1. The Quadratic, Cubic and Quartic formulas

> *I added up the area of my two squares:* 1300. *The side of one exceeds the side of the other by* 10.
>
> Babylonian tablet, 2000-1600 BCE, British Museum

Problem 1.1. Let $x^2 + bx + c$ be a polynomial with complex coefficients and let its roots be α_1 and α_2. Express the following quantities in terms of α_1 and α_2. In the expressions with a square root, you may choose which square root to use.

$$b \qquad c \qquad b^2 - 4c \qquad \sqrt{b^2 - 4c} \qquad \frac{-b + \sqrt{b^2 - 4c}}{2}.$$

Problem 1.2. Let the symmetric group S_2 act by switching α_1 and α_2. Describe the effect of S_2 on each of the expressions you derived in Problem 1.1.

> *When the cube with the cose beside it / equates itself to some other whole number . . .* Tartaglia, 1543

Let $\omega = \frac{-1+\sqrt{-3}}{2}$; we recall that $\omega^2 + \omega + 1 = 0$ and $\omega^3 = 1$. Let β_1, β_2 and β_3 be complex numbers. Define:

$$\begin{array}{rcrcrcr} s & = & \beta_1 & + & \beta_2 & + & \beta_3 \\ \sigma_1 & = & \beta_1 & + & \omega\beta_2 & + & \omega^2\beta_3 \\ \sigma_2 & = & \beta_1 & + & \omega^2\beta_2 & + & \omega\beta_3 \end{array}$$

Problem 1.3. Let S_3 permute $\beta_1, \beta_2, \beta_3$.

(1) Describe how S_3 acts on $\{\sigma_1,\ \omega\sigma_1,\ \omega^2\sigma_1,\ \sigma_2,\ \omega\sigma_2,\ \omega^2\sigma_2\}$.
(2) Describe how S_3 acts on $\{\sigma_1^3,\ \sigma_2^3\}$.
(3) Show that S_3 fixes s and the coefficients of the quadratic polynomial $y^2 - f_1 y + f_2 := (y - \sigma_1^3)(y - \sigma_2^3)$.

Let $(x - \beta_1)(x - \beta_2)(x - \beta_3) = x^3 - e_1x^2 + e_2x - e_3$. To make your lives easier, here are some useful formulas:

$$\begin{array}{|l|} \hline e_1 = \beta_1 + \beta_2 + \beta_3 \\ e_2 = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 \qquad e_1^2 = \beta_1^2 + 2\beta_1\beta_2 + 2\beta_1\beta_3 + \beta_2^2 + 2\beta_2\beta_3 + \beta_3^2 \\ e_3 = \beta_1\beta_2\beta_3 \qquad e_1e_2 = \beta_1^2\beta_2 + \beta_1^2\beta_3 + \beta_1\beta_2^2 + 6\beta_1\beta_2\beta_3 + \beta_1\beta_3^2 + \beta_2^2\beta_3 + \beta_2\beta_3^2 \\ e_1^3 = \beta_1^3 + 3\beta_1^2\beta_2 + 3\beta_1^2\beta_3 + 3\beta_1\beta_2^2 + 6\beta_1\beta_2\beta_3 + 3\beta_1\beta_3^2 + \beta_2^3 + 3\beta_2^2\beta_3 + 3\beta_2\beta_3^2 + \beta_3^3 \\ \hline \sigma_1\sigma_2 = \beta_1^2 - \beta_1\beta_2 - \beta_1\beta_3 + \beta_2^2 - \beta_2\beta_3 + \beta_3^2 \\ \sigma_1^3 + \sigma_2^3 = 2\beta_1^3 - 3\beta_1^2\beta_2 - 3\beta_1^2\beta_3 - 3\beta_1\beta_2^2 + 12\beta_1\beta_2\beta_3 - 3\beta_1\beta_3^2 + 2\beta_2^3 - 3\beta_2^2\beta_3 - 3\beta_2\beta_3^2 + 2\beta_3^3 \\ \hline \end{array}$$

Problem 1.4. Give formulas for the following, as polynomials in e_1, e_2, e_3:

$$s \qquad \sigma_1\sigma_2 \qquad f_1 \qquad f_2.$$

Problem 1.5. Show that σ_1 and σ_2 can be computed from e_1, e_2, e_3 using the operations $+$, $-$, $\times$, $\sqrt{\ }$ and $\sqrt[3]{\ }$, together with multiplication by rational numbers and the number ω. Show how to likewise compute β_1, β_2 and β_3.

> *Given an equation in which the unknown quantity has four dimensions . . . reduce it to another of the third degree, in the following manner . . .*
>
> Descartes, *La Géometrié*, 1637

Let γ_1, γ_2, γ_3 and γ_4 be complex numbers. Set

$$\begin{array}{rcrcrcrcr} t & = & \gamma_1 & + & \gamma_2 & + & \gamma_3 & + & \gamma_4 \\ \tau_1 & = & \gamma_1 & + & \gamma_2 & - & \gamma_3 & - & \gamma_4 \\ \tau_2 & = & \gamma_1 & - & \gamma_2 & + & \gamma_3 & - & \gamma_4 \\ \tau_3 & = & \gamma_1 & - & \gamma_2 & - & \gamma_3 & + & \gamma_4 \end{array}$$

Problem 1.6. Let S_4 permute $\gamma_1, \gamma_2, \gamma_3, \gamma_4$. Describe how S_4 acts on

(1) $\{\pm\tau_1, \pm\tau_2, \pm\tau_3\}$
(2) $\{\tau_1^2, \tau_2^2, \tau_3^2\}$
(3) Show that S_4 fixes t and the coefficients of the polynomial $(x - \tau_1^2)(x - \tau_2^2)(x - \tau_3^2)$.

Problem 1.7. How would you compute the γ_i from the coefficients of the quartic $\prod(x - \gamma_i)$, using the operations $+$, $-$, $\times$, $\div$ and $\sqrt[n]{\ }$?

2. A WEAK VERSION OF UNSOLVABILITY OF THE QUINTIC

Perhaps it will not be so difficult to prove, with all rigor, the impossibility for the fifth degree.

Karl Freidrich Gauss, 1799

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 $\mathbb{C}(r_1, r_2, \dots, r_5)$. Define e_1, e_2, e_3, e_4, $e_5 \in L$ as the coefficients in

$$(x - r_1)(x - r_2)(x - r_3)(x - r_4)(x - r_5) = x^5 - e_1 x^4 + e_2 x^3 - e_3 x^2 + e_4 x - e_5.$$

Theorem (Ruffini)**.** Starting from e_1, e_2, $\dots$, e_5, it is impossible to obtain the elements r_1, r_2, $\dots$, r_5 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.

Let S_5 act on L by permuting the r_i. Let K be the subfield of L fixed by S_5.

Problem 2.1. Show that the e_j are in K.

Problem 2.2. Set $\Delta = \prod_{i<j}(r_i - r_j)$. Show that $\Delta^2 \in K$ but $\Delta \notin K$.

We define A_5 to be the subgroup of S_5 fixing Δ. 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 $\{i_1, i_2, \dots, i_k\}$.

Problem 2.3. Check that (123), (124) and (125) $\in A_5$.

Problem 2.4. Verify the following identities in the group A_5:

$$(123)^3 = (124)^3 = (125)^3 = \mathrm{Id} \qquad ((123)(124))^2 = ((123)(125))^2 = ((124)(125))^2 = \mathrm{Id}\,.$$

Problem 2.5. Show that there are no nontrivial group homomorphisms from A_5 to an abelian group. You may assume that (123), (124) and (125) generate A_5; you'll check this on the problem set.

Let F be the subfield of L fixed by A_5.

Problem 2.6. Suppose that $f \in L$ is nonzero, and $f^n \in F$. For $\sigma \in A_5$, show that $\frac{\sigma(f)}{f} \in \mathbb{C}^\times$.

Problem 2.7. Let f be as in Problem 2.6. For $\sigma \in A_5$, define $\chi_f(\sigma) = \frac{\sigma(f)}{f}$. Show that $\chi_f : A_5 \to \mathbb{C}^\times$ is a group homomorphism.

Problem 2.8. Show that, if $f \in L$ and $f^n \in F$, then $f \in F$.

Problem 2.9. Prove Ruffini's Theorem.

History, and plan of the course: Paolo Ruffini, *Teoria generale delle equazioni*, 1799 gave what, in modern language, is a proof of this result. His work was difficult to understand, and the assumption that one would not leave $\mathbb{C}(r_1, \dots, r_5)$ when extracting n-th roots was only stated implicitly. Calling this result Ruffini's Theorem is not standard, but seems appropriate.

Abel replaced the use of rational functions with multivalued complex analytic functions of the r_j. He proved the corresponding result with no restriction on taking roots in 1824, just four years prior to his death of tuberculosis at age 26. Because the foundations of complex analysis were not yet settled, his work was also hard to follow. He died only four years later of tuberculosis. The unsolvability of the quintic is now known as the Abel-Ruffini Theorem.

Neither Abel nor Ruffini was able to prove that the roots of a particular quintic with, for example, rational coefficients, were not expressible in terms of the coefficients of that quintic; that would wait for Galois in 1831, just a year before his death in a duel at age 20. Our course will follow the ideas of Galois.

We can see from these early attempts that the lack of a notion of adjoining an n-th root to an arbitrary field, without some ambient field to work inside, was a major obstacle to clear proofs. For this reason, we will be studying abstract fields. That will require replacing the groups S_n and A_n with general abstract groups, so first we will study groups.

Abel has left mathematicians enough to keep them busy for 500 years. Atttributed to Charles Hermite.

3. 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 3.1. Show that a group G only has one element 1 obeying the condition (1).

Problem 3.2. 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 3.3. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi(1) = 1$ and $\phi(g^{-1}) = \phi(g)^{-1}$.

Problem 3.4. 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 3.5. 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:

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

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 will often denote $*$ by $+$ and 1 by 0. We will **never** use these notations for a non-abelian group.

Problem 3.6. Let G be a group. Show that G is abelian if and only if:

1. The map $g \mapsto g^{-1}$ is a group homomorphism.
2. The map $g \mapsto g^2$ is a group homomorphism.
3. The map $\mu : G \times G \to G$ by $\mu(g, h) = g * h$ is a group homomorphism.

We'll toss in one more definition:

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

4. 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 4.1. 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 4.2. 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 4.3. With G, X and x as above, show that $\mathrm{Stab}(x)$ is a subgroup of X.

Problem 4.4. 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 4.5. (**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 4.6. (**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 4.7. Show that G has a left action on the set G/H of left cosets, such that $g_1 * (g_2H) = (g_1 * g_2)H$. Show that the stabilizer of the coset eH is H.

Problem 4.8. (**Lagrange's Theorem**[2]) Let G be a finite group and let H be a subgroup. Show that $\#(H)$ divides $\#(G)$.

Problem 4.9. 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.

5. Normal subgroups, quotient groups, short exact sequences

Problem 5.1. 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) All elements of G/N have the same stabilizer, for the left action of G on G/N.
(3) Every left coset of N in G is also a right coset.
(4) If $g_1 N = g_1' N$ and $g_2 N = g_2' N$, then $g_1 g_2 N = g_1' g_2' N$.

Definition. A subgroup N obeying the equivalent conditions of Problem 5.1 is called a ***normal subgroup*** of G. We write $N \trianglelefteq G$ to indicate that N is a normal subgroup of G.

Problem 5.2. 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 5.3. 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 an 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 $(g_1 N)(g_2 N) = g_1 g_2 N$.

This definition makes sense by Part (4) of Problem 5.1. 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 5.4. Show that the kernel of ϕ is a normal subgroup of G.

Problem 5.5. 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 5.6. Show that there is a short exact sequence $1 \to C_m \to C_{mn} \to C_n \to 1$.

Problem 5.7. Show that there is a short exact sequence $1 \to C_3 \to S_3 \to S_2 \to 1$.

Problem 5.8. Show that there is a short exact sequence $1 \to C_2^2 \to S_4 \to S_3 \to 1$.

Problem 5.9. What is the relationship between Problems 5.7 and 5.8 and your computations on the first day of class involving $\{(\beta_1 + \omega\beta_2 + \omega^2\beta_3)^3,\ (\beta_1 + \omega^2\beta_2 + \omega\beta_3)^3\}$ and $\{(\gamma_1 + \gamma_2 - \gamma_3 - \gamma_4)^2,\ (\gamma_1 - \gamma_2 + \gamma_3 - \gamma_4)^2,\ (\gamma_1 - \gamma_2 - \gamma_3 + \gamma_4)^2\}$?

6. 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 6.1. Let G be simple and let H be any group. Show that, for every group homomorphism $\phi : G \to H$, either ϕ is injective or else ϕ is trivial.

Problem 6.2. Let p be a prime. Show that C_p is simple.

Problem 6.3. In this problem, we use a slick trick to check that A_5 is simple. The conjugacy classes of A_5 are as follows. (You may trust this; it will probably show up on homework eventually.)

representative element	e	(123)	$(12)(34)$	(12345)	(12354)
size of conjugacy class	1	20	15	12	12

(1) Show that any normal subgroup of A_5 must have size contained in the list

$$\left\{ \begin{array}{c} 1,\ 1+12,\ 1+15,\ 1+20, \\ 1+12+12,\ 1+12+15,\ 1+12+20,\ 1+15+20, \\ 1+12+12+15,\ 1+12+12+20,\ 1+12+15+20, \\ 1+12+12+15+20 \end{array} \right\} = \{1,\ 13,\ 16,\ 21,\ 25,\ 28,\ 33,\ 36,\ 40,\ 45,\ 48,\ 60\}.$$

(2) Explain why the only possibilities in this list which can occur are 1 and 60.

Problem 6.4. Let G_1 and G_2 be simple groups and let N be a normal subgroup of $G_1 \times G_2$. Prove that one of the following cases must hold:

I: $N = \{1\}$
II: $N = G_1 \times \{1\}$
III: $N = \{1\} \times G_2$
IV: $N = G_1 \times G_2$ or
V: $G_1 \cong G_2$ and $N = \{(g, \phi(g)) : g \in G_1\}$ where $\phi : G_1 \to G_2$ is an isomorphism.

Hint: Think of ways to use N to make subgroups of G_1 and G_2.

Problem 6.5. Let G be a group and let N_1 and N_2 be distinct normal subgroups of G such that G/N_1 and G/N_2 are simple. Show that $G/(N_1 \cap N_2) \cong G/N_1 \times G/N_2$. Hint: What can the image of G in $G/N_1 \times G/N_2$ be?

After the prime cyclic groups C_p, the two most important families of simple groups are the alternating groups A_n (for $n \geq 5$), and the projective special linear groups $\mathrm{PSL}_n(F)$ (other than $\mathrm{PSL}_2(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_3)$). Here, for any field F, the group $\mathrm{PSL}_n(F)$ is defined to be $\mathrm{SL}_n(F)/\,\mathrm{SL}_n(F) \cap Z$ where $\mathrm{SL}_n(F)$ is $n \times n$ matrices with determinant 1 and Z is matrices of the form $z \,\mathrm{Id}_n$ for $z \in F^\times$.

All proofs that these groups are simple are a bit lengthy; I have not decided to what extent we will prove this claim.

7. Subnormal series, composition series and the Jordan-Holder theorem

Today, we are going to want the result of Problem 6.5, so we repeat it:

Problem 6.5 again: Let G be a group and let N_1 and N_2 be distinct normal subgroups of G such that G/N_1 and G/N_2 are simple. Show that $G/(N_1 \cap N_2) \cong G/N_1 \times G/N_2$. Hint: What can the image of G in $G/N_1 \times G/N_2$ be?

Definition. A ***subnormal series*** of a group G is a chain of subgroups $G = G_0 \rhd G_1 \rhd G_2 \rhd G_3 \rhd \cdots \rhd G_N = \{e\}$ where G_{j+1} is normal in G_j. A ***composition series*** is a subnormal series where each subquotient G_j/G_{j+1} is simple.

Problem 7.1. Show that every finite group has a composition series.

Problem 7.2. Show that S_4 has a composition series with subquotients C_2, C_3, C_2 and C_2.

Problem 7.3. Show that $\mathrm{GL}_2(\mathbb{F}_7)$ has a composition series with subquotients C_2, C_3, $\mathrm{PSL}_2(\mathbb{F}_7)$ and C_2. You may assume that $\mathrm{PSL}_2(\mathbb{F}_7)$ is simple.

Problem 7.4. Let G be a group with a composition series and let N be a normal subgroup of G. Show that N and G/N have composition series.

The aim of this worksheet is to prove:

Theorem (Jordan-Holder)**.** Let G be a group with two composition series $G_0 \rhd G_1 \rhd \cdots \rhd G_M = \{e\}$ and $H_0 \rhd H_1 \rhd \cdots \rhd H_N = \{e\}$. Then $M = N$ and the list of subquotents $(G_0/G_1, G_1/G_2, \ldots, G_{M-1}/G_M)$ is a permutation of $(H_0/H_1, H_1/H_2, \ldots, H_{N-1}/H_N)$.

Our proof will be by induction on $\min(M, N)$.

Problem 7.5. Prove the base case, where $\min(M, N) = 0$.

Problem 7.6. Explain why we are done if $G_1 = H_1$.

Problem 7.7. Suppose that $G_1 \neq H_1$. Explain how to finish the proof in this case.

The Jordan-Holder theorem gives the basic strategy for studying groups: Understand the simple groups, and understand how they can be assembled into short exact sequences.

8. Semidirect products

Let A be a group and let C be a group with a left action on A by a map $\phi : C \to \mathrm{Aut}(A)$. In other words, we require that $\phi(c)(a_1 * a_2) = \phi(c)(a_1) * \phi(c)(a_2)$ as well as the usual left action axiom that $\phi(c_1 c_2)(a) = \phi(c_1)\big(\phi(c_2)(a)\big)$.

Definition. With the above notation, the ***semidirect product*** $A \rtimes_\phi C$ is defined as the set of ordered pairs $(a, c) \in A \times C$ with multiplication $(a_1, c_1) * (a_2, c_2) = (a_1 * \phi(c_1)(a_2),\ c_1 * c_2)$.

The subscript ϕ is often omitted when it is clear from context.

Note that we use a left action of C on A to define $A \rtimes C$. Likewise, given a right action of C on A, we define $C \ltimes A$. This may seem odd, but I promise it is less confusing this way.

Problem 8.1. Verify that $A \rtimes_\phi C$ is a group.

Problem 8.2. In the above setting, show that:

(1) $\{(a, 1)\}$ is a normal subgroup of $A \rtimes_\phi C$, isomorphic to A.
(2) $\{(1, c)\}$ is a subgroup of $A \rtimes_\phi C$, isomorphic to C.
(3) $\{(a, 1)\} \cap \{(1, c)\} = \{(1, 1)\}$.
(4) Every element of $A \rtimes_\phi C$ can be written uniquely in the form $(a, 1)(1, c)$ for $a \in A$, $c \in C$.

Problem 8.3. Let G be a group with subgroups A and C such that, for $c \in C$, we have $cAc^{-1} = A$. When this condition holds, we say that C ***normalizes*** A.

(1) Show that $\{ac : a \in A,\ c \in C\}$ is a subgroup of G. We call this subgroup AC.
(2) Suppose, in addition that $A \cap C = \{1\}$. Show that[1] $AC \cong A \rtimes C$.
(3) Suppose that $A \cap C = \{1\}$ and both that A normalizes C and C normalizes A. Show that $AC \cong A \times C$.

The rest of the worksheet is examples.

Problem 8.4. 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 8.5. Let p be prime. Show that $C_{p^2} \ncong C_p \rtimes C_p$ for any action of C_p on C_p.

Let k be a field and let V be a k vector space; we'll write V_+ for V considered as an additive group. Let $\mathrm{GL}(V)$ be a group of invertible k-linear maps $V \to V$. Let $\mathrm{Aff}(V)$ be the group of maps $V \to V$ of the form $\vec{v} \mapsto a\vec{v} + \vec{b}$ for $a \in \mathrm{GL}(V)$ and $\vec{b} \in V$.

Problem 8.6. Show that $\mathrm{Aff}(V) \cong V_+ \rtimes \mathrm{GL}(V)$.

Problem 8.7. Let $\dim_k V = n$. Show that $\mathrm{Aff}(V)$ is isomorphic to the group of $(n+1) \times (n+1)$ matrices of the form

$$\begin{bmatrix} * & * & \cdots & * & * \\ * & * & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & \cdots & * & * \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

[1] It is possible that $G = AC$ and $A \cap C = \{1\}$, yet neither of A nor C normalizes each other. An example is $G = S_4$ with A the three element subgroup generated by (123) and C the eight element subgroup generated by (1234) and $(12)(34)$. In this case, we do not get to write G as a semidirect product.

9. Abelianization and the commutator subgroup

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

Problem 9.1. Show that $[G, G]$ is normal in G.

Problem 9.2. Show that $G/[G, G]$ is abelian.

Definition. The quotient $G/[G, G]$ is called the ***abelianization*** of G and denoted G^{ab}.

Problem 9.3. 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:

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

Problem 9.4. Show that the commutator subgroup of S_n is A_n.

Problem 9.5. Show that the commutator subgroup of A_n is A_n for $n \geq 5$.

Remark. Way back in Problem 2.5, you showed that there are no nontrivial homomorphisms from A_5 to an abelian group. We can now state that result in a more sophisticated sounding way: The abelianization of A_5 is trivial.

Problem 9.6. Suppose that we have a short exact sequence $1 \to H \to G \to A \to 1$ where A is abelian. Show that $[G, G] \subseteq H$.

Problem 9.7. Many people believe that the every element in the commutator subgroup is of the form $ghg^{-1}h^{-1}$. This is need not be true. Let V be a vector space of dimension ≥ 4 over a field of characteristic $\neq 2$ and let G be the group whose underlying set is $V \times \bigwedge^2(V)$, with multiplication:

$$(v, \alpha) * (w, \beta) = (v + w, \alpha + \beta + v \wedge w).$$

You checked on the problem sets that G is a group.

(1) Show that $(0, \alpha)$ is a commutator if and only if α is of the form $v \wedge w$.
(2) Show that the commutator subgroup is all pairs $(0, \alpha)$ for $\alpha \in \bigwedge^2 V$.

10. Solvable groups

We recall that the commutator subgroup $[G, G]$ of a group G is the subgroup generated by all products $ghg^{-1}h^{-1}$.

Definition. The ***derived series*** of G is the sequence of subgroups $D_0(G) \supseteq D_1(G) \supseteq D_2(G) \supseteq \cdots$ defined inductively by $D_0(G) = G$ and $D_k(G) = [D_{k-1}(G),\ D_{k-1}(G)]$. We call $D_k(G)$ the ***k-th derived subgroup***.

Remark. The k-derived subgroup is often also denoted $G^{(k)}$. The parentheses in $G^{(k)}$ is meant to distinguish $G^{(k)}$ from the k-fold product of G with itself. Professor Speyer recommends, instead, using words to do this: Say "let $G^{(k)}$ be the k-th derived subgroup ..." or "let G^k be the k-fold product of G with itself ...."

Problem 10.1. Check that the derived series of S_4 is $S_4 \supset A_4 \supset V \supset \{e\}$ where V is the four element group generated by $(12)(34)$ and $(13)(24)$.

Definition. A group G is called ***solvable*** if there is some index N such that the N-th derived subgroup is trivial.

Problem 10.2. Show that a group G is solvable if and only if it has a subnormal series in which each subquotient is abelian.

Problem 10.3. Show that subgroups of solvable groups are solvable.

Problem 10.4. Show that quotients of solvable groups are solvable.

Problem 10.5. Let $1 \to A \to B \to C \to 1$ be a short exact sequence with A and C solvable. Show that B is solvable.

Problem 10.6. Let G be the group of bijections $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ of the form $x \mapsto ax + b$. Show that G is solvable.

Problem 10.7. Let k be a field and let B be the group of invertible upper triangular $n \times n$ matrices with entries in k. Show that B is solvable.

11. Center, central series and nilpotent groups

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

Problem 11.1. Let G be a group.

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

Problem 11.2. Let k be a field and let U be the group of matrices with entries in k of the form $\left[\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right]$. Show that the center of U is the group of matrices of the form $\left[\begin{smallmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$.

Problem 11.3. Check that the center of S_n is trivial for $n \geq 3$.

Problem 11.4. Let F be a field with more than two elements. Let B be the group of matrices of the form $\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]$. Show that the center of F is $\{\left[\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right] : z \in F^{\times}\}$.

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

Problem 11.5. Let p be a prime and let G be a group of order p^k for some $k \geq 1$. 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 $G_N = G$.

Remark. In many sources, a central series is required to have $G_0 = \{e\}$ and $G_N = G$, but then the "upper central series" and the "lower central series", which you will meet on the problem sets, are not central series. I prefer to take the more general definition.

Problem 11.6. 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 11.7. 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 11.8. 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.

Problem 11.9. Show that a nilpotent group is solvable.

Problem 11.10. Show that a subgroup of a nilpotent group is nilpotent.

Problem 11.11. Show that a quotient of a nilpotent group is nilpotent.

Problem 11.12. Show that the following groups are solvable but not nilpotent.

(1) The symmetric groups S_3 and S_4.
(2) The group of invertible matrices of the form $\left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]$ with entries in a field with more than two elements.

Problem 11.13. Give an example of a short exact sequence $1 \to A \to B \to C \to 1$ with A and C nilpotent but B not nilpotent.

12. 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 12.1. 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.

Large parts of the following problems appeared on the homework; please remind each other of the solutions.

Problem 12.2. Let $\mathrm{GL}_n(\mathbb{F}_p)$ be the group of $n \times n$ matrices with entries in the field with p elements.

(1) Show that $\# \mathrm{GL}_n(\mathbb{F}_p) = \prod_{j=0}^{n-1}(p^n - p^j)$.
(2) Show that $\mathrm{GL}_n(\mathbb{F}_p)$ has a Sylow p-subgroup.

Problem 12.3. Let $v(n)$ be the exponent such that $n! = p^{v(n)}m$ with p not dividing m.

(1) Write $n = pm + r$ with $0 \leq r \leq p-1$. Show that $v(n) = m + v(m)$.
(2) Show that S_n has a Sylow p-subgroup.

Problem 12.4. 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 12.4.

Problem 12.5. (**The first Sylow theorem**) Show that every finite group G has a Sylow p-subgroup.

Problem 12.6. 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 12.7. (**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 12.8. 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 12.9. (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 12.10. 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 12.11. (**The third Sylow theorem**) The number of Sylow p-subgroups of G is $\equiv 1 \bmod p$.

13. Some problems with Sylow groups

Problem 13.1. 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 13.2. 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 13.3. 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 13.4. 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 13.5. Show that there are no simple groups of order 40. (Hint: Look at 5-Sylows.)

Problem 13.6. 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 13.7. Recall that, for a subgroup H of a group G, the normalizer $N_G(H)$ is defined to be $\{g \in G : gHg^{-1} = H\}$. Let G be a finite group and P a p-Sylow subgroup of G.

(1) Show that P is canonical in $N_G(P)$.
(2) Show that $N_G(N_G(P)) = N_G(P)$.

Problem 13.8. Let G be a finite nilpotent group. On the homework you showed/will show that, if $H \subsetneq G$ is a proper subgroup, then $N_G(H) \supsetneq H$.

(1) Show that every Sylow p-subgroup of a finite nilpotent group G is normal.
(2) Let P and Q be Sylow subgroups of G for different primes, p and q. Show that, if $g \in P$ and $h \in Q$, then $gh = hg$.
(3) Let G_p be the Sylow p-subgroup of G. Show that $G \cong \prod G_p$, where the right hand side is the direct product.

In other words, every finite nilpotent group is the direct product of its Sylow subgroups.

Problem 13.9. Let $1 \to A \to B \xrightarrow{\beta} C \to 1$ and let P be a Sylow p-subgroup of A. We'll identify A with its image in B.

(1) (**Frattini's argument**) Show that $B = AN_B(P)$. Hint: Let $b \in B$. What can you say about nPb^{-1}?
(2) Show that $N_B(P) \xrightarrow{\beta} C$ is surjective.
(3) Show that $1 \to N_A(P) \to N_B(P) \to C \to 1$ is exact.

14. 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:

Today's goal: 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 14.1. 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 14.2. 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 14.3. 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 14.4. 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 14.5. 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 14.6. 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 14.7. 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 14.8. 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.

Remark. For this remark, I'll switch to writing A additively. There are useful situations where A is infinite but we can still show $a \mapsto na$ is bijective. For example, we can consider $0 \to V \to B \to C \to 1$ where C is finite and V is a vector space over a field of characteristic zero. A more sophisticated examples is short exact sequences of Lie groups $0 \to \mathbb{R}^k \to G \to K \to 1$ where K is compact; here we replace the product in $(*)$ with $\int_{k \in K} \sigma_1(k)\sigma_2^{-1}(k)$.

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

15. 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. On the previous worksheet, we showed that (A, C) is straightforward if A is abelian and $\mathrm{GCD}(\#(A), \#(C)) = 1$.

Problem 15.1. 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 15.2. 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 15.3. Show that P is canonical in $N_A(P)$.

Problem 15.4. 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 15.5. (**Frattini's argument**) Show that $B = AN_B(P)$. Hint: Let $b \in B$. What can you say about bPb^{-1}?

Problem 15.6. 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 15.7. Show that $1 \to A \to B \to C \to 1$ is right split.

Remark. Problem 15.1 has uses outside of finite groups. For example, let K be a compact Lie group and let U be a simply connected nilpotent Lie group. An analogous argument shows that (U, K) is straightforward.

16. SIMPLICITY OF $\mathrm{PSL}_n(F)$

The three most important families of simple groups are

- The cyclic groups C_p for p prime.
- The alternating groups A_n for $n \geq 5$.
- The projective special linear groups $\mathrm{PSL}_n(F)$, except for $\mathrm{PSL}_2(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_3)$.

In this worksheet, we'll show $\mathrm{PSL}_n(F)$ is simple for $\#(F) > 5$. The fields of orders 2, 3, 4 and 5 are not deeper, but the details are messier.

Let F be a field. The groups $\mathrm{GL}_n(F)$ and $\mathrm{SL}_n(F)$ are the groups of $n \times n$ matrices with entries in F which, respectively, have nonzero determinant and have determinant 1. Let Z be the group of matrices of the form $z \, \mathrm{Id}_n$, for $z \in F^{\times}$. The ***projective general linear group*** and ***projective special linear group*** are, respectively, $\mathrm{PGL}_n(F) := \mathrm{GL}_n(F)/Z$ and $\mathrm{PSL}_n(F) := \mathrm{SL}_n(F)/(Z \cap \mathrm{SL}_n(F))$.

For $1 \leq i \neq j \leq n$ and $r \in F$, the matrix $E_{ij}(r)$ is the $n \times n$ matrix with ones on the diagonal, an r in position (i, j) and zeroes everywhere else. A matrix of the form $E_{ij}(r)$ is called an ***elementary matrix***. We proved in 593 (and you may use) that the elementary matrices generate $\mathrm{SL}_n(F)$ for any F.

Problem 16.1. Let N be a normal subgroup of $\mathrm{SL}_n(F)$. Suppose that there a pair of indices (a, b) so that N contains all the matrices $E_{ab}(r)$. Show that $N = \mathrm{SL}_n(F)$.

A ***companion matrix*** is a matrix of the form

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & * \\ 1 & 0 & 0 & \cdots & * \\ 0 & 1 & 0 & \cdots & * \\ 0 & 0 & \ddots & \cdots & * \\ 0 & 0 & \cdots & 1 & * \end{bmatrix}.$$

By the Rational Canonical Form Theorem, for $\alpha \in \mathrm{GL}_n(F)$, there is $g \in \mathrm{GL}_n(F)$ such that $g\alpha g^{-1}$ is block diagonal with blocks that are companion matrices and, furthermore, we can take the largest block to have size equal to the degree of the minimal polynomial of α. We will want a variant of this for $\mathrm{SL}_n(F)$.

Problem 16.2. Define a ***generalized companion matrix*** to be an $m \times m$ matrix of the form

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & * \\ * & 0 & 0 & \cdots & * \\ 0 & * & 0 & \cdots & * \\ 0 & 0 & \ddots & \cdots & * \\ 0 & 0 & \cdots & * & * \end{bmatrix}.$$

(1) Let $\alpha \in \mathrm{SL}_n(F)$. Show that there is $h \in \mathrm{SL}_n(F)$ such that $h\alpha h^{-1}$ is block diagonal with blocks that are generalized companion matrices.
(2) If $\alpha \notin Z$, show furthermore that we can assume the largest block has size ≥ 2.

Problem 16.3. Let β be an $m \times m$ generalized companion matrix for $m \geq 2$. Assume that $\#(F) > 5$. Show that we can find a diagonal matrix $d \in \mathrm{SL}_n(F)$ such that $d^{-1}\beta^{-1}d\beta$ is of the form

$$\begin{bmatrix} \gamma_1 & 0 & 0 & \cdots & * \\ 0 & \gamma_2 & 0 & \cdots & * \\ 0 & 0 & \gamma_3 & \cdots & * \\ 0 & 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \cdots & \gamma_m \end{bmatrix} \qquad (*)$$

with $\gamma_1 \neq \gamma_m$. Hint: I found it helpful to write

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & * \\ * & 0 & 0 & \cdots & * \\ 0 & * & 0 & \cdots & * \\ 0 & 0 & \ddots & \cdots & * \\ 0 & 0 & \cdots & * & * \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} * & 0 & 0 & \cdots & * \\ 0 & * & 0 & \cdots & * \\ 0 & 0 & \ddots & \cdots & * \\ 0 & 0 & \cdots & * & * \\ 0 & 0 & 0 & \cdots & * \end{bmatrix}.$$

Problem 16.4. Let $m \geq 2$ and let N be a normal subgroup of $\mathrm{SL}_m(F)$ containing a matrix γ of the form $(*)$ with $\gamma_1 \neq \gamma_m$. Show that N contains all matrices of the form $E_{1m}(r)$. Hint: Compute $\gamma^{-1}E_{1m}(s)^{-1}\gamma E_{1m}(s)$.

Problem 16.5. Let $\#(F) > 5$ and let N be a normal subgroup of $\mathrm{SL}_n(F)$ not contained in Z. Show $N = \mathrm{SL}_n(F)$.

Problem 16.6. Let $\#(F) > 5$. Show that $\mathrm{PSL}_n(F)$ is simple.

Remark. The assumption that $\#(F) > 5$ was used in Problem 16.3. A case by case analysis can derive the same conclusion for $\#(F) = 4$, 5 and for $\#(F) = 3$ with $n \geq 3$. If $\#(F) = 2$, it is impossible to have $\gamma_1 \neq \gamma_m$, but a case by case analysis can show that, for $n \geq 3$ a normal subgroup of $\mathrm{SL}_n(\mathbb{F}_2)$ containing a generalized companion matrix with a block of size ≥ 2 contains an elementary matrix, and then the proof finishes as before.

Remark. The slickest proof that $\mathrm{PSL}_n(F)$ is simple uses Iwasawa's Criterion, but that is not closely related to other material we have covered. See Keith Conrad's lecture notes at `https://kconrad.math.uconn.edu/blurbs/grouptheory/PSLnsimple.pdf` for a good exposition of that approach.

Remark. $\mathrm{PSL}_n(F)$ is an example of a "group of Lie type", which roughly means to take a complex simple Lie group like $\mathrm{PSL}_n(\mathbb{C})$ and make "the same definition over a general field". The complex simple Lie groups are classified. A given complex simple Lie group can correspond to more than one group of Lie type, but the groups of Lie type are also classified. The Classification of Finite Simple Groups says that every finite simple group is either cyclic, alternating, of Lie type, or in a list of 26 sporadic examples. The status of the CFSG is a little unclear; a proof was announced in 1983, with the argument spread over hundreds of papers occupying tens of thousands of pages. Two gaps in the argument were found, and fixed in 2004 and 2008 respectively, and no new ones have been found since then. Group theorists are currently at work to produce a shorter, cohesive proof.

17. Review of polynomial rings

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

Problem 17.1. 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

$$a(x) = b(x)q(x) + r(x).$$

In other words, $k[x]$ is a Euclidean ring with respect to the norm of degree. As you hopefully remember, this means that $k[x]$ is a PID and a UFD, and we can compute GCD's using the Euclidean algorithm.

Problem 17.2. 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.

Problem 17.3. Use the Euclidean algorithm to compute the GCD of $t^3 + t$ and $t^4 - 1$ in $\mathbb{Q}[t]$

Problem 17.4. Use the Euclidean algorithm to find polynomials $f(t)$ and $g(t) \in \mathbb{Q}[t]$ such that

$$f(t)(t^2 + t + 2) + g(t)(t^3 - 2) = 1.$$

Problem 17.5. Let $b(x)$ be an irreducible polynomial in $k[x]$. Show that $k[x]/b(x)k[x]$ is a field.

Problem 17.6. The polynomial $t^3 - 2$ is irreducible in $\mathbb{Q}[t]$, so the previous problem says that $\mathbb{Q}[t]/(t^3 - 2)\mathbb{Q}[t]$ is a field. Compute $(t^2 + t + 2)^{-1}$ in this field.

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

(1) Show that I is an ideal.
(2) Show that $I = m(t)k[t]$ for some irreducible polynomial m.
(3) 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 17.8. Show that θ is algebraic over k if and only if $\dim_k k[\theta] < \infty$.

Problem 17.9. Show that the set of elements of K which are algebraic over k is a subfield of K.

18. 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 18.1. 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 18.2. 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.

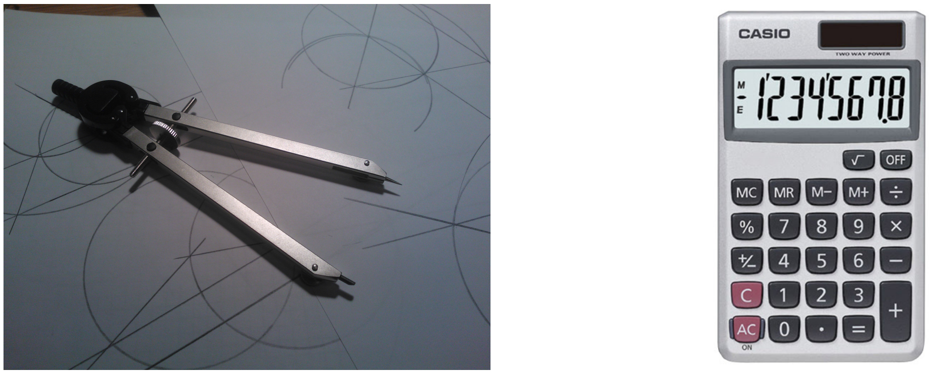


Figure: Two ancient mathematical tools

Problem 18.3. Suppose we compute a sequence of real numbers θ_1, θ_2, θ_3, …, θ_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 18.4. 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 18.5. (**The impossibility of doubling the cube**.) Show that $\sqrt[3]{2}$ is not constructible.

Problem 18.6. (**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:

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

19. SPLITTING FIELDS

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 θ_1, θ_2, …, θ_n are the roots of $f(x)$ in $\mathbb{C}$, then $\mathbb{Q}[\theta_1,\ldots,\theta_n]$ is a splitting field of $f(x)$.

Problem 19.1. Let k be a field and let $f(x)$ be a polynomial in $k[x]$. Show that f has a splitting field. (Please do not use that every field has an algebraic closure. That is a much[1] harder result than this one.)

Problem 19.2. 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.[2] 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 19.3. 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 $\mathbb{R}$.)

This is a good time to discuss separable polynomials.

Definition: Let k be a field and let $f(x)$ be a polynomial in $k[x]$. We say f is ***separable*** if $\mathrm{GCD}(f(x),f'(x))=1$.

Problem 19.4. Let k be a field, let $f(x)$ be a polynomial in $k[x]$ and let K be a field where f splits as $c\prod_{j=1}^{n}(x-\theta_j)$. Show that f is separable if and only if θ_1, θ_2, …, θ_n are distinct.

Problem 19.5. Let k be a field of characteristic zero.

(1) Show that a polynomial in $k[x]$ is separable if and only if it is square free.
(2) Show that irreducible polynomials in $k[x]$ are separable.

[1] In particular, the fact that every field embeds in an algebraically closed field uses the Axiom of Choice, and this problem does not.

[2] The most straightforward way to check this is to use the rational root theorem. The slickest is to note that $f(x+1)=\frac{1}{8}(8x^3+28x^2+28x+7)$ and apply Eisenstein's irreducibility theorem.

20. Maps between splitting fields

Problem 20.1. Let k be a field, let $f(x)$ be an irreducible polynomial in $k[x]$ and let L be an extension of k in which f has a root θ. Show that there is an injection $\phi : k[x]/f(x)k[x] \to L$ with $\phi(x) = \theta$ making the diagram

$$\begin{tikzcd}
k \arrow[d] \arrow[dr] & \\
k[x]/f(x)k[x] \arrow[r, dashed, "\phi"] & L
\end{tikzcd}$$

commute.

We recall the definition

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.

Problem 20.2. 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 $\prod(x - \alpha_j)$. and let L be a field in which f splits as $\prod(x - \beta_j)$. Show that there is an injection $\phi : K \to L$ making the diagram

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

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

Problem 20.3. 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.

Problem 20.4. Let k be a field, let $f(x) = \sum f_j x^j$ be a polynomial in $k[x]$ and let σ be an automorphism of k. 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

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

commute.

21. 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 $\operatorname{Aut}(L)$ for the automorphisms of L and $\operatorname{Aut}(L/K)$ for the automorphisms of L fixing K.

Problem 21.1. 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 $\operatorname{Aut}(L/K)$ maps $\{\theta_1, \theta_2, \dots, \theta_r\}$ to itself.
(2) Show that stabilizer of θ_j in $\operatorname{Aut}(L/K)$ is $\operatorname{Aut}(L/K(\theta_j))$.

Problem 21.2. . Let K be a field, let f be a separable 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. Show that the action of $\operatorname{Aut}(L/K)$ on $\{\theta_1, \theta_2, \dots, \theta_n\}$ gives an **injection** $\operatorname{Aut}(L/K) \hookrightarrow S_n$.

Problem 21.3. Let K, f, L and $\{\theta_1, \theta_2, \dots, \theta_n\}$ be as in Problem 21.2. 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 $\operatorname{Aut}(L/K)$-orbit of θ_1 in L. Hint: Apply Problem 20.4 to the diagram

$$\begin{tikzcd}
K[\theta_1] \arrow[d] & K[x]/g(x)K[x] \arrow[l, "\cong"'] \arrow[r, "\cong"] & K[\theta_j] \arrow[d] \\
L \arrow[rr, dashed] & & L
\end{tikzcd}$$

Problem 21.4. Let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Show that $\operatorname{Aut}(L/\mathbb{Q}) \cong S_3$.

Problem 21.5. Let $L = \mathbb{Q}(\cos \frac{2\pi}{7})$. Show that $\operatorname{Aut}(L/\mathbb{Q}) \cong C_3$.

22. Galois extensions

Problem 22.1. 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) Show that we have equality if and only if g is separable and g splits in L.

Problem 22.2. 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 22.2. This is answered by the following:

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

(1) We have $\#\,\mathrm{Aut}(L/K) = [L : K]$.
(2) The fixed field of $\mathrm{Aut}(L/K)$ 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***.

The next four problems prove this theorem.

Problem 22.3. Show that (1) implies (2).

Problem 22.4. Let $\theta \in L$ and let $\{\theta_1, \theta_2, \ldots, \theta_r\}$ be the orbit of θ under $\mathrm{Aut}(L/K)$. Let $f(x) = \prod_j (x - \theta_j)$.

(1) Assuming condition (2), Show that $f(x) \in K[x]$.
(2) Continuing to assume (2), show that $f(x)$ is the minimal polynomial of θ over K.
(3) Deduce that (2) implies (3).

Remark. The fact that, in a Galois extension, the minimal polynomial of θ is $\prod_{\theta' \in \mathrm{Aut}(L/K)\theta} (x - \theta')$ will be useful many times again.

Problem 22.5. Show that (3) implies (4).

Problem 22.6. Show that (4) implies (1).

Definition When L/K is Galois, we denote $\mathrm{Aut}(L/K)$ by $\mathrm{Gal}(L/K)$ and call it the ***Galois group of*** L ***over*** K.

23. Separability, Galois closure, perfect fields

Remark: This worksheet covers a number of topics which are often glossed over in first courses on Galois theory. We could afford to gloss over them too, but this seems like the natural spot for them.

Definition Let $K \subseteq L$ be an extension of fields. An element $\theta \in L$ is called ***separable*** over K if θ is algebraic over K and the minimal polynomial of θ over K is a separable polynomial. The extension L/K is called ***separable*** if it is generated by separable elements.

Problem 23.1. Show that, if K has characteristic zero then every finite degree extension of K is separable.

So, in characteristic zero, the "separable" condition usually comes for free. At the end of the worksheet, we'll return to think harder about separability in characteristic p.

Problem 23.2. Let L/K be a separable field extension; specifically, let $\theta_1, \dots, \theta_N$ be separable elements generating L/K and let $g_j(x)$ be the (separable) minimal polynomial of θ_j over K. Let M be the splitting field of $\prod_j g_j(x)$ over K. Show that M/K is Galois.

The field M is what we will eventually call ***the Galois closure of*** L/K, but we haven't proved any uniqueness properties of it yet. Before we address that, some more basic things.

Problem 23.3. Let K, L and M be as in the previous problem. Show that every element of M is separable over K.

Problem 23.4. Let L/K be a separable field extension. Show that every element of L is separable over K.

We now address the uniqueness of the Galois closure.

Problem 23.5. Let K, L and M be as in the previous problem. Let $L \subseteq Q$ be a field extension such that Q/K is Galois. Show that there is an injection $M \hookrightarrow Q$ making the diagram

$$\begin{tikzcd}
K \arrow[r, phantom, "\subseteq"] \arrow[d, equal] & L \arrow[r, phantom, "\subseteq"] \arrow[d, equal] & M \arrow[d, dashed] \\
K \arrow[r, phantom, "\subseteq"] & L \arrow[r, phantom, "\subseteq"] & Q
\end{tikzcd}$$

commute.

Problem 23.6. Let L/K be a separable field extension. Let $\theta_1, \dots, \theta_N$ be a list of separable elements generating L over K, and let $\widehat{\theta}_1, \dots, \widehat{\theta}_{\widehat{N}}$ be another such list. Let $g_j(x)$ be the minimal polynomial of θ_j over K and let $\widehat{g}_j(x)$ be the minimal polynomial of $\widehat{\theta}_j$. Let M be the splitting field of $\prod g_j(x)$ and let $\widehat{M}$ be the splitting field of $\prod \widehat{g}_j(x)$. Show that $M \cong \widehat{M}$.

So Galois closures are unique up to isomorphism.

Finally, we address separability in characteristic p.

Definition Let k be a field of characteristic p. We define k to be ***perfect*** if every element of k has a p-th root. We also define all fields of characteristic zero to be perfect.

The next problem was on the problem sets, check that your whole group knows how to do it:

Problem 23.7. Show that finite fields are perfect.

Problem 23.8. Let k be a perfect field of characteristic p and let $f(x) \in k[x]$. Show that, if the derivative $f'(x)$ is 0, then $f(x) = g(x)^p$ for $g(x) \in k[x]$.

Problem 23.9. Let k be a perfect field and let $f(x) \in k[x]$ be an irreducible polynomial. Show that $f(x)$ is separable.

Problem 23.10. Show that, if K is perfect then every finite degree extension of K is separable.

The simplest example of a nonperfect field is $\mathbb{F}_p(t)$.

24. ARTIN'S LEMMA

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

Problem 24.1. 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 has a basis whose elements lie in 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 24.2. 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

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

Problem 24.3. Show that V is an L-vector subspace of L^n and that H takes V to itself.

Problem 24.4. Show that $\dim_L V > 0$.

Problem 24.5. Deduce a contradiction, and explain why you have proved $[L : F] = \#(H)$.

Problem 24.6. Show that $H = \mathrm{Aut}(L/F)$.

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

Problem 24.7. Let L, H and F be as in Artin's Lemma. Show that $[L : F]$ is Galois.

25. 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.

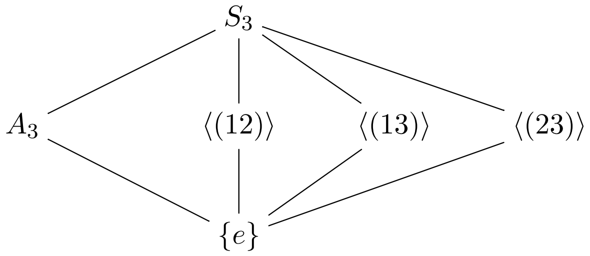
Problem 25.1. Let L/K be Galois and let F be a field with $K \subseteq F \subseteq L$. Show that L/F is Galois and identify $\operatorname{Gal}(L/F)$ with a subgroup of $\operatorname{Gal}(L/K)$.

Problem 25.2.
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 25.3.
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 25.3 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 25.4. 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 25.5. 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 25.6. Let L/K be a Galois extension. Let F be a field with $K \subseteq F \subseteq L$.

1. Show that L/F is Galois.
2. Show that $\operatorname{Aut}(L/F)$ is the subgroup $\operatorname{Stab}(F)$ of $\operatorname{Aut}(L/K)$.
3. Show that $\operatorname{Fix}(\operatorname{Stab}(F)) = F$. Hint: What can you say about $[L : \operatorname{Fix}(\operatorname{Stab}(F))]$?

Problem 25.7. Let L/K be a Galois extension with Galois group G. Let H be a subgroup of G and let $F = \operatorname{Fix}(H)$. Show that $\operatorname{Stab}(\operatorname{Fix}(H)) = H$.

Problem 25.8. Check the remaining claims of the Fundamental Theorem.

You have now proved:

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 $\mathrm{Stab}(F_1) \supseteq \mathrm{Stab}(F_2)$ and $[\mathrm{Stab}(F_1) : \mathrm{Stab}(F_2)] = [F_2 : F_1]$. If $H_1 \subseteq H_2$ then $\mathrm{Fix}(H_1) \supseteq \mathrm{Fix}(H_2)$ and $[\mathrm{Fix}(H_1) : \mathrm{Fix}(H_2)] = [H_2 : H_1]$.

We proceed to corollaries and related results.

Problem 26.1. Let L/K be a Galois extension with Galois group G. Let H be a subgroup of G with corresponding subfield F.

(1) For $\sigma \in G$, show that the subfield $\sigma(F)$ corresponds to the subgroup $\sigma H \sigma^{-1}$.
(2) Show that the following are equivalent:
  - The extension F/K is Galois.
  - For all $\theta \in F$ and all $\sigma \in G$, we have $\sigma(\theta) \in F$.
  - For all $\theta \in F$ and all $\sigma \in G$, we have $\theta \in \sigma(F)$.
  - The subgroup H of G is normal.
(3) Suppose that the above conditions hold. Show that $\mathrm{Gal}(F/K) \cong G/H$.

Problem 26.2. Let's do an old QR problem! Let $\zeta \in \mathbb{C}$ be a root of unity. Show that $2^{1/3} \not\in \mathbb{Q}(\zeta)$.

Problem 26.3. Let K be a field and let $L_1, L_2, \dots, L_r$ be finite Galois extensions of K.

(1) Show that there is a Galois extension M of K such that all of the L_j embed into M and the L_j generate M as a field. (Hint: Take the splitting field of an appropriate polynomial.)
(2) Show that $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of $\prod \mathrm{Gal}(L_j/K)$.

Problem 26.4. Let L/K be a Galois extension with Galois group G. Suppose that G is a 2-group.

(1) Show that there a chain of subfields $K = K_0 \subset K_1 \subset \cdots \subset K_N = L$ with $[K_{j+1} : K_j] = 2$.
(2) Suppose that the characteristic of K is not 2. Show that, in the preceeding chain, we can find elements $\phi_j \in K_j$ such that $K_{j+1} \cong K_j(\sqrt{\phi_j})$.
(3) (**Characterization of constructible numbers**) Let θ be algebraic over $\mathbb{Q}$ and let L be the Galois closure of $\mathbb{Q}(\theta)$. Show that θ is constructible[1] if and only if $[L : \mathbb{Q}]$ is a power of 2.
(4) (**Gauss's construction of the 17-gon**) Show that a primitive 17-th root of unity is constructible.

Problem 26.5. The following problem is on the homework, check that everyone can solve it: Let K be an infinite field, let V be a finite dimensional K-vector space and let $H_1, H_2, \dots, H_N$ be finitely many proper K-subspaces of V. Show that there is an element of V not in any H_j.

Problem 26.6. Let L/K be a Galois extension.

(1) Show that there are only finitely many fields F with $K \subseteq F \subseteq L$.
(2) Assume furthermore that K is infinite. For every F with $K \subseteq F \subseteq L$, show that there is an element $\theta \in F$ which is not in F' for any $K \subseteq F' \subsetneq F$.
(3) (**The primitive element theorem**) Let K be an infinite field and let L be a separable extension of finite degree. Then there is $\theta \in L$ such that $L = K(\theta)$.

Remark. Given a finite degree field extension L/K, an element θ of L such that $L = K(\theta)$ is called ***primitive***. We have just show that separable extensions of infinite fields have primitive elements. It is also true that, if L and K are finite, then L has a primitive element; the simplest proof I know is that the multiplicative group $L^{\times}$ will be cyclic and a generator for this group clearly must be primitive. The simplest example of an extension without a primitive element is $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p,y^p)$: Every element θ of $\mathbb{F}_p(x,y)$ has $\theta^p \in \mathbb{F}_p(x^p,y^p)$, so any such element only generates an extension of degree p inside this degree p^2 extension.

[1] To make this problem easier, I will allow you to take square roots of negative, and more generally of complex numbers, when discussing constructibility.

27. Solvable extensions

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

Problem 27.1. Let K be the splitting field of $x^n - 1$ over F. Show that $\mathrm{Gal}(K/F)$ is abelian.

Problem 27.2. 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 27.3. 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 27.4. Let F be a field and let K_1/F, K_2/F, …, 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 26.3.)

Problem 27.5. (**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 27.6. 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 $\sqrt[m]{}$.

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

On the previous worksheet 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 28.1 through 28.4: 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 whose Galois group is cyclic of order n and let g generate $\mathrm{Gal}(L/K)$.

Problem 28.1. 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 28.2. Let $J \subseteq \mathbb{Z}/n\mathbb{Z}$ be $\{j : L_j \neq (0)\}$.

(1) Show that J is a subgroup of $\mathbb{Z}/n\mathbb{Z}$.
(2) Show that $J = \mathbb{Z}/n\mathbb{Z}$. (Hint: All subgroups of $\mathbb{Z}/n\mathbb{Z}$ are of the form $d\mathbb{Z}/n\mathbb{Z}$ for some divisor d of n. Think about $g^{n/d}$.)
(3) Show that $\dim_K L_j = 1$

Problem 28.3. 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 28.4. Let $\alpha \in L_1$ and put $\theta = \alpha^n$. Show that $L = K(\theta^{1/n})$.

You have now proved:

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 28.5. Let L/K be a ~~solvable extension~~ Galois extension with solvable Galois group of order N. Suppose that $N \neq 0$ in K and that K contains a primitive N-th root of unity. Show that there is a chain of subfields $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$ such that $K_{j+1} = K_j(\theta_j^{1/d_j})$ for some $\theta_j \in K_j$ and some d_j dividing N.

We are now ready to prove

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

We have already shown that, if a radical formula for θ exists, then $\mathrm{Gal}(K/\mathbb{Q})$ is solvable. We now prove the converse:

Problem 28.6. Let K be a Galois extension of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q})$ solvable of order N.

(1) Show that there is a solvable extension L of $\mathbb{Q}$ that contains both K and a primitive N-th root of unity.
(2) Finish the proof of Galois's criterion.

29. Symmetric polynomials and computing Galois groups

This worksheet attempts to address two questions from past classes:

(1) "Is there an algorithm to compute Galois groups?" and
(2) What is the relationship between symmetries of polynomials and Galois symmetries?

It will be important to remain a careful distinction between formal polynomials, and those polynomials evaluated at specific algebraic numbers. I'll use capital letters for the former, and for the fields that contain them, and lower case letters for the latter.

Let $f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots \pm e_n$ be a separable polynomial in $\mathbb{Q}[x]$, let $r_1, \ldots, r_n$ be the roots of f in $\mathbb{C}$ and let $\ell = \mathbb{Q}(r_1, \ldots, r_n)$. So we identify $Gal(\ell/\mathbb{Q})$ with a subgroup of S_n.

Let $L = \mathbb{Q}(R_1, \ldots, R_n)$ and let K be the field of symmetric rational functions in L, so $K = \mathbb{Q}(E_1, \ldots, E_n)$ where the E_j are the elementary symmetric polynomials, so $\prod(x - R_j) = x^n - E_1 x^{n-1} + E_2 x^{n-2} - \cdots \pm E_n$.

Let $H \in \mathbb{Q}[R_1, \ldots, R_n]$. Let Γ be the subgroup $\{\gamma \in S_n : H(R_1, \ldots, R_n) = H(R_{\gamma(1)}, \ldots, R_{\gamma(n)})\}$. As an example, if $H = R_1^2 R_2 + R_2^2 R_3 + R_3^2 R_1$, then $\Gamma = \langle (123) \rangle$. Let h be the complex number $H(r_1, \ldots, r_n)$.

Problem 29.1. Suppose that $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \Gamma$. Show that $h \in \mathbb{Q}$.

Problem 29.2. Suppose that, for $\sigma \not\in \Gamma$, we have $H(r_1, \ldots, r_n) \neq H(r_{\sigma(1)}, \ldots, r_{\sigma(n)})$. Then show that $h \in \mathbb{Q}$ if and only if $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \Gamma$.

So, we can test whether $\mathrm{Gal}(\ell/\mathbb{Q})$ is contained in a particular subgroup of S_n by testing whether or not $H(r_1, \ldots, r_n) \in \mathbb{Q}$, subject to needing the extra hypothesis that, if $H(R_1, \ldots, R_n) \neq H(R_{\sigma(1)}, \ldots, R_{\sigma(n)})$ then $H(r_1, \ldots, r_n) \neq H(r_{\sigma(1)}, \ldots, r_{\sigma(n)})$.

The next problems discuss two approaches to teach whether $h \in \mathbb{Q}$. As our running example, we will look at the cubics $x^3 - 4x - 1$ and $x^3 + x^2 - 2x - 1$ and test whether their Galois groups are contained in the subgroup $\langle (123) \rangle$ of S_3. We'll look at the polynomial $H(R_1, R_2, R_3) = R_1^2 R_2 + R_2^2 R_3 + R_3^2 R_1$ which, indeed, has symmetry group $\langle (123) \rangle$.

First approach

Problem 29.3. Suppose that all the e_j (the coefficients of $f(x)$) are integers and let $H \in \mathbb{Z}[R_1, \ldots, R_n]$. Show that $h \in \mathbb{Q}$ if and only if $h \in \mathbb{Z}$.

This is useful, because it means that we can just compute $h(r_1, \ldots, r_n)$ to enough numerical accuracy to determine whether or not it is an integer.

Example: We have $x^3 - 4x - 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ and $x^3 + x^2 - 2x - 1 = (x - \beta_1)(x - \beta_2)(x - \beta_3)$ where $(\alpha_1, \alpha_2, \alpha_3) = (-1.8608, -0.2541, 2.1149)$ and $(\beta_1, \beta_2, \beta_3) = (-1.8019, -0.4450, 1.2470)$. We compute

$$\alpha_1^2 \alpha_2 + \alpha_2^2 \alpha_3 + \alpha_3^2 \alpha_1 = -9.066 \qquad \beta_1^2 \beta_2 + \beta_2^2 \beta_3 + \beta_3^2 \beta_1 = -4.000.$$

Thus, in the first case, the Galois group cannot be contained in $\langle (123) \rangle$ and, in the second, it is highly likely to be.

Second approach

$$G(x) = \prod_{\sigma \in \Gamma \backslash S_n} \Big(x - H(R_{\sigma(1)}, \ldots, R_{\sigma(n)}) \Big).$$

Here the product if over cosets of $\Gamma \backslash S_n$, choosing one element from each coset.

Problem 29.4. Explain why the product is well defined, independent of the choice of element from each coset.

Problem 29.5. Show that the coefficients of G lie in $\mathbb{Q}[E_1, \ldots, E_n]$ (this is just quoting a very old problem).

Let $g(x)$ be the polynomial in $\mathbb{Q}[x]$ that we get by evaluating the coefficients of G at $E_j = e_j$.

Problem 29.6. Show that h is a root of g. Conclude that, if $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \Gamma$, then g has a rational root.

Problem 29.7. Suppose g has a rational root of multiplicity 1. Show that there is some $\sigma \in S_n$ such that $\mathrm{Gal}(\ell/\mathbb{Q}) \subseteq \sigma \Gamma \sigma^{-1}$.

Our running example: We have

$$(x - R_1^2R_2 - R_2^2R_3 - R_3^2R_1)(x - R_2^2R_1 - R_3^2R_2 - R_1^2R_3) = x^2 - (E_1E_2 - 3E_3)x + (E_2^3 - 6E_1E_2E_3 + E_1^3E_3).$$

Evaluating $E_1E_2 - 3E_3$ and $E_2^3 - 6E_1E_2E_3 + E_1^3E_3$ at the coefficients of our two example cubics gives: $x^2 + 3x - 55$ and $x^2 - x - 12$ respectively. The first does not have a rational root and the second does, so the splitting field of the first cubic does not have Galois group contained in $\langle(123)\rangle$ and the second does. In approach, all computations are done with rational numbers, so there is no fear of round off error. However, the computations are much larger, and you have to deal with the complication of finding an S_n-conjugate of the correct group rather than the group itself.

Example – the alternating group: Homework problem 9.4 was an example of this approach: Let $\Delta = \prod_{i<j}(R_i - R_j)$ and let $\Phi = \Delta^2$, so Φ is a symmetric polynomial. The symmetry group of Δ is A_n, and the minimal polynomial of Δ is $x^2 - \Phi$, so we get that $\mathrm{Gal}(\ell/\mathbb{Q}) \subset A_n$ if and only if $\Phi(r_1, \ldots, r_n)$ is a square. The polynomial Φ is called the ***discriminant***.

Example – constructibility of roots of quartics: Let Γ be the subgroup $\langle(12), (34), (13)(24)\rangle$ of S_4; this is a 2-Sylow subgroup. We have

$$(y - R_1R_2 - R_3R_4)(y - R_1R_3 - R_2R_4)(y - R_1R_4 - R_2R_3) = y^3 - E_2y^2 + (E_1E_3 - E_4)y - (E_1^3 + E_1^2E_4 - 4E_2E_4).$$

Let ℓ be the splitting field of a quartic $x^4 - e_1x^3 + e_2x^2 - e_3x + e_4$. Then $\mathrm{Gal}(\ell/\mathbb{Q})$ is contained in a conjugate of Γ if and only if $\mathrm{Gal}(\ell/\mathbb{Q})$ is a 2-group (by the second Sylow theorem). And Γ is a 2-group if and only if the roots of $x^4 - e_1x^3 + e_2x^2 - e_3x + e_4$ are constructible. So we deduce that the roots of $x^4 - e_1x^3 + e_2x^2 - e_3x + e_4$ are constructible if and only if $y^3 - e_2y^2 + (e_1e_3 - e_4)y - (e_1^3 + e_1^2e_4 - 4e_2e_4)$ has a rational root.

30. Transcendence bases and transcendence degree

For most of this class, we have discussed field extensions of finite degree. We will now discuss a notion of "size" for extensions of infinite degree.

Let K/k be a field extension and let $\theta_1, \ldots, \theta_r \in K$.

Definition: We say that $\theta_1, \ldots, \theta_r$ are ***algebraically independent over*** k if, for all nonzero polynomials $f(t_1, \ldots, t_r) \in k[t_1, \ldots, t_r]$, we have $f(\theta_1, \ldots, \theta_r)$ nonzero.

Definition: The ***algebraic span of*** θ_1***, …*** θ_r ***in*** K ***over*** k is the set of those $\phi \in K$ which are algebraic over $k(\theta_1, \ldots, \theta_r)$. We say that $\theta_1, \ldots, \theta_r$ is an ***algebraic spanning set for*** K ***over*** k if every $\phi \in K$ is algebraic over $k(\theta_1, \ldots, \theta_r)$.

Definition: We say that $\theta_1, \ldots, \theta_r$ is a ***transcendence basis for*** K ***over*** k if $\theta_1, \ldots \theta_r$ is both algebraically independent and an algebraic spanning set.

The analogy with linear algebra should be clear. We start by showing the analogue of "finitely generated vector spaces have bases".

Problem 30.1. Suppose that $\theta_1, \ldots, \theta_r$ is an algebraic spanning set for K over k. Show that there is some subset of $\{\theta_1, \ldots, \theta_r\}$ which is a transcendence basis for K over k.

We now prove some useful lemmas:

Problem 30.2. Let $\theta_1, \ldots, \theta_r \in K$ and let $0 < q < r$. Show that $\theta_1, \ldots, \theta_r$ are an algebraic spanning set over k if and only if $\theta_{q+1}, \ldots, \theta_r$ are an algebraic spanning set over $k(\theta_1, \ldots, \theta_q)$.

Problem 30.3. Let $\theta_1, \ldots, \theta_r \in K$ and let $0 < q < r$. Show that $\theta_1, \ldots, \theta_r$ are algebraically independent over k if and only if the following two conditions hold:

- $\theta_1, \ldots, \theta_q$ are algebraically independent over k and
- $\theta_{q+1}, \ldots, \theta_{q+1}$ are algebraically independent over $k(\theta_1, \ldots, \theta_q)$.

We can now prove the analogue of "linearly independent sets can be extended to bases":

Problem 30.4. Let $\theta_1, \theta_2, \ldots, \theta_r$ be algebraically independent over k. Let $\phi_1, \ldots, \phi_s$ be an algebraic spanning set for K over k. Show that there is some subset S of $\{\phi_1, \ldots, \phi_s\}$ such that $\{\theta_1, \ldots, \theta_r\} \cup S$ is a transendence basis for K over k.

We now start in on proving that all transcendence bases have the same size.

Problem 30.5. Let $\alpha_1, \alpha_2, \ldots, \alpha_p$ be an algebraic spanning set for K over k. Let $\beta \in K$ be not algebraic over k. Show that there is some index j such that $\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_p$ is an algebraic spanning set for K over k.

Problem 30.6. Let $\alpha_1, \alpha_2, \ldots, \alpha_p$ be an algebraic spanning set for K over k and let $\beta_1, \ldots, \beta_q$ be algebraically independent over k. Show that $p \geq q$. Hint: Induct on the number of elements of $\{\beta_1, \ldots, \beta_q\}$ which are not in $\{\alpha_1, \ldots, \alpha_p\}$.

Problem 30.7. Show that any two finite transcendence bases of K over k have the same size. This size is called the ***transcendence degree*** of K over k.

Remark: This worksheet is deliberately written to avoid the Axiom of Choice. If you are comfortable with the Axiom of Choice, then we can define infinite transcendence bases in the obvious way and show that every field extension has a transcendence basis, and that any two transcendence bases have the same cardinality.

A. Abelian extensions

We understand groups by assembling them from simpler groups. In this worksheet, we will consider the case that we have a group G and an abelian group A, and we want to understand extensions

$$0 \to A \xrightarrow{\exp} E \xrightarrow{\pi} G \to 1.$$

I find it generally helpful to write A additively, so I'll call the map $A \to E$ by the name $\exp$. **Throughout this worksheet, A will denote an abelian group.**

Problem A.1. Suppose that we have a short exact sequence $0 \to A \to E \to G \to 1$. Show that the conjguation action of E on A factors through the quotient G.

Thus, classifying extensions $0 \to A \to E \to G \to 1$ breaks down to (1) classifying actions of G on A and (2) for each action of G on A, determining all ways to extend it to a group E. We'll write $\rho : G \to \mathrm{Aut}(A)$ for the action of G on A.

For any abelian group A and action ρ of another group G on A, we can always form the semidirect product $A \rtimes_\rho G$. But, in general, there are many other options:

Problem A.2. Show that all of the following groups can play the role of E in a short exact sequence

$$0 \to C_2 \to E \to C_2^2 \to 1.$$

(1) C_2^3.
(2) $C_4 \times C_2$.
(3) The subgroup $\{\pm 1, \pm i, \pm j, \pm k\}$ of the quaternions.
(4) The group of symmetries of a square.

Given a map $\pi : E \to G$, recall that a ***right inverse*** of π is a map $\sigma : G \to E$ obeying $\pi(\sigma(g)) = g$.

Problem A.3. Let $0 \to A \xrightarrow{\exp} E \xrightarrow{\pi} G \to 1$ be a short exact sequence and let $\sigma : G \to E$ be a set-theoretic right inverse to π. Show that every element of E can be uniquely written in the form $\exp(a)\sigma(g)$ for $a \in A$ and $g \in G$.

Problem A.4. Let $0 \to A \xrightarrow{\exp} E \xrightarrow{\pi} C_n \to 1$ be a short exact sequence. Show that E is abelian. (Hint: Choose your right inverse σ to make this computation easy.)

Let $0 \to A \xrightarrow{\exp} E \xrightarrow{\pi} C_n \to 1$ be a short exact sequence and let σ be a right inverse of π. For g_1 and $g_2 \in G$, define $\psi(g_1, g_2)$ by

$$\sigma(g_1)\sigma(g_2) = \exp(\psi(g_1, g_2))\sigma(g_1 g_2).$$

Problem A.5. Write a formula for the element a such that $\exp(a_1)\sigma(g_1)\exp(a_2)\sigma(g_2) = \exp(a)\sigma(g_1 g_2)$ in terms of a_1, a_2, g_1, g_2, ρ and ψ.

Problem A.6. Show that

$$\psi(g_1, g_2) - \psi(g_1, g_2 g_3) + \psi(g_1 g_2, g_3) - \rho(g_1)\left(\psi(g_2, g_3)\right) = 0. \qquad (*)$$

A function $\psi : G \to A$ obeying $(*)$ is called a ***2-cocycle***.

Problem A.7. Let ψ be a 2-cocycle. Show that your formula from Problem A.5 defines an associative multiplication on the set of ordered paris (a, g), with $a \in A$ and $g \in G$.

Thus, every extension can be described using 2-cocycles. However, this description is not unique.

A function $\psi : G^2 \to A$ is called a ***2-coboundary*** if there is a function $\alpha : G \to A$ such that

$$\psi(g_1, g_2) = \alpha(g_1) - \alpha(g_1 g_2) + \rho(g_1)\alpha(g_2) \qquad (\dagger)$$

Problem A.8. Show that every 2-coboundary is a 2-cocycle.

Problem A.9. Let $0 \to A \to E \xrightarrow{\pi} G \to 1$ be an extension and let $\sigma_1, \sigma_2 : G \to E$ be two right inverses of π. Let ψ_1 and ψ_2 be the corresponding 2-cocyles. Show that $\psi_1 - \psi_2$ is a 2-coboundary.

Problem A.10. Conversely, let ψ_1 and ψ_2 be two 2-cocycles which differ by a coboundary. Show that the corresponding extensions are isomorphic.

B. Derivations and transcendence degree

Definition: Let R be a commutative ring and let M be an R-module. A ***derivation*** is a map $D : R \to M$ satisfying $D(u+v) = D(u) + D(v)$ and $D(uv) = uD(v) + vD(u)$.

The following facts were checked on the homework:

Problem B.1. Let k be a field, M a $k[x]$-module, $d : k \to M$ a derivation and m an element of M. Show that there is a unique derivation $D : k[x] \to M$ which restricts to d on k and obeys $D(x) = m$.

Problem B.2. Let K/k be a separable field extension of finite degree, let M be a K-vector space and let $d : k \to M$ be a derivation. Show that there is a unique derivation $D : K \to M$ which restricts to d on K.

Please also check the following:

Problem B.3. Let M be a vector space over $k(x)$, and let $d : k[x] \to M$ be a derivation. Show that d has a unique extension to a derivation $D : k(x) \to M$. (Recall that $k[x]$ is the ring of polynomial with coefficients in k and that $k(x)$ is the field of fractions of $k[x]$.)

Definition: Let k be a field and K a larger field containing k. We define $\mathcal{D}_{K/k}$ to be the set of derivations $K \to K$ which obey $D(a) = 0$ for $a \in k$. This is a K-vector space, where scalar multiplication is defined by $(fD)(g) = f \cdot D(g)$ for f and $g \in K$.

From now on, let k be a field of characteristic zero. Since we are in characteristic zero, all algebraic field extensions are automatically separable.

Problem B.4. Show that $\mathcal{D}_{k(x_1,\dots,x_r)/k}$ is a $k(x_1, \dots, x_r)$-vector space of dimension r. (Recall that $k(x_1, \dots, x_r)$ is the fraction field of the polynomial ring $k[x_1, \dots, x_r]$.)

Problem B.5. Let K be a finitely generated field extension of k with transcendence degree r. Show that $\mathcal{D}_{K/k}$ is a K-vector space of dimension r.

Definition: Let k be a field and K a larger field containing k. We define $\Omega^1_{K/k}$ to be $\mathrm{Hom}_K(\mathcal{D}_{K/k}, K)$, in other words, the dual vector space to $\mathcal{D}_{K/k}$. For $u \in K$, we define the element du of $\Omega^1_{K/k}$ to be the map $D \to D(u)$ from $\mathcal{D}_{K/k}$ to K.

Problem B.6.

(1) Show that $dx_1, \dots, dx_r$ is a basis for $\Omega^1_{k(x_1,\dots,x_r)/k}$.

(2) For $f \in k(x_1, \dots, x_r)$, show that $df = \sum \frac{\partial f}{\partial x_j} dx_j$.

Problem B.7. Let $g_1, g_2, \dots, g_s \in k(x_1, \dots, x_r)$. Let $K \subseteq k(x_1, \dots, x_r)$ be the subfield generated by the g_j.

(1) Show that the transcendence degree of K of k is equal to the dimension of the subspace of $\Omega^1_{k(x_1,\dots,x_r)/k}$ spanned by the dg_j.

(2) Show that the g_j are algebraically independent over k if and only if the dg_j are linearly independent over $k(x_1, \dots, x_r)$.

(3) Show that the g_j algebraically span $k(x_1, \dots, x_r)$ if and only if the dg_j span $\Omega^1_{k(x_1,\dots,x_r)/k}$ as a $k(x_1, \dots, x_r)$-vector space.

This means that, in characteristic zero, we can study algebraic independence using techniques from ordinary linear algebra. For example, given two functions f and $g \in \mathbb{C}(x, y)$, these functions will be a transcendence basis if and only if $\det \begin{bmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} \\ \frac{\partial g}{\partial x} & \frac{\partial g}{\partial y} \end{bmatrix}$ is nonzero.

Contents