Worksheets from Math 594: Algebra II, University of Michigan, Winter 2022

These are the worksheets from a graduate algebra course focusing on rings and modules, taught at the University of Michigan in Fall 2021. The worksheets were written by David E Speyer and are released under a Creative Commons By-NC-SA 4.0 International License. If you wish to use them for teaching, contact David E Speyer (`speyer@umich.edu`) for the LaTeX source.

Many thanks to the students: Emilee Cardin, Heitor Anginski Cotosky, Zach Deiman, Ram Ekstrom, Taeyoung Em, Yuqin Kewang, Sandra Nair, Mia Smith and Ying Wang, for their work and suggestions.

Contents

1. Symmetries of polynomials

Let S_n be the group of permutations of 1, 2, ..., n. For two permutations σ and τ, we will write either $\sigma \circ \tau$ or $\sigma\tau$ for the composition: $(\sigma\tau)(j) := \sigma(\tau(j))$. We will often write permutations using cycle notation: $(i_1 i_2 \cdots i_k)$ means the permutation which cycles $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$ and fixes everything not in $\{i_1, i_2, \ldots, i_k\}$. We will let S_n act on the ring of polynomials $\mathbb{C}[r_1, \ldots, r_n]$ in the obvious way.

Set

$$\Delta = \prod_{i<j} (r_i - r_j).$$

Problem 1.1. (1) For any permutation σ in S_n, show that $\sigma(\Delta^2) = \Delta^2$.
(2) For any permutation σ in S_n, show that $\sigma(\Delta) = \pm\Delta$.

Let $\omega = \frac{-1+\sqrt{-3}}{2}$. When we studied the cubic formula, we set

$$P = r_1 + \omega r_2 + \omega^2 r_3.$$

Let A_3 be the subgroup $\{e,\ (123),\ (123)^2\}$ of S_3.

Problem 1.2. (1) For any permutation $\sigma \in A_3$, show that $\sigma(P^3) = P^3$.
(2) For any permutation $\sigma \in A_3$, show that $\sigma(P) = \omega^k P$ for some integer k.

We set $\epsilon(\sigma) = \frac{\sigma(\Delta)}{\Delta}$, so $\epsilon(\sigma) \in \{\pm 1\}$. For $\sigma \in A_3$, we set $\eta(\sigma) = \frac{\sigma(P)}{P}$, so $\eta(\sigma) \in \{1, \omega, \omega^2\}$.

Problem 1.3. Show that $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$, for σ and $\tau \in S_n$. Show that $\eta(\sigma\tau) = \eta(\sigma)\eta(\tau)$, for σ and $\tau \in A_3$.

We generalize these two examples. Let f be a nonzero polynomial in $\mathbb{C}[r_1, r_2, \ldots, r_n]$ and let m be a positive integer. Define

$$G = \{\sigma \in S_n : \sigma(f^m) = f^m\} \qquad H = \{\sigma \in S_n : \sigma(f) = f\}.$$

Problem 1.4. (1) For $\sigma \in G$, define $\chi_f(\sigma) = \frac{\sigma(f)}{f}$. Show that $\chi_f(\sigma)$ is an m-th root of unity in $\mathbb{C}^*$.
(2) Show that G and H are subgroups of S_n.
(3) Show that, for σ and $\tau \in G$, we have $\chi_f(\sigma\tau) = \chi_f(\sigma)\chi_f(\tau)$.

Here are polynomials related to the quartic formula:

f	f^m
$T = r_1 + r_2 - r_3 - r_4$	T^2
$U = r_1 - r_2 + r_3 - r_4$	U^2
$V = r_1 - r_2 - r_3 + r_4$	V^2
$T + \omega U + \omega^2 V$	$\left(T + \omega U + \omega^2 V\right)^3$

Problem 1.5. For each of the polynomials in the table above, describe G, H and χ_f.

2. CHARACTERS OF THE SYMMETRIC AND ALTERNATING GROUPS

We recall the map $\epsilon : S_n \to \{\pm 1\}$, defined by $\epsilon(\sigma) = \frac{\sigma(\prod(r_i - r_j))}{\prod(r_i - r_j)}$. You showed that $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$. This means that ϵ is an example of a ***character***:

Let G be a group. A ***character*** of G is a map $\chi : G \to \mathbb{C}^*$ obeying $\chi(gh) = \chi(g)\chi(h)$. The ***kernel*** of χ is $\{g \in G : \chi(g) = 1\}$. We define the ***alternating group***, A_n, to be the kernel of ϵ.

Problem 2.1. Which of the following permutations are in A_4:

$$\mathrm{Id},\ (12),\ (123),\ (12)(34),\ (1234)?$$

Two elements, g and h of G, are called ***conjugate***, if there is an element $c \in G$ with $h = cgc^{-1}$.

Problem 2.2. Let g and h be conjugate and let $\chi : G \to \mathbb{C}^*$ be a character. Show that $\chi(g) = \chi(h)$.

A ***transposition*** is a permutation of the type (ij). A 3-***cycle*** is a permutation of the type (ijk).

Problem 2.3. Let (ij) and $(k\ell)$ be two transpositions in S_n. Show that (ij) and $(k\ell)$ are conjugate.

Problem 2.4. Let $n \geq 5$ and let (ijk) be a 3-cycle in A_n. Show that (ijk) and $(ijk)^{-1}$ are conjugate in A_n, meaning that there is a permutation $c \in A_n$ with $c(ijk)c^{-1} = (ijk)^{-1}$.

Problem 2.5.
(1) Show that any permutation in S_n is a product of transpositions.
(2) Show that any permutation in A_n is a product of 3-cycles.

Problem 2.6. Let $\chi : S_n \to \mathbb{C}^*$ be a character.

(1) Show that either $\chi((ij)) = 1$ for all transpositions $(ij) \in S_n$ or else $\chi((ij)) = -1$ for all transpositions $(ij) \in S_n$.
(2) Show that either $\chi(g) = 1$ for all permutations $g \in S_n$ or else $\chi(g) = \epsilon(g)$ for all permutations $g \in S_n$.

Problem 2.7. Let $\chi : A_n \to \mathbb{C}^*$ be a character.

(1) Show that, for every 3-cycle (ijk), we have $\chi((ijk)) \in \{1, \omega, \omega^2\}$.
(2) Assuming that $n \geq 5$, show that, for all 3-cycles (ijk), we have $\chi((ijk)) = 1$.
(3) Assuming that $n \geq 5$, show that, for all $g \in A_n$, we have $\chi(g) = 1$.

3. A WEAK VERSION OF UNSOLVABILITY OF THE QUINTIC

One of the highlights of this course will be the proof of the unsolvability of the quintic. This worksheet proves a weaker version of this result.

Let L be the field of rational functions $\mathbb{C}(r_1, r_2, \ldots, r_n)$. Define e_1, e_2, …, e_n as the coefficients of the polynomial:

$$(x - r_1)(x - r_2) \cdots (x - r_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - e_3 x^{n-3} + \cdots \pm e_n.$$

Theorem (Ruffini): Starting from e_1, e_2, …, e_n, it is impossible to obtain the elements r_1, r_2, …, r_n of L by the operations $+$, $-$, $\times$, $\div$, $\sqrt[n]{}$, **under the condition that**, every time we take an n-th root, we must stay in L.

At any point in the computation, there will be some list of elements of L which we have computed so far. Call them θ_1, θ_2, θ_3, … where each θ_k is either

(1) An element of $\mathbb{C}(e_1, \ldots, e_n)$.
(2) Of the form $\theta_i + \theta_j$, $\theta_i - \theta_j$, $\theta_i \times \theta_j$ or θ_i / θ_j, for i, $j < k$.
(3) Of the form $\sqrt[n]{\theta_j}$ for $j < k$.

Let G_j be the subgroup of S_n fixing θ_1, θ_2, …, θ_j.

Problem 3.1. (1) If $\theta_k \in \mathbb{C}(e_1, \ldots, e_n)$, show that $G_k = G_{k-1}$.
(2) If θ_k is of the form $\theta_i + \theta_j$, $\theta_i - \theta_j$, $\theta_i \times \theta_j$ or θ_i / θ_j, for i, $j < k$, show that $G_k = G_{k-1}$.
(3) If θ_k is of the form $\sqrt[n]{\theta_j}$ for $j < k$, show that there is a character $\chi : G_{k-1} \to \mathbb{C}^*$ with kernel G_k.

Deleting the duplicate groups, we obtain a chain of subgroups

$$S_n = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots$$

such that, for each $k \geq 1$, there is a character $\chi : G_{k-1} \to \mathbb{C}^*$ with kernel G_k.

Problem 3.2. Let $n \geq 2$. Show that the first step of the chain must be $S_n \supsetneq A_n$.

Problem 3.3. Let $n \geq 5$. Show that the chain ends at A_n.

Problem 3.4. Prove Ruffini's Theorem!

4. GROUPS

Definition: A ***group*** G is a set with a binary operation $* : G \times G \to G$ obeying the properties

1. There is an element 1 of G such that $1 * g = g * 1 = g$ for all $g \in G$.
2. For all $g \in G$, there is an element g^{-1} obeying $g * g^{-1} = g^{-1} * g = 1$.
3. For all $g_1, g_2, g_3 \in G$, we have $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.

Given a group G, a ***subgroup*** of G is a subset containing 1 and closed under $*$ and $g \mapsto g^{-1}$.

Depending on context, we may denote $*$ by $*$, $\times$, $\cdot$ or no symbol at all, and we may denote 1 as 1, e or Id.

Problem 4.1. Show that a group G only has one element 1 obeying the condition (1).

Problem 4.2. Let G be a group and let $g \in G$. Show that G only has one element obeying the condition (2).

Definition: Given two groups G and H, a ***group homomorphism*** is a map $\phi : G \to H$ obeying $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$. A bijective group homomorphism is called an ***isomorphism*** and two groups are called ***isomorphic*** if there is an isomorphism between them.

A group homomorphism can also be called a "map of groups" or a "group map".

Problem 4.3. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi(1) = 1$ and $\phi(g^{-1}) = \phi(g)^{-1}$.

Problem 4.4. Let $\phi : G \to H$ be a group homomorphism.

1. The ***image*** of ϕ is $\mathrm{Im}(\phi) := \{\phi(g) : g \in G\}$. Show that $\mathrm{Im}(\phi)$ is a subgroup of G.
2. The ***kernel*** of ϕ is $\mathrm{Ker}(\phi) := \{g \in G : \phi(g) = 1\}$. Show that $\mathrm{Ker}(\phi)$ is a subgroup of G.

Definition: Given two groups G and H, the ***product group*** is the group whose underlying set is $G \times H$, with multiplication structure $(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Problem 4.5. Let G and H be two groups and let π_1 and π_2 be the projections $G \times H \to G$ and $G \times H \to H$ onto the first and second factor. Show that $G \times H$ obeys the ***universal property of products***, meaning that, for any group F with maps $\phi_1 : F \to G$ and $\phi_2 : F \to H$, there is a unique map $(\phi_1, \phi_2) : F \to G \times H$ such that the diagram below commutes:

$$\begin{tikzcd}
F \arrow[rrd, bend left, "\phi_1"] \arrow[rd, dashed, "{(\phi_1,\phi_2)}"] \arrow[rdd, bend right, "\phi_2"'] & & \\
& G \times H \arrow[r, "\pi_1"] \arrow[d, "\pi_2"] & G \\
& H &
\end{tikzcd}$$

We close with a few more definitions:

Definition: For $g \in G$, the ***conjugacy class*** of g is the set $\mathrm{Conj}(g) := \{hgh^{-1} : h \in G\}$.

Definition: A group G is called ***abelian*** if $g_1 * g_2 = g_2 * g_1$ for all $g_1, g_2 \in G$.

If G is abelian, we often denote $*$ by $+$ and 1 by 0. We **never** use these notations for a non-abelian group.

5. Group actions

Definition: Let G be a group and let X be a set. An ***action*** of G on X is a map $* : G \times X \to X$ obeying $(g_1 * g_2) * x = g_1 * (g_2 * x)$ and $e * x = x$.

Depending on context, we may denote $*$ by $*$, $\times$, $\cdot$ or no symbol at all. This notion of an action can also be called a "left action"; a "right action" is a map $* : X \times G \to X$ obeying $x * (g_2 * g_1) = (x * g_2) * g_1$.

Problem 5.1. Let $G \times X \to X$ be a left action of G on X. Define a map $X \times G \to X$ by $(x, g) \mapsto g^{-1}x$. Show that this is a right action of G on X.

Problem 5.2. Let S_X be the group of bijections $X \to X$, with the group operation of composition. Show that an action of G on X is the same as a group homomorphism $G \to S_X$.

Definition: Let G be a group which acts on a set X. For $x \in X$, the ***stabilizer*** $\mathrm{Stab}(x)$ of x is $\{g \in G : g * x = x\}$. For $g \in G$, the***fixed points*** $\mathrm{Fix}(g)$ of g are $\{x \in X : g * x = x\}$.

Problem 5.3. With G, X and x as above, show that $\mathrm{Stab}(x)$ is a subgroup of X.

Problem 5.4. Let G, X and x be as above and let $g \in G$. Show that $\mathrm{Stab}(gx) = g\,\mathrm{Stab}(x)g^{-1}$.

Definition: For G, X and x as above, the ***orbit*** of x, written Gx, is $\{gx : g \in G\}$.

Problem 5.5. (**The Orbit-Stabilizer theorem**) If G is finite, show that $\#(G) = \#(Gx)\#(\mathrm{Stab}(x))$.

The set of orbits of G on X is denoted $G\backslash X$. If we have a right action, we write X/G.

Problem 5.6. (**Burnside's Lemma**[1]) Let G be a finite group and let X be a finite set on G acts. Show that

$$\frac{1}{\#G}\sum_{g \in G} \#\mathrm{Fix}(g) = \#(G\backslash X).$$

Definition: Let G be a group and let H be a subgroup. Let H act on G by $h * g = hg$. The orbits of this action are called the ***right cosets*** of H in G. The ***left cosets*** are the orbits for the right action $G * H \to G$. The number of cosets of H in G is called the ***index*** of H in G and written $[G : H]$.

Problem 5.7. Show that G has a left action on the set G/H of left cosets, such that $g_1 * (g_2 H) = (g_1 * g_2)H$. Show that the stabilizer of the coset eH is H.

Problem 5.8. (**Lagrange's Theorem**[2]) Let G be a finite group and let H be a subgroup. Show that $\#(H)$ divides $\#(G)$.

Problem 5.9. Let G be a finite group with $\#(G) = N$. Let $g \in G$ and let the group generated by g have n elements.

(1) Show that n divides N.
(2) Show that $g^N = 1$.

[1] Proved by Ferdinand Georg Frobenius.

[2] Proved by Camille Jordan.

6. Normal subgroups, quotient groups, short exact sequences

Problem 6.1. Let G be a group and let N be a subgroup. Show that the following are equivalent:

(1) For all $g \in G$, we have $gNg^{-1} = N$.
(2) N is a union of (some of the) conjugacy classes of G.
(3) All elements of G/N have the same stabilizer, for the left action of G on G/N.
(4) Every left coset of N in G is also a right coset.
(5) If $g_1N = g_1'N$ and $g_2N = g_2'N$, then $g_1g_2N = g_1'g_2'N$.

Definition: A subgroup N obeying the equivalent conditions of Problem 6.1 is called a ***normal subgroup*** of G. We write $N \trianglelefteq G$ to indicate that N is a normal subgroup of G.

Problem 6.2. Let G be S_3. Which of the following subgroups are normal?

(1) The subgroup generated by (12).
(2) The subgroup generated by (123).

Problem 6.3. Let G be a group and let N be a normal subgroup of G.

(1) Prove or disprove: Let $\alpha : F \to G$ be a group homomorphism. Then $\alpha^{-1}(N)$ is normal in F.
(2) Prove of disprove: Let $\beta : G \to H$ be a group homomorphism. Then $\beta(N)$ is normal in H.
(3) At least one of the statements above is false. Find an additional hypothesis you could add to make it true.

Definition: Given a group G and a normal subgroup N, the ***quotient group*** G/N is the group whose underlying set is the set of cosets G/N with multiplication such that $(g_1N)(g_2N) = g_1g_2N$.

This definition makes sense by Part (4) of Problem 6.1. I won't make you check that this is a group, but do so on your own time if you have any doubt. Also, I won't make you check this, but the groups G/N and $N\backslash G$, defined in the obvious ways, are isomorphic.

Let $\phi : G \to H$ be a group homomorphism. Recall that the image and kernel of ϕ are $\operatorname{Ker}(\phi) := \{g \in G : \phi(g) = 1\}$ and $\operatorname{Im}(\phi) := \{\phi(g) : g \in G\}$.

Problem 6.4. Show that the kernel of ϕ is a normal subgroup of G.

Problem 6.5. Show that the "obvious" map from $G/\operatorname{Ker}(\phi)$ to $\operatorname{Im}(\phi)$ is an isomorphism.

We often discuss quotients using the language of short exact sequences:

Definition: A ***short exact sequence*** $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ is three groups A, B and C, and two group homomorphisms $\alpha : A \to B$ and $\beta : B \to C$ such that α is injective, β is surjective, and $\operatorname{Im}(\alpha) = \operatorname{Ker}(\beta)$.

I will occasionally write 0 instead of 1 at one end or the other of a short exact sequence. I do this when the adjacent group (meaning A or C) is abelian and it would feel bizarre to denote the identity of that abelian group as 1.

We'll write C_n for the abelian group $\mathbb{Z}/n\mathbb{Z}$. This is called the ***cyclic group*** of order n.

Problem 6.6. Show that there is a short exact sequence $1 \to C_m \to C_{mn} \to C_n \to 1$.

Problem 6.7. Show that there is a short exact sequence $1 \to C_3 \to S_3 \to S_2 \to 1$.

Problem 6.8. Show that there is a short exact sequence $1 \to C_2^2 \to S_4 \to S_3 \to 1$.

7. Simple groups

Definition: A group G is called ***simple*** if G has precisely two normal subgroups, G and $\{1\}$.

We remark that the trivial group is not simple, since it only has one normal subgroup.

Problem 7.1. Prove or disprove: Let G be simple and let H be any group. For every group homomorphism $\phi : G \to H$, either ϕ is injective or else ϕ is trivial.

Problem 7.2. Prove or disprove: Let G be any group and let H be simple. For any group homomorphism $\phi : G \to H$, either ϕ is surjective or else ϕ is trivial.

Problem 7.3. Let p be a prime. Show that C_p (the cyclic group of order p) is simple.

Problem 7.4. In this problem we will show that A_n is simple, for $n \geq 5$. Let N be a nontrivial normal subgroup of A_n. Let g be a non-trivial element of N.

(1) Show that there is some 3-cycle (ijk) in A_n which does not commute with g.

We set $h = g(ijk)g^{-1}(ijk)^{-1}$.

(2) Show that $h \in N$.
(3) Show that h has one of the following cycle structures: $(abc)(def)$, $(abcde)$, $(ab)(cd)$, (abc).
(4) Show that N contains a 3-cycle. In the case where h has cycle type $(ab)(cd)$, you'll need to use that $n \geq 5$. **This part is a nuisance, and you may want to skip ahead and come back to it.**
(5) Show that $N = A_n$.

After C_p and A_n, the most important simple groups are the projective special linear groups. Let F be a field. The group $\mathrm{SL}_n(F)$ is the group of $n \times n$ matrices with entries in F and determinant 1. Let $Z \subset \mathrm{SL}_n(F)$ be $\{\zeta \, \mathrm{Id}_n : \zeta \in F \text{ with } \zeta^n = 1\}$. The ***projective special linear group*** $\mathrm{PSL}_n(F)$ is defined to be $\mathrm{SL}_n(F)/Z$. The group $\mathrm{PSL}_n(F)$ is simple, except in the cases of $\mathrm{PSL}_2(\mathbb{F}_2)$ (which is isomorphic to S_3) and $\mathrm{PSL}_2(\mathbb{F}_3)$ (which is isomorphic to A_4). The proof that $\mathrm{PSL}_n(F)$ has a lot of good ideas in it, but it is too long to make a worksheet problem; it might appear as a bonus lecture.

8. Subnormal series, composition series

Definition: A ***subnormal series*** of a group G is a chain of subgroups $G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft G_3 \triangleleft \cdots \triangleleft G_N \subseteq G$ where G_{j-1} is normal in G_j. A ***composition series*** is a subnormal series where $G_0 = \{e\}$, $G_N = G$ and each subquotient G_j/G_{j-1} is simple. A ***quasi-composition series*** is a composition series where $G_0 = \{e\}$, $G_N = G$ and each subquotient is either simple or trivial.

Problem 8.1. Show that a group which has a quasi-composition series has a composition series.

Problem 8.2. Show that every finite group has a composition series.

Problem 8.3. Show that S_4 has a composition series with subquotients C_2, C_2, C_3 and C_2.

Problem 8.4. Show that $\mathrm{GL}_2(\mathbb{F}_7)$ has a composition series with subquotients C_2, $\mathrm{PSL}_2(\mathbb{F}_7)$, C_2 and C_3. You may assume that $\mathrm{PSL}_2(\mathbb{F}_7)$ is simple. (For a field of characteristic $\neq 2$, the group $\mathrm{PSL}_2(F)$ is $\mathrm{SL}_2(F)/\pm\mathrm{Id}$. See the worksheet on simple groups for the definition of $\mathrm{PSL}_n(F)$ in general.)

Problem 8.5. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence, and let $\{1\} = A_0 \subset A_1 \subset \cdots \subset A_a = A$ and $\{1\} = C_0 \subset C_1 \subset \cdots \subset C_c = C$ be composition series of A and C. Show that

$$\{1\} = \alpha(A_0) \subset \alpha(A_1) \subset \cdots \subset \alpha(A_a) = \beta^{-1}(C_0) \subset \beta^{-1}(C_1) \subset \cdots \subset \beta^{-1}(C_c) = B$$

is a composition series for B.

Problem 8.6. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence and let $\{1\} = B_0 \subset B_1 \subset \cdots \subset B_b = B$ be a composition series of B.

(1) Show that $\{1\} = \alpha^{-1}(B_0) \subseteq \alpha^{-1}(B_1) \subseteq \cdots \subseteq \alpha^{-1}(B_b) = A$ is a quasi-composition series for A.
(2) Show that $\{1\} = \beta(B_0) \subseteq \beta(B_1) \subseteq \cdots \subseteq \beta(B_b) = C$ is a quasi-composition series for C.

We are setting up to prove the Jordan-Holder theorem for groups. Here is a useful lemma.

Problem 8.7. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence and let B' be a normal subgroup of B. Set $A' = \alpha^{-1}(B)$ and $C' = \beta(B)$. You might find it useful to think of A as a subgroup of B, and A' as $A \cap B'$.

(1) Show that $1 \to A' \to B' \to C' \to 1$ is a short exact sequence.
(2) Show that $1 \to A/A' \to B/B' \to C/C' \to 1$ is a short exact sequence.

9. The Jordan-Holder theorem

We recall the definitions from last time:

Definition: A ***subnormal series*** of a group G is a chain of subgroups $G_0 \lhd G_1 \lhd G_2 \lhd G_3 \lhd \cdots \lhd G_N \subseteq G$ where G_{j-1} is normal in G_j. A ***composition series*** is a subnormal series where $G_0 = \{e\}$, $G_N = G$ and each subquotient G_j/G_{j-1} is simple. A ***quasi-composition series*** is a composition series where $G_0 = \{e\}$, $G_N = G$ and each subquotient is either simple or trivial.

Let G be a group with a composition series $\{e\} = G_0 \rhd G_1 \rhd \cdots \rhd G_N = G$. We define N to be the length of the composition series and write $N = \ell(G)$. For a simple group Γ and a composition series $G_\bullet$, we define $m(G_\bullet, \Gamma)$ to be the number of quotients G_j/G_{j-1} which are isomorphic to Γ. Our aim today is to prove

Theorem (Jordan-Holder): Let G be a group and let $G_\bullet$ and $G'_\bullet$ be two composition series for G. Then $\ell(G_\bullet) = \ell(G'_\bullet)$ and, for any simple group Γ, we have $m(G_\bullet, \Gamma) = m(G'_\bullet, \Gamma)$.

Let $1 \to A \xrightarrow{\alpha} B \to\xrightarrow{\beta} C \to 1$ be a short exact sequence of groups. Let $B_\bullet$ be a composition series for B. Recall that we proved on the previous worksheet that $\{1\} = \alpha^{-1}(B_0) \subseteq \alpha^{-1}(B_1) \subseteq \cdots \subseteq \alpha^{-1}(B_b) = A$ is a quasi-composition series for A and $\{1\} = \beta(B_0) \subseteq \beta(B_1) \subseteq \cdots \subseteq \beta(B_b) = C$ is a quasi-composition series for C.

Problem 9.1. With the above notations, let $A_\bullet$ and $C_\bullet$ be the composition series obtained from deleting duplicate entries from the quasi-composition series above.

1. Show that $\ell(B_\bullet) = \ell(A_\bullet) + \ell(C_\bullet)$.
2. For any simple group Γ, show that $m(B_\bullet, \Gamma) = m(A_\bullet, \Gamma) + m(C_\bullet, \Gamma)$.

At this point, you have enough to prove the Jordan-Holder theorem for finite groups, by induction on $\#(G)$.

Problem 9.2. Check the base case: Jordan-Holder holds for the trivial group.

Problem 9.3. Check also that Jordan-Holder holds for simple groups.

Problem 9.4. Suppose that G is a finite group which is neither simple nor trivial, and suppose that Jordan-Holder holds for all groups of size less than $\#(G)$. Show that Jordan-Holder holds for G. This completes the induction, for $\#(G) < \infty$.

The Jordan-Holder theorem is also true for infinite groups that have composition series! Proving this requires no big new ideas, but a little more finesse. Define $L(G) = \min \ell(G_\bullet)$, where the minimum is over all composition series for G. Note $L(G) = 0$ if and only if G is trivial, and $L(G) > 0$ for any nontrivial G.

Problem 9.5. Check that $L(G) = 1$ if and only if G is simple.

Problem 9.6. Let $1 \to A \to B \to C \to 1$ be a short exact sequence of groups.

1. Show that $L(B) \geq L(A) + L(C)$.[1]
2. If A and C are nontrivial, show that $L(B) > L(A)$ and $L(B) > L(C)$.

Problem 9.7. Prove the Jordan-Holder theorem by induction on $L(G)$.

[1] In fact, equality holds and you have the tools to show it, but you don't need this.

10. SOLVABLE GROUPS

Now that we have the Jordan-Holder theorem, we can start to classify groups according to what kind of factors appear in their composition/subnormal series. A basic example of this is the solvable groups:

> **Definition:** A group G is called ***solvable*** if it has a subnormal series $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_N = G$ such that G_j/G_{j-1} is abelian.

Problem 10.1. Show that S_3 and S_4 are solvable.

Problem 10.2. Show that a subgroup of a solvable group is solvable.

Problem 10.3. Show that a quotient group of a solvable group is solvable.

Problem 10.4. Show that, if $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ is a short exact sequence, and A and C are solvable, then B is solvable.

Problem 10.5. Show that a finite group is solvable if and only if all its Jordan-Holder factors are cyclic of prime order.

There is a standard algorithm to test whether a group is solvable, using the ***derived series***.

> **Definition:** Let G be a group. The ***commutator subgroup***, also called the ***derived subgroup***, is the group generated by all products $ghg^{-1}h^{-1}$ for g and $h \in G$. It can be denoted $D(G)$ or $[G, G]$.

Problem 10.6. Show that $D(G)$ is normal in G.

Problem 10.7. Show that $G/D(G)$ is abelian.

> **Definition:** The quotient $G/D(G)$ is called the ***abelianization*** of G and denoted G^{ab}.

Problem 10.8. Prove the ***universal property of the abelianization***: If G is a group, A is an abelian group and $\chi : G \to A$ is a group homomorphism, then there is a unique homomorphism $\phi : G^{\mathrm{ab}} \to A$ such that the diagram below commutes:

$$\begin{tikzcd}
G \arrow[d, two heads] \arrow[dr, "\chi"] & \\
G^{\mathrm{ab}} \arrow[r, "\phi"'] & A
\end{tikzcd} .$$

> **Definition:** The ***derived series*** of G is the chain of subgroups $G \trianglerighteq D(G) \trianglerighteq D(D(G)) \trianglerighteq \cdots$. We'll denote the k-th group in this chain as $D_k(G)$.

Problem 10.9. Show that G is solvable if and only if there is some N for which $D_N(G) = \{e\}$.

Problem 10.10. (1) For $n \geq 2$, show that $S_n^{\mathrm{ab}} \cong \{\pm 1\}$.
(2) For $n \geq 5$, show that A_n^{ab} is trivial.
(3) For $n \geq 5$, show that S_n is not solvable.

11. Direct products

Before starting our main topic, we want some lemmas about the following definition:

Definition: Let B be a group and let A and C be subgroups. Then AC is the set $\{ac : a \in A,\ c \in C\}$.

Problem 11.1. Show that, if B is a group and A and C are subgroups with $A \cap C = \{e\}$, then the map of sets $A \times C \to AC$ by $(a, c) \mapsto ac$ is a bijection.

Problem 11.2. Give an example of a group B and two subgroups A and C such that AC is not a subgroup of B. (Hint: There is an example in S_3.)

In light of the Jordan-Holder theorem, it is natural to ask, given two groups A and C, how we can put them together into a short exact sequence $1 \to A \to B \to C \to 1$. The most basic way to do this is by a direct product. As with modules and vector spaces, these come in both internal and external versions. I'll underline the internal products for this worksheet, but the usual notation is to use $\times$ for both of them.

Definition: Given two groups A and C, the ***direct product*** is the group whose underlying set is $A \times C$, with multiplication structure $(a_1, c_1) * (a_2, c_2) = (a_1 a_2, c_1 c_2)$.

Problem 11.3. Let B be a group which has two normal subgroups A and C, such that $A \cap C = \{e\}$ and such that $B = AC$.

(1) Show that, for any $a \in A$ and $c \in C$, we have $ac = ca$. (Hint: Think about $aca^{-1}c^{-1}$.)
(2) Show that B is isomorphic to the direct product $A \times C$.

We will write $B = A \underline{\times} C$ in this case when A and C are as above. This is an "internal direct product".

Problem 11.4. Show that $\mathrm{GL}_3(\mathbb{R}) = \mathrm{SL}_3(\mathbb{R}) \underline{\times} \mathbb{R}^\times \, \mathrm{Id}_3$.

Problem 11.5. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence and suppose that there is a group homomorphism $\rho : B \to A$ with $\rho \circ \alpha = \mathrm{Id}$. In this case, we will say that the sequence $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ is ***left split***.

(1) Show that $B = \alpha(A) \underline{\times} \operatorname{Ker}(\rho)$.
(2) Show that $\alpha(A) \cong A$ and $\operatorname{Ker}(\rho) \cong C$, so $B \cong A \times C$.

Problem 11.6. For any groups A and C, show that there is a left split short exact sequence

$$1 \to A \to A \times C \to C \to 1.$$

12. Semidirect products

Once again, we ask how we can stick groups A and C together into a short exact sequence $1 \to A \to B \to C \to 1$. After direct products, the next most basic way is semidirect products. This time, we'll do the internal version first. Again, I'll underline the internal version for this worksheet, but the standard notation is to use the same symbol for both. We recall the definition:

Definition: Let B be a group and let A and C be subgroups. Then AC is the set $\{ac : a \in A,\ c \in C\}$.

We proved last time that, if $A \cap C = \{e\}$, then the map $(a, c) \mapsto ac$ is a bijection from $A \times C$ to AC.

Problem 12.1. Let B be a group, let A be a **normal** subgroup of B and let C be any subgroup of B. Show that AC is a subgroup of B.

Definition: Let B be a group, let A be a normal subgroup of B and let C be any subgroup of B. Suppose that $A \cap C = \{e\}$ and that $B = AC$. Then we say that B is the ***internal semidirect product*** of A and C and write $B = A \underline{\rtimes} C$.

Problem 12.2. Show that $S_3 = A_3 \underline{\rtimes} S_2$, with S_2 embedded as the permutations that fix 3.

Problem 12.3. Let $B = A \underline{\rtimes} C$. Define a map $\phi : C \to \mathrm{Aut}(A)$ by $\phi(c)(a) = cac^{-1}$.

(1) Show that $\phi(c)$ is, as promised, an automorphism of A.
(2) Show that $\phi : C \to \mathrm{Aut}(A)$ is a group homomorphism.
(3) Show that
$$(a_1 c_1)(a_2 c_2) = \big(a_1 \phi(c_1)(a_2)\big)(c_1 c_2).$$

We use the formula in the last problem to define the external semidirect product:

Definition: Let A and C be groups and let $\phi : C \to \mathrm{Aut}(A)$ be a group homomorphism. We define $A \rtimes_\phi C$ to be the group whose underlying set is $A \times C$, with multiplication
$$(a_1, c_1)(a_2, c_2) = (a_1 \phi(c_1)(a_2), c_1 c_2).$$
We sometimes omit ϕ when it is clear from context.

Problem 12.4. Check that $A \rtimes_\phi C$ is a group.

So Problem 12.3 says that, if $B = A \underline{\rtimes} C$, then $B \cong A \rtimes_\phi C$ for the action $\phi(c)(a) = cac^{-1}$.

Problem 12.5. Give two actions of C_2 on C_3 such that $S_3 \cong C_3 \rtimes C_2$ for one action and $C_6 \cong C_3 \rtimes C_2$ for the other.

Problem 12.6. Let p be prime. Show that $C_{p^2} \not\cong C_p \rtimes C_p$ for any action of C_p on C_p.

Problem 12.7. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence and suppose that there is a group homomorphism $\sigma : C \to B$ with $\beta \circ \sigma = \mathrm{Id}$. In this case, we will say that the sequence $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ is ***right split***.

(1) Show that $B = \alpha(A) \underline{\rtimes} \sigma(C)$.
(2) Show that $\alpha(A) \cong A$ and $\sigma(C) \cong C$, so $B \cong A \rtimes C$.

Problem 12.8. For any groups A and C, and any action of C on A, show that there is a right split short exact sequence
$$1 \to A \to A \rtimes_\phi C \to C \to 1.$$

13. Abelian extensions

Here is a lemma from the homework; check that everyone in your group solved it.

Problem 13.1. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be short exact. Let $\tilde{C}$ be any subset of G such that $\beta : \tilde{C} \to C$ is bijective. Then every $b \in B$ can be uniquely written in the form $\alpha(a)\tilde{c}$ for $a \in A$ and $\tilde{c} \in \tilde{C}$.

In this worksheet, we will study short exact sequences $1 \to A \to G \to H \to 1$ with A abelian; when such a short exact sequence exists, we say that G is an ***abelian extension*** of H. A special case is when A is central in G, in this case, we say that G is a ***central extension*** of H.

Problem 13.2. Let $1 \to A \to G \to H \to 1$ be an abelian extension. Since A is normal in G, we get an action of G on A by $g : a \mapsto gag^{-1}$. Show that the map $G \to \mathrm{Aut}(A)$ factors through H.

We'll write $\phi : H \to \mathrm{Aut}(A)$ for the resulting action.

Problem 13.3. Show that the action ϕ is trivial (meaning $\phi(h)(a) = a$ for all $h \in H$ and $a \in A$) if and only if the extension $1 \to A \to G \to H \to 1$ is central.

Classifying abelian extensions with fixed (A, H) thus comes down to two parts (1) classifying all actions of H on A and (2) for each action ϕ, classifying all abelian extensions that result. We know there is always at least one such extension: the semidirect product $A \rtimes_\phi H$.

Problem 13.4. Let p be a prime number, let H be a group of order p^k and let $1 \to C_p \to G \to H$ be an abelian extension. Show that it must be a central extension.

Problem 13.5. Let n be a positive integer and let $1 \to Z \to G \to C_n \to 1$ be a **central** extension. Show that G is abelian. (Hint: Let $g \in G$ map to a generator of C_n. Use Problem 13.1 with $S = \{1, g, g^2, \dots, g^{n-1}\}$.)

Problem 13.6. Let p be a prime number and let G be a group of order p^k. Show that G lies in a central extension $1 \to C_p \to G \to H \to 1$ for some H of order p^{k-1}.

Problem 13.7. Let p be prime. Show that every group of order p^2 is isomorphic to C_p^2 or C_{p^2}.

Problem 13.8. Let p and q be distinct prime numbers, let $A \cong C_p$, $H \cong C_q$ and let $1 \to A \to G \to H \to 1$ be an abelian extension.

1. If $p \not\equiv 1 \bmod q$, show that the action of H on A is trivial.
2. If the action of H on A is trivial, show that $G \cong C_{pq} \cong C_p \times C_q$.
3. If the action ϕ of H on A is nontrivial, show that $G \cong C_p \rtimes_\phi C_q$.

Problem 13.9. Let p be an odd prime, let $A \cong C_p$, $H \cong C_p^2$. In this problem, we will classify abelian extensions $1 \to A \to G \to H \to 1$. We write z for a generator of A and $\tilde{x}$ and $\tilde{y}$ for lifts of x and y to G.

1. Show that z is central in G. (Hint: What can ϕ be?)
2. Show that every element of G is uniquely of the form $\tilde{x}^a \tilde{y}^b z^c$ for $a, b, c \in \{0, 1, \dots, p-1\}$.
3. Show that $\tilde{x}^p$, $\tilde{y}^p$ and $\tilde{y}\tilde{x}\tilde{y}^{-1}\tilde{x}^{-1}$ are of the form z^i, z^j and z^k for some i, j and $k \in \mathbb{Z}/p\mathbb{Z}$.
4. Suppose that $k = 0$. Show that G is abelian and is isomorphic to either C_p^3 or $C_{p^2} \times C_p$.
5. Suppose that $k \neq 0$ and $(i, j) = (0, 0)$. Show that $(\tilde{x}^{a_1}\tilde{y}^{b_1}z^{c_1})(\tilde{x}^{a_2}\tilde{y}^{b_2}z^{c_2}) = \tilde{x}^{a_1+a_2}\tilde{y}^{b_1+b_2}z^{c_1+c_2+kb_1a_2}$. Show that G is isomorphic to the group of matrices of the form $\left[\begin{smallmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{smallmatrix}\right]$ with entries in $\mathbb{Z}/p\mathbb{Z}$.
6. Suppose that $(i, j) \neq (0, 0)$. Show that there are a and b not both $0 \bmod p$ such that $(\tilde{x}^a\tilde{y}^b)^p = 1$. This is where you will need that p is odd.
7. Suppose that $(i, j) \neq (0, 0)$ Show that $G \cong C_{p^2} \rtimes_\phi C_p$ and describe the action of C_p on C_{p^2}.

Problem 13.10. Let p be an odd prime. Show that every group of order p^3 is isomorphic to one of

$$C_p^3, \quad C_{p^2} \times C_p, \quad C_{p^3}, \quad C_{p^2} \rtimes C_p, \quad \left\{ \left[\begin{smallmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{smallmatrix}\right] : a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

14. THE SYLOW THEOREMS

Let p be a prime.

Definition: A ***p-group*** is a group P with $\#(P) = p^k$ for some k. For a group G, a ***p-subgroup*** of G is a subgroup which is a p-group.

Problem 14.1. Let P be a p group and let X be a finite set on which P acts. Suppose that $\#(X) \not\equiv 0 \bmod p$. Show that P fixes some point of X.

Let G be a group. Factor $\#(G)$ as $p^k m$ where p does not divide m.

Definition: A ***Sylow p-subgroup*** of G is a subgroup of G of order p^k.

Problem 14.2. Let Γ be a finite group with a Sylow p-subgroup Π. Let G be a subgroup of Γ.

(1) Show that G has a Sylow p-subgroup P. Hint: Consider G acting on Γ/Π.
(2) Show, more specifically, that there is some $\gamma \in \Gamma$ such that $P = G \cap \gamma\Pi\gamma^{-1}$.

Hint for the following three problems: Use Problem 14.2.

Problem 14.3. (**The first Sylow theorem**) Show that every finite group G has a Sylow p-subgroup.

Problem 14.4. Let G be a finite group and let P be a Sylow p-subgroup with $\#(P) = p^k$.

(1) Let Q be a p-subgroup of G. Show that there is some $g \in G$ such that $Q \subseteq gPg^{-1}$.
(2) Let H be a subgroup of G whose order is divisible by p^k. Show that there is some $g \in G$ such that $H \supseteq gPg^{-1}$.

Problem 14.5. (**The second Sylow theorem**) Let G be a finite group and let P_1 and P_2 be two Sylow p-subgroup of G. Show that there is some $g \in G$ such that $P_2 = gP_1g^{-1}$.

Let G be a group and let H be a subgroup of G. We define $N_G(H) = \{g \in G : gHg^{-1} = H\}$. The group $N_G(H)$ is called the ***normalizer*** of H in G.

Problem 14.6. Map $G/N_G(P)$ to the set of Sylow p-subgroups by sending the coset $gN_G(P)$ to gPg^{-1}. Show that this map is well defined, and is a bijection.

Problem 14.7. (1) Show that P is normal in $N_G(P)$.
(2) Let Q be a p-subgroup of $N_G(P)$. Show that $Q \subseteq P$.
(3) Let H be a p-subgroup of G. Show that $H \cap N_G(P) = H \cap P$.

Problem 14.8. Since P is a subgroup of G, the group P acts on $G/N_G(P)$. Show that the only coset which is fixed for this action is $eN_G(P)$.

Problem 14.9. (**The third Sylow theorem**) The number of Sylow p-subgroups of G is $\equiv 1 \bmod p$.

15. Some problems with Sylow groups

Problem 15.1. Let G be a group of order $p^k m$ where p does not divide m. Show that the number of p-Sylow subgroups of G divides m.

Problem 15.2. Let G and H be finite groups and p a prime number. Let P and Q be p-Sylow subgroups of G and H.

(1) Show that $P \times Q$ is a p-Sylow subgroup of $G \times H$.
(2) Show that every p-Sylow subgroup of $G \times H$ is of the form $P' \times Q'$ for P' and Q' p-Sylow subgroups of G and H.

Problem 15.3. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence of finite groups and let Q be a p-Sylow subgroup of B. Show that $\alpha^{-1}(Q)$ and $\beta(Q)$ are p-Sylow subgroups of A and C respectively.

Problem 15.4. Let $p < q$ be primes and let G be a group of order pq.

(1) Show that the q-Sylow subgroup of G is normal.
(2) Conclude that there is a short exact sequence $1 \to C_q \to G \to C_p \to 1$.
(3) Show that $G \cong C_q \rtimes C_p$ for some action of C_p on C_q.

Problem 15.5. Show that there are no simple groups of order 40. (Hint: Look at 5-Sylows.)

Problem 15.6. In this problem, we will show that there is no simple group G of order 80.

(1) Show that, if G were such a group, then G would have five 2-Sylow subgroups.
(2) Consider the map $G \to S_5$ to get a contradiction.

Problem 15.7. A standard rite of passage is to check that there are no non-abelian simple groups of order < 60, so let's do that. Let G be a non-abelian simple group.

(1) Show that the order of G is not a prime power.
(2) Show that, for every prime p dividing $\#(G)$, there must be some n_p dividing $\#(G)$ with $n_p > 1$ and $n_p \equiv 1 \bmod p$.

At this point, we have ruled out all cases except 12, 24, 30, 36, 48 and 56.

(3) In the notation of the previous problem, show that furthermore we must have $\#(G) | \frac{n_p!}{2}$.

This rules out 12, 24, 48 (take $p = 2$) and 36 (take $p = 3$).

(4) Suppose that G were a simple group of order 30. Show that G would contain 24 elements of order 5 and 20 elements of order 3; deduce a contradiction.
(5) Suppose that G were a simple group of order 56. Show that G would contain 48 elements of order 7 and > 8 elements whose order is a power of 2; deduce a contradiction.

16. Review of polynomial rings

Throughout this worksheet, let k be a field. Let $k[x]$ be the ring of polynomials with coefficients in k.

Here are some things that you hopefully know, and may use without proof.

- Let $b(x) \in k[x]$ be a nonzero polynomial of degree d. Let $a(x)$ be any polynomial in $k[x]$. Show that there are unique polynomials $q(x)$ and $r(x)$, with $\deg r < d$, such that
$$a(x) = b(x)q(x) + r(x).$$
- The ring $k[x]$ is Euclidean, is a PID and a UFD.
- If $p(x)$ is an irreducible polynomial, then $p(x)k[x]$ is a maximal ideal, and $k[x]/p(x)k[x]$ is a field.

Problem 16.1. Let $b(x) \in k[x]$ be a nonzero polynomial of degree d. Show that the ring $k[x]/b(x)k[x]$ is a k-vector space of dimension d.

Let K be a larger field containing k. For $\theta \in K$, we say that θ is ***algebraic*** over k if there is a nonzero polynomial $f(t)$ in $k[t]$ with $f(\theta) = 0$.

Problem 16.2. Let $\theta \in K$ be algebraic over k. Let $I \subset k[t]$ be $\{f(t) \in k[t] : f(\theta) = 0\}$.

(1) Show that $I = m(t)k[t]$ for some irreducible polynomial m.
(2) Show that $k[\theta]$, meaning the subring of K generated by k and θ, is isomorphic to $k[t]/m(t)k[t]$.

The polynomial $m(t)$ is called the ***minimal polynomial*** of θ.

Problem 16.3. Let K be a larger field containing k. Let α and β be two algebraic elements of K which have the same minimal polynomial. Show that there is an isomorphism $k[\alpha] \to k[\beta]$ taking α to β.

Problem 16.4. Show that θ is algebraic over k if and only if $\dim_k k[\theta] < \infty$.

Problem 16.5. Show that the set of elements of K which are algebraic over k is a subfield of K.

17. Degrees of field extensions, and constructible numbers

Definition: Let L be a field and K a subfield. The ***degree of*** L ***over*** K, written $[L : K]$, is the dimension of L as a K-vector space.

Problem 17.1. Let $K \subseteq L \subseteq M$ be three fields with $[L : K]$ and $[M : L] < \infty$. Show that $[M : K] = [M : L][L : K]$.

Problem 17.2. Let $k \subseteq K$ be a field extension with $[K : k] < \infty$. Let $\theta \in K$ and let $m(x)$ be the minimal polynomial of θ over k. Show that $\deg m(x)$ divides $[K : k]$.

We illustrate these results with an extremely classical application. A real number $\theta \in \mathbb{R}$ is called ***constructible*** if it can be written in terms of rational numbers using the operations $+$, $-$, $\times$, $\div$ and $\sqrt{\ }$. Classically, these numbers were studied because the distance between any two points constructed with straightedge and compass is constructible; now we can motivate them by saying they are the numbers which can be computed exactly with a four function calculator.

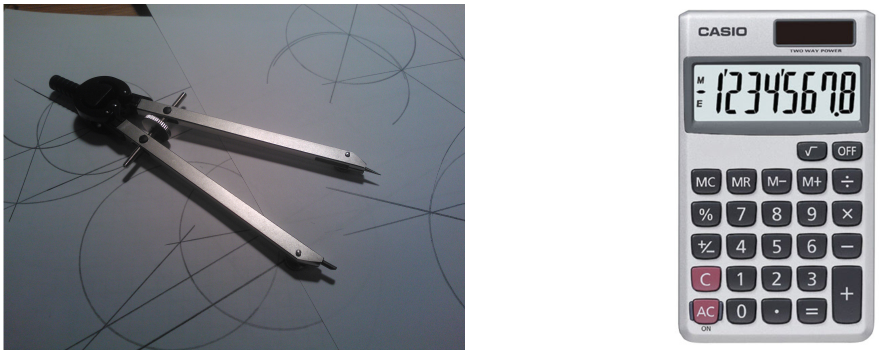


Figure: Two ancient mathematical tools

Problem 17.3. Suppose we compute a sequence of real numbers $\theta_1, \theta_2, \theta_3, \dots, \theta_N$ where each θ_k is either

- a rational number,
- of one of the forms $\theta_i + \theta_j$, $\theta_i - \theta_j$, $\theta_i\theta_j$ or θ_i/θ_j for some $i, j < k$ or
- of the form $\sqrt{\theta_j}$ for some $j < k$.

Show that $[\mathbb{Q}[\theta_1, \theta_2, \dots, \theta_N] : \mathbb{Q}]$ is a power of 2.

Problem 17.4. Let θ be a constructible real number and let $m(x)$ be its minimal polynomial over $\mathbb{Q}$. Show that $\deg m(x)$ is a power of 2.

Problem 17.5. (**The impossibility of doubling the cube**.) Show that $\sqrt[3]{2}$ is not constructible.

Problem 17.6. (**The impossibility of trisecting the angle**) It is well known that a 60° angle is constructible with straightedge and compass. Show, however, that $\cos 20^\circ$ is not constructible. Hint:

$$4\cos^3 20^\circ - 3\cos 20^\circ = \cos 60^\circ = \frac{1}{2}.$$

18. Splitting fields and maps between them

Definition: Let k be a field, let $f(x)$ be a polynomial in $k[x]$ and let K be an extension field of f. We will say that f ***splits in*** K if f factors as a product of linear polynomials in $K[x]$. We say that K is a ***splitting field of*** f if f splits as a product $c\prod(x-\theta_j)$ in $K[x]$ and the field K is generated by k and by the θ_j.

For example, if $k = \mathbb{Q}$ and $\theta_1, \theta_2, \dots, \theta_n$ are the roots of $f(x)$ in $\mathbb{C}$, then $\mathbb{Q}[\theta_1, \dots, \theta_n]$ is a splitting field of $f(x)$.

Problem 18.1. Let k be a field and let $f(x)$ be a polynomial in $k[x]$. Show that f has a splitting field.

Problem 18.2. Let L be a splitting field for $x^3 - 2$ over $\mathbb{Q}$. Show that $[L : \mathbb{Q}] = 6$. (Hint: At one point, it will be very useful to use the fact that $\mathbb{Q}[\sqrt[3]{2}]$ is a subfield of $\mathbb{R}$.)

Problem 18.3. Let $L = \mathbb{C}(x_1, x_2, \dots, x_n)$. Let e_k be the k-th elementary symmetric polynomial and let $K = \mathbb{C}(e_1, e_2, \dots, e_n) \subset L$. Show that L is a splitting field for $x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots \pm e_n$ over K.

Problem 18.4. Let

$$f(x) = \left(x - \cos\tfrac{2\pi}{7}\right)\left(x - \cos\tfrac{4\pi}{7}\right)\left(x - \cos\tfrac{8\pi}{7}\right) = \tfrac{1}{8}\left(8x^3 + 4x^2 - 4x - 1\right).$$

I promise, and you may trust me, that $f(x)$ is irreducible. Let $K = \mathbb{Q}(\cos\frac{2\pi}{7})$.

(1) Show that $[K : \mathbb{Q}] = 3$.
(2) Show that $f(x)$ splits in K. Hint: Use the double angle formula.
(3) Show that there is an automorphism $\sigma : K \to K$ with $\sigma(\cos\frac{2\pi}{7}) = \cos\frac{4\pi}{7}$.

Problem 18.5. Let k be a field and let $f(x)$ be a polynomial in $k[x]$. Let K be a splitting field of f in which f splits as $\prod(x - \alpha_j)$. Let $\sigma : k \to L$ be a field homomorphism and let $\sigma(f) := \sum \sigma(f_j)x^j$ split in L. Show that there is an injection $\phi : K \to L$ making the diagram

$$\begin{tikzcd}
k \arrow[d] \arrow[dr, "\sigma"] & \\
K \arrow[r, dashed, "\phi"] & L
\end{tikzcd}$$

commute. Hint: Think about $k \subseteq k[\alpha_1] \subseteq k[\alpha_1, \alpha_2] \subseteq \cdots \subseteq k[\alpha_1, \alpha_2, \dots, \alpha_n] = K$.

Problem 18.6. Let k_1 and k_2 be two fields and let $\sigma : k_1 \to k_2$ be an isomorphism. Let $(x) = \sum f_j x^j$ be a polynomial in $k_1[x]$ and let $\sigma(f)(x) := \sum \sigma(f_j)x^j$. Let K_1 be a splitting field of f and let K_2 be a splitting field of $\sigma(f)$. Show that there is an isomorphism $K_1 \cong K_2$ making the diagram

$$\begin{tikzcd}
k_1 \arrow[r, "\sigma"] \arrow[d] & k_2 \arrow[d] \\
K_1 \arrow[r, dashed, "\cong"] & K_2
\end{tikzcd}$$

commute.

Problem 18.7. Let k be a field and let $f(x)$ be a polynomial in $k[x]$. Let K_1 and K_2 be two splitting fields of f. Show that there is an isomorphism $K_1 \cong K_2$ making the diagram

$$\begin{tikzcd}
k \arrow[d] \arrow[dr] & \\
K_1 \arrow[r, dashed, "\cong"] & K_2
\end{tikzcd}$$

commute. **So splitting fields are unique.**

19. Introduction to field automorphisms

Definition: Let $K \subseteq L$ be fields. An ***automorphism*** of L is a bijection $\sigma : L \to L$ with $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$. An ***automorphism of*** L ***fixing*** K is an automorphism of L obeying $\sigma(a) = a$ for all $a \in K$. We write $\mathrm{Aut}(L)$ for the automorphisms of L and $\mathrm{Aut}(L/K)$ for the automorphisms of L fixing K.

Problem 19.1. Let $K \subseteq L$ be fields. Let $f(x)$ be a polynomial in $K[x]$; let $\{\theta_1, \theta_2, \dots, \theta_r\}$ be the roots of f in L.

(1) Show that $\mathrm{Aut}(L/K)$ maps $\{\theta_1, \theta_2, \dots, \theta_r\}$ to itself.
(2) Show that stabilizer of θ_j in $\mathrm{Aut}(L/K)$ is $\mathrm{Aut}(L/K(\theta_j))$.
(3) Let $L = \mathbb{Q}(\sqrt[4]{2})$ and let $f(x) = x^2 - 2$. Show that the roots of $f(x)$ in L are $\{\pm\sqrt{2}\}$ and show that $\mathrm{Aut}(L/\mathbb{Q})$ fixes both of them.

Problem 19.2. . Let K be a field, let f be a polynomial in $K[x]$, let L be a splitting field for f and let $\{\theta_1, \theta_2, \dots, \theta_n\}$ be the roots of f in L. Assume $\{\theta_1, \theta_2, \dots, \theta_n\}$ are distinct.[1]

(1) Show that the action of $\mathrm{Aut}(L/K)$ takes $\{\theta_1, \theta_2, \dots, \theta_n\}$ to itself.
(2) Show that this action of $\mathrm{Aut}(L/K)$ gives an **injection** $\mathrm{Aut}(L/K) \hookrightarrow S_n$.

Problem 19.3. Let K, f, L and $\{\theta_1, \theta_2, \dots, \theta_n\}$ be as in Problem 19.2. Let $g(x)$ be an irreducible factor of $f(x)$ in $K[x]$ and renumber the θ's so that $\{\theta_1, \theta_2, \dots, \theta_m\}$ are the roots of g in L. Show that $\{\theta_1, \theta_2, \dots, \theta_m\}$ is the $\mathrm{Aut}(L/K)$-orbit of θ_1 in L. Hint: Apply Problem 18.6 to the diagram

$$\begin{tikzcd}
K[\theta_i] \arrow[d] & K[x]/g(x)K[x] \arrow[l, "\cong"'] \arrow[r, "\cong"] & K[\theta_j] \arrow[d] \\
L \arrow[rr, dashed] & & L
\end{tikzcd}$$

Problem 19.4. Let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Show that $\mathrm{Aut}(L/\mathbb{Q}) \cong S_3$.

Problem 19.5. Let $L = \mathbb{Q}(\cos \frac{2\pi}{7})$. Show that $\mathrm{Aut}(L/\mathbb{Q}) \cong C_3$.

[1] This happens if and only if $\mathrm{GCD}(f(x), f'(x)) = 1$, see the homework.

20. Galois extensions

Problem 20.1. Let $K \subseteq L$ be a field extension of finite degree. Let $\theta \in L$ and let $g(x)$ be the minimal polynomial of θ over K.

(1) Show that the size of the $\mathrm{Aut}(L/K)$ orbit of θ is $\leq [K[\theta] : K]$.
(2) If we have equality, show that g is separable and splits in L.
(3) If L is the splitting field of some separable polynomial $f(x)$, and $g(x)$ is an irreducible factor of $f(x)$, show that we have equality.

The last part of Problem 20.1 is phrased in an awkward way; a better statement, which you can prove once you've proved the main results of this worksheet, is "if L is Galois, then we have equality."

Problem 20.2. Let $K \subseteq L$ be a field extension of finite degree. Show that $\# \mathrm{Aut}(L/K) \leq [L : K]$.

It is natural to ask when we have equality in Problem 20.2. This is answered by the following:

Theorem/Definition: Let L/K be a field extension of finite degree. The following are equivalent:

(1) For every $\theta \in L$, the minimal polynomial of θ over K is separable and splits in L.
(2) L is the splitting field of a separable polynomial $f(x) \in K[x]$.
(3) We have $\# \mathrm{Aut}(L/K) = [L : K]$.
(4) The fixed field of $\mathrm{Aut}(L/K)$ is K.

A field extension L/K which satisfies these equivalent definitions is called ***Galois***.

Problem 20.3. Prove the implications $(1) \implies (2) \implies (3) \implies (4)$ of this theorem.

The last statement is a bit harder, here is one route:

Problem 20.4. Assume condition (4). Let $\theta \in L$ and let $\{\theta_1, \theta_2, \ldots, \theta_r\}$ be the orbit of θ under $\mathrm{Aut}(L/K)$. Let $g(x) = \prod_j (x - \theta_j)$.

(1) Show that $g(x)$ has coefficients in K.
(2) Show that $g(x)$ is the minimal polynomial of θ over K.
(3) Deduce condition (1).

Definition: When L/K is Galois, we denote $\mathrm{Aut}(L/K)$ by $\mathrm{Gal}(L/K)$.

We note that we have just proved the following:

Theorem: Let L/K be a Galois extension. Let $\theta \in L$. Then the minimal polynomial of θ over K is $\prod_{\phi \in \mathrm{Gal}(L/K)\theta} (x - \phi)$.

21. Towers of field extensions and Galois groups

We recall from last time:

Theorem/Definition: Let L/F be a field extension of finite degree. The following are equivalent:

(1) For every $\theta \in L$, the minimal polynomial of θ over F is separable and splits in L.
(2) L is the splitting field of a separable polynomial $f(x) \in F[x]$.
(3) We have $\# \operatorname{Aut}(L/F) = [L : F]$.
(4) The fixed field of $\operatorname{Aut}(L/F)$ is F.

A field extension L/F which satisfies these equivalent definitions is called ***Galois***.

Theorem: Let L/F be a Galois extension. Let $\theta \in L$. Then the minimal polynomial of θ over F is $\prod_{\phi \in \mathrm{Gal}(L/F)\theta}(x - \phi)$.

Throughout this worksheet, let $F \subseteq K \subseteq L$ be field extensions of finite degree, with L/F Galois.

Problem 21.1. Show that L/K is Galois.

Problem 21.2. Show that $\mathrm{Gal}(L/K)$ is a subgroup of $\mathrm{Gal}(L/F)$.

Problem 21.3. Show that $\# \mathrm{Gal}(L/K) = [L : K]$ and $[\mathrm{Gal}(L/F) : \mathrm{Gal}(L/K)] = [K : F]$.

Problem 21.4. Show that the fixed field of $\mathrm{Gal}(L/K)$ is K.

Problem 21.5. Let L/F be a Galois extension. Show that the map

$$\{\text{fields } K \text{ with } F \subseteq K \subseteq L\} \longrightarrow \{\text{subgroups of } \mathrm{Gal}(L/F)\}$$

given by $K \mapsto \mathrm{Gal}(L/K)$ is injective. (In fact, it is bijective, but I don't think we have the toolkit to prove that yet.)

Problem 21.6. Let $\sigma \in \mathrm{Gal}(L/F)$. Show that $\mathrm{Gal}(L/\sigma(K)) = \sigma \, \mathrm{Gal}(L/K)\sigma^{-1}$ (as subgroups of $\mathrm{Gal}(L/F)$).

Problem 21.7. Show that the following are equivalent:

(1) The subgroup $\mathrm{Gal}(L/K)$ is normal in $\mathrm{Gal}(L/F)$.
(2) For all $\sigma \in \mathrm{Gal}(L/F)$, we have $\sigma(K) = K$.
(3) For all $\theta \in K$, the minimal polynomial of θ over F splits in K.
(4) K is the splitting field of a separable polynomial with coefficients in F.
(5) K/F is Galois.

Problem 21.8. In the situation above, show that we have a short exact sequence $1 \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F) \to 1$.

22. Artin's lemma

The following problem was on the problem sets, check that everyone knows how to solve it:

Problem 22.1. Let L be a field, let H be a group of automorphisms of L and let $F = \mathrm{Fix}(H)$, the elements of L fixed by H. Suppose that V is an L-vector subspace of L^n and that H takes V to itself. Show that V contains a nonzero element of F^n.

One of several results called Artin's Lemma: Let L be a field, let H be a finite group of automorphisms of L and let $F = \mathrm{Fix}(H)$, the elements of L fixed by H. Then $[L : F] = \#(H)$ and $H = \mathrm{Aut}(L/F)$.

Throughout this worksheet, let L, H and F be as above.

Problem 22.2. Show that $\#(H) \leq [L : F]$. This is just quoting something you've already done.

Suppose for the sake of contradiction that there are $n > \#(H)$ elements α_1, α_2, …, $\alpha_n \in L$ which are linearly independent over F. Define

$$V = \left\{ (c_1, c_2, \ldots, c_n) \in L^n \ : \ \sum\nolimits_j c_j h(\alpha_j) = 0 \ \forall h \in H \right\}.$$

Problem 22.3. Show that V is an L-vector subspace of L^n and that H takes V to itself.

Problem 22.4. Show that $\dim_L V > 0$.

Problem 22.5. Deduce a contradiction, and explain why you have proved $[L : F] = \#(H)$.

Problem 22.6. Show that $H = \mathrm{Aut}(L/F)$.

Artin's Lemma gives us a wide source of Galois extensions:

Problem 22.7. Let L, H and F be as in Artin's Lemma. Show that $[L : F]$ is Galois.

23. Kummer's theorem and Galois's criterion for radical extensions

We showed that, if we adjoin elements to a field by taking m-th roots, we will never leave the solvable fields. On this worksheet, we will prove a converse.

Here is the set up for problems 23.1 through 23.4: Let K be a field where $n \neq 0$ and let $\zeta \in K$ be a primitive n-th root of unity. Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \cong C_n$ and let g generate $\mathrm{Gal}(L/K)$.

Problem 23.1. Show that, as a K-vector space, L splits up as $\bigoplus_{j=0}^{n-1} L_j$ where $L_j := \{x \in L : g(x) = \zeta^j x\}$.

Problem 23.2. With notation as in the previous problems, let $\alpha \in L_j$ and $\beta \in L_k$. Show that $\alpha\beta \in L_{j+k}$.

Problem 23.3. Suppose for the sake of contradiction that, for some j, we have $\dim L_j \geq 2$.

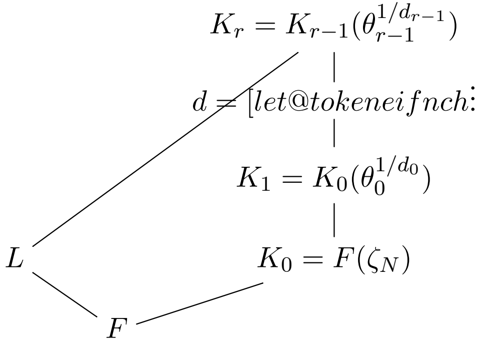
(1) Show that $L_0 \supsetneq K$.
(2) Deduce a contradiction, and conclude that $\dim L_j = 1$ for all $j \in \mathbb{Z}/n\mathbb{Z}$.

Problem 23.4. Let $\alpha \in L_1$ and put $\theta = \alpha^n$. Show that $L = K(\alpha) \cong K[x]/(x^n - \theta)K[x]$.

Theorem (Kummer's Theorem): Let K be a field where $n \neq 0$ and suppose that K contains a primitive n-th root of unity. Let L/K be a Galois extension whose Galois group is cyclic of order n. Then $L = K(\theta^{1/n})$ for some $\theta \in K$.

Problem 23.5. Let L/F be a Galois extension with solvable Galois group of order N. Suppose that $N \neq 0$ in F and $x^N - 1$ splits in F. Show that there is a chain of subfields $F = K_0 \subset K_1 \subset \cdots \subset K_r = L$ where $K_{j+1} = K_j(\theta_j^{1/d_j})$ for some $\theta_j \in K_j$ and some d_j dividing N.

Problem 23.6. Let L/F be a Galois extension with solvable Galois group of order N. Suppose that $N \neq 0$ in F. Show that there is a chain of subfields $F \subseteq K_0 \subset K_1 \subset \cdots \subset K_r \supseteq L$ where $K_0 = F(\zeta_N)$ and $K_{j+1} = K_j(\theta_j^{1/d_j})$ for some $\theta_j \in K_j$ and some d_j dividing N. (See diagram below.) You have proved:



$K_r = K_{r-1}(\theta_{r-1}^{1/d_{r-1}})$
$d = [let@tokeneifnch:$
$K_1 = K_0(\theta_0^{1/d_0})$
L
$K_0 = F(\zeta_N)$
F

Theorem (Galois's characterization of equations solvable by radicals): Let θ be algebraic over $\mathbb{Q}$ and let L be the Galois closure of $\mathbb{Q}(\theta)$. There is a formula for θ using $+$, $-$, $\times$, $\div$, $\sqrt[d]{\ }$ if and only if $\mathrm{Gal}(L/\mathbb{Q})$ is solvable.

Finally, we apply this to study constructible numbers again:

Problem 23.7. Let F be a field of characteristic $\neq 2$. Let L/F be a Galois extension with Galois group of order 2^r. Show that there is a chain of fields $F = K_0 \subset K_1 \subset \cdots \subset K_r = L$ such that $K_{i+1} = K_i(\sqrt{\theta_i})$ for $\theta_i \in K_i$. You have proved:

Theorem: Let θ be algebraic over $\mathbb{Q}$ and let L be the Galois closure of $\mathbb{Q}(\theta)$. There is a formula for θ using $+$, $-$, $\times$, $\div$, $\sqrt{\ }$ if and only if $\mathrm{Gal}(L/\mathbb{Q})$ is a 2-group.

A. Left and right splittings

Here is some useful vocabulary: Let X and Y be sets and let $X \xrightarrow{\lambda} Y$ and $Y \xrightarrow{\rho} X$ be maps obeying $\lambda \circ \rho = \mathrm{Id}$.

Definition: In the above context, λ is called a ***left inverse of*** ρ and ρ is called a ***right inverse of*** λ. We also say that λ is a ***retraction of*** ρ and ρ is a ***section of*** λ.

Problem A.1. If λ and ρ are as above, show that λ is injective and ρ is surjective.

We now turn back to groups.

Definition: Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence. A ***left splitting*** of this sequence is a group homomorphism $\lambda : B \to A$ which is left inverse to α. A ***right splitting*** is a group homomorphism $\rho : C \to B$ which is right inverse to β. A sequence is called "left split" or "right split" if it has the corresponding sort of splitting.

We'll think about left splittings first.

Remark: If I type "left splitting" into Google, the first suggestion is "left splitting headache".

Problem A.2. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence and let $\lambda : B \to A$ be a left splitting. Show that $(\lambda, \beta) : B \to A \times C$ is an isomorphism.

Problem A.3. Show that every left split short exact sequence is also right split.

Now we think about right splittings.

Problem A.4. Let A be a group and let C be a group acting on A. Construct a right split short exact sequence $1 \to A \to A \rtimes_\phi C \to C \to 1$.

Problem A.5. Let $1 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 1$ be a short exact sequence and let $\rho : C \to B$ be a right splitting.

(1) Show that $c{*}a := \rho(c)a\rho(c)^{-1}$ is an action of the group C on the group A by group automorphisms.

(2) Show that $B \cong A \rtimes C$, where the action of C on A is as in the previous part. Hint: See Problem **??**.

Thus, right split sequences occur when the middle group is the semidirect product of the ends.

Problem A.6. Let $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ be a right split short exact sequence of abelian groups. Show that $B \cong A \times C$ and the sequence is left split.

Thus, in the abelian setting, left and right splittings are equivalent.

B. Center, central series and nilpotent groups

A particularly nice sort of subnormal series is a central series, and a particularly nice kind of solvable group is a nilpotent group.

Definition: The ***center*** of a group G is the set $Z(G) := \{h : \ gh = hg \ \forall g \in G\}$.

Problem B.1. Let G be a group.

(1) Check that $Z(G)$ is a normal subgroup of G.
(2) Check that every subgroup of $Z(G)$ is normal in G.

Problem B.2. Let k be a field and let U be the group of matrices with entries in k of the form $\begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix}$. Show that the center of U is the group of matrices of the form $\begin{bmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

This problem was on the problem sets; check that everyone in your group remembers how to do it.

Problem B.3. Let p be a prime and let G be a group of order p^k for $k \geq 1$. Show that $Z(G)$ is nontrivial.

Definition: Let G be a group. A ***central series*** of G is a sequence of subgroups $G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_N$ such that, if $g \in G$ and $h \in G_i$ then $ghg^{-1}h^{-1} \in G_{i-1}$, for $1 \leq i \leq N$. G is called ***nilpotent*** if it has a central series $G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_N$ with $G_0 = \{e\}$ and $G_N = G$.

Problem B.4. Let $G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_N$ be a series of subgroups of G. Show that G is a central series if and only if all the G_i are normal in G, and $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$ for $1 \leq i \leq N$.

Problem B.5. Let k be a field and let U be the group of matrices with entries in k of the form

$$\begin{bmatrix} 1 & * & * & \cdots & * \\ & 1 & * & \cdots & * \\ & & 1 & \cdots & * \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}.$$

Show that U is nilpotent.

Problem B.6. Let p be a prime and let G be a group of order p^k for some $k \geq 1$. Show that G is nilpotent.

There is a converse to Problem B.6 which I hope to prove: The finite nilpotent groups are precisely the direct products of p-groups.

Problem B.7. Show that a nilpotent group is solvable.

Problem B.8. Show that a subgroup of a nilpotent group is nilpotent.

Problem B.9. Show that a quotient of a nilpotent group is nilpotent.

C. Finite nilpotent groups are products of p-groups.

Today's goal is to show:

Theorem: Let G be a finite group. Then G is nilpotent if and only if it is a direct product of p-groups.

Problem C.1. Show the easy direction: A direct product of p-groups is nilpotent.

From now on, let G be a finite nilpotent group with $\#(G) = \prod p_i^{k_i}$. We will be proving, by induction on $\#(G)$, that G is the direct product of its Sylow subgroups.

Problem C.2. Show that G has a central subgroup Z which is cyclic of prime order.

Let $G' = G/Z$, so we have a short exact sequence $1 \to Z \to G \xrightarrow{\beta} G' \to 1$. Let P_i' be a p_i-Sylow of G'. **By induction,** $G' = \prod_i P_i'$**.** We number the prime factors of $\#(G)$ such that $\#(Z) = p_1$. We analyze the Sylows of G, starting with the p_1-Sylow, and then the others.

Problem C.3. (1) Show that $\beta^{-1}(P_1')$ is normal in G.
(2) Show that $\beta^{-1}(P_1')$ is a p_n-Sylow of G.

Problem C.4. Now, let $i > 1$. We have a short exact sequence $1 \to Z \to \beta^{-1}(P_i') \to P_i' \to 1$.

(1) Show that $\beta^{-1}(P_i')$ is normal in G.
(2) Show that the p_i-Sylow of $\beta^{-1}(P_i')$ is also a p_i-Sylow of G.
(3) Show that $\beta^{-1}(P_i') \cong Z \times P_i'$ (here is where you use Schur-Zassenhaus).
(4) Show that the p_i-Sylow of $\beta^{-1}(P_i')$ is a characteristic subgroup of $\beta^{-1}(P_i')$.
(5) Show that the p_i-Sylow of G is normal in G.

We have now shown that every Sylow subgroup of G is normal in G.

Problem C.5. Conclude by proving that G is the direct product of its Sylow subgroups.

D. SCHUR-ZASSENHAUS, THE ABELIAN CASE

The aim of the next two worksheets will be to prove:

> **Theorem Schur-Zassenhaus:** Let $1 \to A \to B \to C \to 1$ be a short exact sequence of finite groups where $\mathrm{GCD}(\#(A), \#(C)) = 1$. Then this sequence is right split, so $B \cong A \rtimes C$.

This is the start of an answer to the question "how are groups assembled out of smaller groups": When you put groups of relatively prime order together, you just get semidirect products.

Today, we'll be proving the case where A is abelian.[1] Here is our main result:

> **Theorem:**Let A be an abelian group, C a finite group of size n, and suppose that $a \mapsto a^n$ is a bijection from A to A. Let $1 \to A \to B \to C \to 1$ be a short exact sequence. Then this sequence is right split.

Problem D.1. Show that, if A is a finite abelian group and n an integer such that $\mathrm{GCD}(\#(A), n) = 1$, then $a \mapsto a^n$ is a bijection. Thus, the above Theorem does imply the Schur-Zassenhaus theorem for A abelian.

From now on, let A be an abelian group, let C be a finite group and let $1 \to A \to B \xrightarrow{\beta} C \to 1$ be a short exact sequence. We abbreviate $\#(C)$ to n; we will not introduce the hypothesis on $a \mapsto a^n$ until later. We'll identify A with its image in B.

Let $\mathcal{S}$ be the set of right inverses of β, meaning maps $\sigma : C \to B$ such that $\beta(\sigma(c)) = c$. We emphasize that σ is not required to be compatible with the group multiplication in any way. Let B act on $\mathcal{S}$ by $(b\sigma)(c) = b\sigma(\beta(b)^{-1}c)$.

Problem D.2. Check that this is an action.

Let σ_1 and $\sigma_2 \in \mathcal{S}$. Set

$$d(\sigma_1, \sigma_2) = \prod_{c \in C} \left(\sigma_1(c)\sigma_2(c)^{-1}\right). \qquad (*)$$

We don't have to specify the order of the product, because every term is in A.

Problem D.3. Show that $d(\sigma_1, \sigma_2)d(\sigma_2, \sigma_3) = d(\sigma_1, \sigma_3)$ and $d(\sigma_1, \sigma_2) = d(\sigma_2, \sigma_1)^{-1}$.

Problem D.4. For the action of B on $\mathcal{S}$ described above, check that $d(b\sigma_1, b\sigma_2) = bd(\sigma_1, \sigma_2)b^{-1}$.

Define $\sigma_1 \equiv \sigma_2$ if $d(\sigma_1, \sigma_2) = 1$.

Problem D.5. Check that $\equiv$ is an equivalence relation.

Define $\mathcal{X}$ to be the set of equivalence classes of $\mathcal{S}$ module the relation $\equiv$.

Problem D.6. Check that the action of B on $\mathcal{S}$ descends to an action of B on $\mathcal{X}$.

Now, we impose the condition that $a \mapsto a^n$ is an automorphism of A.

Problem D.7. Show that the subgroup A of B acts on $\mathcal{X}$ with a single orbit and trivial stabilizers.

The following problem was on the problem sets; check that everyone knows how to do it:

Problem D.8. You have now shown that B acts on $\mathcal{X}$, and that the restriction of this action to A has a single orbit and trivial stabilizers. Explain why this means that $1 \to A \to B \to C \to 1$ is right split.

[1] This approach is closely based on that of Kurzweil and Stellmacher, *The Theory of Finite Groups*, Chapter 3.3, Springer-Verlag (2004).

E. THE SCHUR-ZASSENHAUS THEOREM, GENERAL CASE

Today's goal is to prove:

Theorem (Schur-Zassenhaus): Let A and C be finite groups with $\mathrm{GCD}(\#(A), \#(C)) = 1$. Then any short exact sequence $1 \to A \to B \to C \to 1$ is right split.

We introduce the following (not standard) terminology: We'll say that a pair of groups (A, C) is ***straightforward*** if every short exact sequence $1 \to A \to B \to C \to 1$ is right split. The abelian Schur-Zassenhaus theorem shows that if A is abelian and $\mathrm{GCD}(\#(A), \#(C)) = 1$, then (A, C) is straightforward.

Problem E.1. Suppose that (A_1, C) and (A_2, C) are straightforward and there is a short exact sequence $1 \to A_1 \to A \to A_2 \to 1$ with A_1 canonical in A. Show that (A, C) is straightforward. **Hint/Warning:** Unfortunately, I think this first problem is one of the hardest. First use that (A_2, C) is straightforward, then use that splitting to build a new sequence which we can split using that (A_1, C) is straightforward.

Problem E.2. Let C be a finite group, let p be a prime not dividing $\#(C)$ and let P be a p-group. Show that (P, C) is straightforward.

Let p be a prime dividing $\#(A)$ and let P be a p-Sylow subgroup of A. Let $1 \to A \to B \to C \to 1$ be a short exact sequence, with $\mathrm{GCD}(\#(A), \#(C)) = 1$. **Assume inductively that we have shown (A', C) is straightforward whenever $\mathrm{GCD}(\#(A'), \#(C)) = 1$ for $\#(A') < \#(A)$.**

Recall that $N_A(P) = \{a \in A : aPa^{-1} = P\}$ and likewise for $N_B(P)$.

Problem E.3. Show that P is canonical in $N_A(P)$.

Problem E.4. Suppose that $A = N_A(P)$. Prove that $1 \to A \to B \to C \to 1$ is right split.

So we may now assume that $N_A(P) \neq A$.

Problem E.5. With A, B, C, P as above, show that $1 \to N_A(P) \to N_B(P) \to C \to 1$ is exact.

Problem E.6. Show that $1 \to A \to B \to C \to 1$ is right split.

F. Solvable extensions and unsolvability of the quintic

Throughout this worksheet, let F be a field of characteristic zero.

Problem F.1. Let K be the splitting field of $x^n - 1$ over F. Show that $\mathrm{Gal}(K/F)$ is abelian.

Problem F.2. Let $c \in F$ and let K be the splitting field of $x^n - c$ over F. Show that $\mathrm{Gal}(K/F)$ is solvable.

A field extension K/F is called ***solvable*** if there is a Galois extension L/F with $K \subseteq L$ and $\mathrm{Gal}(L/F)$ solvable.

Problem F.3. Let K/F be a solvable extension. Let K' be an extension of K which is of the form $K[\theta]$ where $\theta^m \in K$ for some $\theta \in K'$. Show that K'/F is solvable.

Problem F.4. Let F be a field and let K_1/F, K_2/F, $\ldots$, K_r/F be solvable extensions of F. Show that there is a solvable extension M of F into which all the K_j embed. (Hint: See Problem **??**.)

Problem F.5. (**The unsolvability of the quintic**) Let $f(x)$ be a degree 5 separable polynomial in $F[x]$ and let L be the splitting field of f over F. Suppose that $\mathrm{Gal}(L/F)$ is A_5 or S_5. Show that L is not contained in any solvable extension of F.

The point of the next problem is to drive home that we have completed the story of the quintic.

Problem F.6. Let $f(x)$ be a degree 5 separable polynomial in $\mathbb{Q}[x]$ and let L be the splitting field of f over $\mathbb{Q}$. Suppose that $\mathrm{Gal}(L/\mathbb{Q})$ is A_5 or S_5. Show that the roots of f cannot be expressed in terms of rational numbers using $+$, $-$, $\times$, $\div$ and $\sqrt[m]{\ }$.

G. The Galois correspondence

Recall:

Theorem/Definition Let L/K be a field extension of finite degree. The following are equivalent:

(1) We have $\# \operatorname{Aut}(L/K) = [L : K]$.
(2) The fixed field of $\operatorname{Aut}(L/K)$ is K.
(3) For every $\theta \in L$, the minimal polynomial of θ over K is separable and splits in L.
(4) L is the splitting field of a separable polynomial $f(x) \in K[x]$.

A field extension L/K which satisfies these equivalent definitions is called ***Galois***.

Given a subfield F with $K \subseteq F \subseteq L$, we write $\operatorname{Stab}(F)$ for the subgroup of G fixing F; given a subgroup H of $\operatorname{Gal}(L/K)$, we write $\operatorname{Fix}(H)$ for the subfield of L fixed by H. Our next main goal will be to show:

The fundamental Theorem of Galois theory Let L/K be a Galois extension with Galois group G. The maps Stab and Fix are inverse bijections between the set of subgroups of G and the set of intermediate fields F with $K \subseteq F \subseteq L$. Moreover, if $F_1 \subseteq F_2$, then $\operatorname{Stab}(F_1) \supseteq \operatorname{Stab}(F_2)$ and $[\operatorname{Stab}(F_1) : \operatorname{Stab}(F_2)] = [F_2 : F_1]$. If $H_1 \subseteq H_2$ then $\operatorname{Fix}(H_1) \supseteq \operatorname{Fix}(H_2)$ and $[\operatorname{Fix}(H_1) : \operatorname{Fix}(H_2)] = [H_2 : H_1]$.

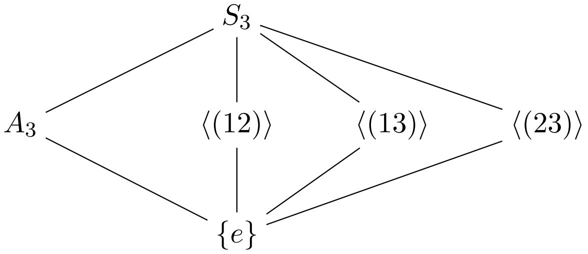
We start by proving some basic results about Fix and Stab.

Problem G.1. (1) Show that, if $F_1 \subseteq F_2$ then $\operatorname{Stab}(F_1) \supseteq \operatorname{Stab}(F_2)$.
(2) Show that, if $H_1 \subseteq H_2$ then $\operatorname{Fix}(H_1) \supseteq \operatorname{Fix}(H_2)$.

Problem G.2. (1) Show that $\operatorname{Stab}(\operatorname{Fix}(H)) \supseteq H$.
(2) Show that $\operatorname{Fix}(\operatorname{Stab}(F)) \supseteq F$.

The Fundamental Theorem tells us that both of the $\supseteq$'s in Problem G.2 are actually equality, but we don't know that yet.

We now give examples. Here is a table of the subgroups of S_3:



Problem G.3. Let $L = \mathbb{Q}(x_1, x_2, x_3)$, let S_3 act on L by permuting the variables and let $K = \operatorname{Fix}(S_3)$. Describe the subfield of L fixed by each of the subgroups of S_3.

Problem G.4. Let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. We number the roots of $x^3 - 2$ as $\sqrt[3]{2}$, $\omega \sqrt[3]{2}$ and $\omega^2 \sqrt[3]{2}$, where ω is a primitive cube root of 1. Described the subfield of L fixed by each of the subgroups of S_3.

Now we prove the theorem!

Problem G.5. Both parts of this problem are things you already did, your job is just to remember when you did them.

(1) Let L/K be a Galois extension. Let F be a field with $K \subseteq F \subseteq L$. Show that $|\operatorname{Stab}(F)| = [L : F]$.
(2) Let L/K be a Galois extension. Let H be a subgroup of $\operatorname{Gal}(L/F)$. Show that $[L : \operatorname{Fix}(H)] = |H|$.

Problem G.6. Prove that the maps Fix and Stab in the Fundamental Theorem are mutually inverse.

Problem G.7. Check the remaining claims of the Fundamental Theorem.