F}^{\times,n}$ and to a subgroup H, generated by elements $a_1, \ldots, a_r$ of $\mathbb{F}^\times$, one associates the Galois extension $L = \mathbb{F}(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$. Furthermore, we have

$$H \cong \widehat{\mathrm{Gal}(L/\mathbb{F})}.$$

Let $M/\mathbb{F}$ be the union of all finite abelian Galois extensions $L/\mathbb{F}$ of exponent dividing n, and let $G = \mathrm{Gal}(M/\mathbb{F})$. Let $\hat{G}$ be the character group of G, comprising continuous homomorphisms $G \to \mu_n$ where μ_n is endowed with the discrete topology, then

$$\hat{G} \cong \mathbb{F}^\times/\mathbb{F}^{\times n}.$$

The proof of the theorem follows from the discussion above, apart from the conclusions concerning $\hat{G}$. This is left as an exercise.

Example 6.2.5. *Quadratic extensions of $\mathbb{R}$.* The group $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \mathbb{R}^\times/\mathbb{R}_{>0}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Thus, $\mathbb{R}$ has a unique quadratic extension. Since -1 gives a non-zero coset, this extension is $\mathbb{R}(\sqrt{-1})$.

Example 6.2.6. *Quadratic extensions of $\mathbb{F}_q$ ($q = p^r$, p an odd prime).* This is rather similar. The map $x \mapsto x^2$ has kernel ± 1 and so $\mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It follows that there is a unique quadratic extension of $\mathbb{F}_q$. We know all that already, of course. Contrary to the case of the real numbers, there is no canonical element in $\mathbb{F}_q^\times$ that is not a square. We just know that such a exists and then the said quadratic extension is $\mathbb{F}_q(\sqrt{a})$.

Example 6.2.7. *Quadratic and bi-quadratic extensions of $\mathbb{Q}$.* The structure of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is of an infinite abelian group, each element of which, different from the identity, has order 2. Let $k, \ell \in \mathbb{Q}^\times$. The extensions $\mathbb{Q}(\sqrt{k})$ and $\mathbb{Q}(\sqrt{\ell})$ are isomorphic if and only if $k\mathbb{Q}^{\times 2} = \ell\mathbb{Q}^{\times 2}$, namely, if and only if k/ℓ is a square of a rational number.

In a similar way, bi-quadartic extensions of $\mathbb{Q}$ correspond to subgroups of order 4 of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Let ℓ, k be two non-zero rational numbers such that k/ℓ is not a square. Then $\mathbb{Q}(\sqrt{k}, \sqrt{\ell})/\mathbb{Q}$ is a bi-quadratic extension. Every bi-quadratic extension is obtained this way. $\mathbb{Q}(\sqrt{k}, \sqrt{\ell})/\mathbb{Q}$ is equal to $\mathbb{Q}(\sqrt{k'}, \sqrt{\ell'})/\mathbb{Q}$ precisely when the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by k, ℓ is equal to the one generated by k', ℓ'.

The Galois extension $\mathbb{Q}(\mu_8)/\mathbb{Q}$ has Galois group $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (as abstract groups). It is a bi-quadratic extension. One quadratic extension is the one generated by $\mathbb{Q}(i)$. Since $i = \zeta_8^2$, this is the extension which is the fixed field of the subgroup $\{1, 5\}$. The quadratic extension corresponding to $\{1, 7\} = \{\pm 1\}$ is generated by $\alpha = \zeta_8 + \bar{\zeta}_8$ and is a real quadratic extension and the Galois group acts by $\alpha \mapsto \zeta_8^3 + \bar{\zeta}_8^3$. Take the Lagrange resolvent $[\alpha, -1] = \zeta_8 + \bar{\zeta}_8 - (\zeta_8^3 + \bar{\zeta}_8^3) = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7$. This element should be a square of a rational number. And indeed

$$[\alpha, -1]^2 = 8.$$

And so we get the quadratic field $\mathbb{Q}(\sqrt{2})$. Thus,

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2}).$$

7. Calculation of Galois groups

The main problem is this. Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ a monic, separable irreducible polynomial of degree n. Let L be the splitting field of f over $\mathbb{F}$ and $G = \mathrm{Gal}(L/\mathbb{F})$. Calculate G.

A priori, we only know that G is a *transitive subgroup* of S_n. Here is the list of possibilities (up to conjugation) for small n.

n	groups
2	S_2
3	S_3, A_3
4	S_4, A_4, D_4, V, C_4
5	$S_5, A_5, F_{20}, D_{10}, C_5$

Here V is the Klein four group $\{1, (12)(34), (13)(24), (14)(23)\}$ and $C_4 = \langle (1234) \rangle$. $C_5 = \langle (12345) \rangle$ and $F_{20} = \langle (12345), (2354) \rangle$.

7.1. **The discriminant.** This is a tool that allows us to decide if $G \subseteq A_n$ or not. Assume that the characteristic of $\mathbb{F}$ is different from 2. Write

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i),$$

in L. We view G as a subgroup of the permutation group of $\alpha_1, \ldots, \alpha_n$, which is identified naturally with S_n. Consider the action of G on

$$\delta := \prod_{i<j} (\alpha_i - \alpha_j).$$

For $\sigma \in G$ we have

$$\sigma(\delta) = \mathrm{sgn}(\sigma) \cdot \delta;$$

Indeed, this is one of the ways one defines the sign of a permutation. Since G fixes δ^2, $\delta^2 \in \mathbb{F}$. Let

$$D(f) := \delta^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

We call $D(f)$ the discriminant of f. To say G fixes δ is to say that $D(f)$ is square in $\mathbb{F}$.

Proposition 7.1.1. *$G \subseteq A_n$ if and only if $D(f)$ is a square in $\mathbb{F}$.*

Example 7.1.2. Consider the polynomial

$$f(x) = (x - \alpha_1)(x - \alpha_2) = x^2 + bx + c.$$

We have

$$D(f) = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c,$$

which is the usual discriminant of the quadratic polynomial.

Example 7.1.3. For a cubic polynomial $x^3 + ax + b$, a brute force calculation gives

$$D(f) = -4a^3 - 27b^2.$$

Given a general monic cubic polynomial $x^3 + \alpha x^2 + \beta x + \gamma$, put $x = y - \frac{\alpha}{3}$ to obtain

$$(y - \frac{\alpha}{3})^3 + \alpha(y - \frac{\alpha}{3})^2 + \cdots = y^3 + ay + b,$$

where a, b are explicit expressions in α, β, γ. We note that in general, $D(f(x)) = D(f(x - \alpha))$ for any $f(x) \in \mathbb{F}[x]$ monic and $\alpha \in \mathbb{F}$, because the roots are just shifted by α. Hence the substitution we made above allows to reduce the calculation of $D(f)$ to the case of $x^3 + ax + b$.

As a concrete example, take the polynomial $f(x) = x^3 - x + 1$. It is an irreducible polynomial. Indeed, if it is reducible over $\mathbb{Q}$ then by Gauss's lemma it is reducible over $\mathbb{Z}$. Which implies it's reducible modulo 2 and therefore that it has a root modulo 2, but $0, 1$ are not roots modulo 2. Alternately, one argues that if there is a root over $\mathbb{Z}$ it must be $\{\pm 1\}$ and we verify this is not the case. [7] Now, we have

$$D(f) = 4 - 27 = -23,$$

which is not a square in $\mathbb{Q}$. Therefore, the Galois group is not contained in A_3, yet a transitive subgroup of S_3. Therefore, the Galois group is S_3.

As another concrete example take $f(x) = x^3 - 21x - 7$ which is an irreducible polynomial by Eisenstein's criterion. The discriminant $D(f)$ is $3^6 7^2$ which is a square in $\mathbb{Q}$ and so the Galois group is A_3.

Example 7.1.4. To construct a family of cubic polynomials over $\mathbb{Q}$ with Galois group A_3 is the same as finding rational points on the curve

$$y^2 = -4A^3 - 27B^2,$$

except that one needs to prove these polynomials are also irreducible. For a fixed B, the complex solutions are an **elliptic curve** and they form a group under the addition law pictured in Figure 1.

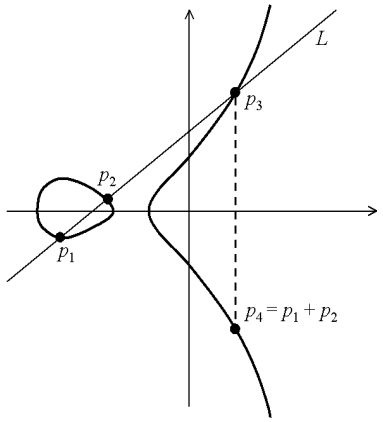


Figure 1. Addition on an elliptic curve

If we take $B = 7$, we have the solution $(y, A) = (3^3 7, -21)$ (derived from the example above). It turns out that this is a point of infinite order on the curve, and so we get infinitely many polynomials

$$x^3 + ax + 7,$$

with Galois group A_3 (if they are irreducible). Note that a is a rational number in general. Note that these polynomials cannot be obtained from each other by a linear change of co-ordinates. Thus, this is a "genuinely" infinite family. Can you prove that they are almost always irreducible? I believe that's true but I didn't prove it.

[7] In general, if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and a is a root of f in $\mathbb{Z}$ then $a | a_0$.

7.2. **Calculating Galois groups by reduction modulo p.** This method rests on the following theorem that we shall not prove in this course.

Theorem 7.2.1. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n. Let $G \subset S_n$ be its Galois group. Suppose that p is a prime and that modulo p we have*

$$f(x) = f_1(x) \cdots f_r(x) \pmod{p},$$

a product of distinct monic irreducible polynomials for degree $\deg(f_i) = n_i$. Then G contains a permutation of cycle type $(n_1, \ldots, n_r)$.

This theorem is a very powerful theorem. For example, for $n = 3$, we know that $G = A_3$ or S_3 and we can distinguish between the possibilities by deciding if G contains a transposition or not. For $n = 4$ we have the following table:

	C_4	V	D_4	A_4	S_4
(12)	×	×	✓	×	✓
(123)	×	×	×	✓	✓
(12)(34)	✓	✓	✓	✓	✓
(1234)	✓	×	✓	×	✓

The table shows that we can distinguish between all the transitive subgroups of S_4 by knowing the cycle types of permutations belonging to it. An even deeper theorem tells us that every cycle type belonging to G arises this way from p large enough. The catch though is that we cannot bound p (although we can do it condition on the Generalized Riemann Hypothesis).

Example 7.2.2. Consider the polynomial $f(x) = x^3 - x + 1$. This polynomial is irreducible modulo 2 and so G has a 3 cycle. Modulo 7 we have $f(x) = (x - 2)(x^2 + 2x + 3)$ and so G contains a transposition. It follows that $G = S_3$.

Example 7.2.3. Consider the polynomial $f(x) = x^4 - 4x^2 + 2$. It is an irreducible polynomial by Eisenstein's criterion. One verifies by a somewhat tedious calculation that f is irreducible modulo 3 and so G has a 4 cycle. Consider the polynomial $y^2 - 4y + 2$ and let α, α' be the roots. We have

$$\alpha = 2 + \sqrt{2}, \quad , \alpha' = 2 - \sqrt{2}, \quad \frac{\alpha}{\alpha'} = (1 + \sqrt{2})^2.$$

The splitting field of f is

$$K = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\alpha'}) = \mathbb{Q}(\sqrt{\alpha}),$$

and so $[K : \mathbb{Q}] = 4$. It follows that $G = C_4$.

We remark that having proved that $|G| = 4$, we can prove G is cyclic "by hand". Consider the diagram

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{\alpha}) & \xrightarrow{\sigma} & \mathbb{Q}(\sqrt{\alpha'}) \\ | & & | \\ \mathbb{Q}(\alpha) & \xrightarrow{\sigma} & \mathbb{Q}(\alpha') \\ | & & | \\ \mathbb{Q} & \longrightarrow & \mathbb{Q} \end{array}$$

We first construct $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha') = \mathbb{Q}(\alpha)$ that takes α to α'. It takes the irreducibly polynomial $x^2 - \alpha$ to $x^2 - \alpha'$ and so σ can be lifted to an automorphism, still denoted σ between the fields $\mathbb{Q}(\sqrt{\alpha})$ and $\mathbb{Q}(\sqrt{\alpha'})$. It takes $\sqrt{\alpha}$ to $\sqrt{\alpha'}$, $\sigma(\sqrt{\alpha}) = \sqrt{\alpha'}$. We calculate the $\sigma(\sqrt{\alpha'}) = \sigma(\sqrt{\alpha'/\alpha} \cdot \sqrt{\alpha}) =$

$\sigma((1+\sqrt{2})^{-1}\cdot\sqrt{\alpha}) = (1-\sqrt{2})^{-1}\cdot\sqrt{\alpha'} = -(1+\sqrt{2})\sqrt{\alpha'} = -\sqrt{\alpha}$. From that we see that σ has order 4 and so that G is cyclic.

Example 7.2.4. Consider the polynomial x^4-2 over $\mathbb{Q}$. It is irreducible by Eisenstein's criterion. The Galois group G is therefore a transitive subgroup of S_4. The splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$. It contains $\mathbb{Q}(\sqrt{2}, i)$ which is a biquadratic extension. We see that $\mathbb{Q}(\sqrt[4]{2}, i)$ has degree 8 over $\mathbb{Q}$. Thus, $G = D_4$.

Example 7.2.5. Consider $x^4+3x+15$, irreducible by Eisenstein. Modulo 2 the polynomial is x^4+x+1. It has no root modulo 2. The quadratic irreducible polynomials modulo 2 are just x^2+x+1 and so x^4+x+1 is irreducible modulo 2. Thus, the Galois group contains a 4-cycle. Modulo 5 we find the polynomial $x(x^3+3) = x(x-3)(x^2+3x-1)$ and we conclude that G contains a transposition, so $G \supseteq D_4$.

The discriminant of a polynomial of the form x^4+qx+r is $-27q^4+256r^3$. [8] So, for our polynomial, the discriminant is $861813 = 3^3\cdot 59\cdot 54$ and so is not a square. So G is not a subgroup of A_4. However, from the classification of subgroups as in the table above, we already know that. It remains to decide if $D = S_4$ or $D = D_4$.

Testing the polynomial modulo 7 we find a unique root 3, $x^4+3x+15 = (x-3)(x^3+3x^2+2x+2)$ and the polynomial x^3+3x^2+2x+2 doesn't have a root modulo 7, hence it is irreducible. Thus, G contains a 3 cycle and so $G = S_4$.

Example 7.2.6. *Constructing S_n Galois extensions.* This is based on the group theoretic fact that for n prime, S_n is generated by σ, τ, where σ can be taken to be any transposition and τ any cycle of length n. Given n prime, find a polynomial f over $\mathbb{Z}/2\mathbb{Z}$ which is irreducible. Also, let p be an odd prime that is greater or equal to $n-2$ and let $h(x)$ be a quadratic irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$. Let $g(x) = h(x)\cdot\prod_{i=0}^{n-3}(x-i)$. Then $g(x)$ is a polynomial of degree n as well. Using the Chinese remainder theorem we may find a polynomial $a(x)\in\mathbb{Z}[x]$ such that

$$a(x) \equiv f(x) \pmod 2, \qquad a(x) \equiv g(x) \pmod p.$$

It follows that the Galois group of $a(x)$ is S_n. This technique can be extended to n that is not prime. We illustrate this is one example below.

It's fun to work some examples. Here is the table of irreducible polynomials of degree at most 5 over $\mathbb{Z}/2\mathbb{Z}$.

[8] More generally (see Dummit and Foote p. 613 ff.) the discriminant of a polynomial of the form x^4+px^2+qx+r is

$$16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

You will also find there a thorough discussion of the determination of the Galois group of a quartic polynomial which is guaranteed to work and doesn't use the method of reducing modulo a prime.

degree	polynomials
1	x
	$x+1$
2	x^2+x+1
3	x^3+x^2+1
	x^3+x+1
4	$x^4+x^3+x^2+x+1$
	x^4+x^3+1
	x^4+x+1
5	$x^5+x^3+x^2+x+1$
	$x^5+x^4+x^2+x+1$
	$x^5+x^4+x^3+x+1$
	$x^5+x^4+x^3+x^2+1$
	x^5+x^3+1
	x^5+x^2+1

(This table should be checked again)

So, to construct a cubic polynomial over $\mathbb{Z}$ with Galois group S_3 we take the polynomials

$$x^3+x+1 \pmod 2, \qquad (x^2+1)x \pmod 3$$

and find a simultaneous lift to $\mathbb{Z}[x]$, for instance x^3+x+3.

To construct a polynomial of degree 5 over $\mathbb{Z}$ with Galois group S_5 we take the polynomials

$$x^5+x^2+1 \pmod 2, \qquad (x^2+1)x(x+1)(x-1)=x^5-x \pmod 3$$

and find a simultaneous lift to $\mathbb{Z}[x]$, for instance x^5+3x^2+2x+3.

To construct a polynomial of degree 4 over $\mathbb{Z}$ with Galois group S_4 we use that S_4 is generated by any choice of a 4 cycle and a 3 cycle. take the polynomials

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

and find a simultaneous lift to $\mathbb{Z}[x]$, for instance x^4+2x^2+x+3.

Example 7.2.7. For $n=5$ we have the table

	C_5	A_5	D_{10}	F_{20}	S_5
(12)	×	×	×	×	✓
(123)	×	✓	×	×	✓
(1234)	×	×	×	✓	✓
(12345)	✓	✓	✓	✓	✓
(12)(34)	×	✓	✓	✓	✓
(12)(345)	×	×	×	×	✓

For example, consider the polynomial x^5-2, an irreducible polynomial by Eisenstein's criterion. The splitting field L contains $\mathbb{Q}(\zeta_5)$ and $L/\mathbb{Q}(\zeta_5)$ is cyclic of degree 1 or 5, according to Kummer theory. Degree 1 is not possible as $[\mathbb{Q}(\zeta_5):\mathbb{Q}]=4$ and we know that $5|[L:\mathbb{Q}]$. Thus, G has degree 20 and so, necessarily, $G\cong F_{20}$.