4 Foundations of Galois theory

4.1 Closure correspondences

In this subsection, we fix two disjoint sets A, B and a subset $R \subset A \times B$, often known as a **binary relation.** For all $X \subset A$ and $Y \subset B$ we define

$$\begin{aligned} X^\dagger &:= \{b \in B \mid (a,b) \in R \quad \text{for all } a \in X\}, \\ Y^* &:= \{a \in A \mid (a,b) \in R \quad \text{for all } b \in Y\}. \end{aligned} \tag{66}$$

Let $P(A)$ be the *power set*, that is, the set of subsets of A. We have thus two maps $\dagger\colon P(A) \to P(B)$ and $*\colon P(B) \to P(A)$.

Remark 67. A better but somewhat pedantic approach is to replace $P(A)$ by $P(A) \times \{1\}$ and $P(B)$ by $P(B) \times \{2\}$. Here 1 and 2 are labels indicating whether we're thinking of a subset of A or one of B. The empty set is a subset of both A and B, but that's the only ambiguity not ruled out by our assumption that A and B are disjoint.

Proposition 68.

(a) For all $X \subset A$, we have $X \subset X^{\dagger *}$.

(b) For all $Y \subset B$, we have $Y \subset Y^{*\dagger}$.

(c) For all $X_1 \subset X_2 \subset A$, we have $X_1^\dagger \supset X_2^\dagger$.

(d) For all $Y_1 \subset Y_2 \subset B$, we have $Y_1^* \supset Y_2^*$.

(e) For all $X \subset A$, we have $X^\dagger = X^{\dagger *\dagger}$, or briefly, $\dagger * \dagger = \dagger$.

(f) For all $Y \subset B$, we have $Y^* = Y^{*\dagger *}$, or briefly, $* \dagger * = *$.

Proof. These are almost trivial as we shall see. We write out the proofs in detail.

Proof of (a). Let $a \in X$ and $b \in X^\dagger$. Then $(a,b) \in R$ by definition of $\dagger$. As this is true for all such b, it implies that $a \in X^{\dagger *}$ by definition of $*$.

Proof of (c). Let $b \in X_2^\dagger$. Then $(a,b) \in R$ for all $a \in X_2$, by definition of $\dagger$. So $(a,b) \in R$ for all $a \in X_1$ (because $X_1 \subset X_2$). This means that $b \in X_1^\dagger$ as required.

Proof of (e). By (a) we have $X \subset X^{\dagger *}$. Applying (c) with $X_1 = X$ and $X_2 = X^{\dagger *}$ gives $X^\dagger \supset X^{\dagger *\dagger}$. In order to prove the reverse inclusion, let $b \in X^\dagger$. By definition of $*$ then, $(a,b) \in R$ for all $a \in X^{\dagger *}$. In other words, $b \in X^{\dagger *\dagger}$.

The remaining three parts follow by interchanging $(A, \dagger)$ and $(B, *)$. □

The $(A,\dagger)$–$(B,*)$ symmetry mentioned in the above proof is often useful.

We call a subset $X \subset A$ **closed** if and only if it is of the form Y^*. This is equivalent to saying that $X = X^{\dagger *}$, by proposition 68f. Closed subsets of B are defined likewise.

Proposition 69. There is a bijection from the set of closed subsets of A to the set of closed subsets of B, given by $X \mapsto X^\dagger$, and whose inverse is $Y \mapsto Y^*$.

Proof. Almost immediate from proposition 68. □

Of course, $X^\dagger$ is defined for *all* subsets X of A. But the formula $X \mapsto X^\dagger$ in proposition 69 assumes that X is closed.

Let us call the bijection given by proposition 69 the **closure correspondence**. Each time we have two sets A, B and a subset $R \subset A \times B$, there is a closure correspondence.

There are lots of closure correspondences in mathematics, and we touch upon some of them in exercises 4.2–4.4. But the most famous of all is a particular closure correspondence called the Galois correspondence which is at the centre of Galois theory.

Exercises

(4.1) Use the notation of this subsection.

(a) Prove that A is closed. Is $\varnothing \subset A$ necessarily closed?

(b) Prove that if $X_1, X_2 \subset A$ are closed, then so is $X_1 \cap X_2$. What about any number of X_i?

(c) Give an example where $X_1, X_2 \subset A$ are closed but $X_1 \cup X_2$ is not.

— ∼ —

To get a feel for closure correspondences in general, we look at a few examples not used later on in the lectures.

(4.2) [Standard representation of GL(n)]. Let K be a field of at least 3 elements. Let $V = K^n$, $G = \mathrm{GL}(n, K)$ and consider the binary relation $R = \{(v, g) \in V \times G \mid g(v) = v\}$. Prove that the closed subsets of V are precisely the vector subspaces of V. If K has 2 elements, describe the closed subsets of V in similar terms.

(4.3) [Downsets]. Let $(P, \leq)$ be an ordered set. (Some people say *partially ordered set* when we say *ordered set*). Let $A = B = P$ and let $R \subset A \times B$ be the binary relation given by $R = \{(a, b) \in A \times B \mid a < b\}$. Prove that a subset $X \subset A$ is closed if and only if for all $x, y \in A$, if $y \in X$ and $x \leq y$ then $x \in X$. Also, if $X \subset A$ is closed, then $X^\dagger$ equals the complement $P \setminus X$.

(4.4) [Affine varieties]. Let $A = \mathbb{C}^n$ and let $B = \mathbb{C}[X_1, \ldots, X_n]$ be the ring of polynomials in n variables. If $a = (a_1, \ldots, a_n) \in A$ and $f \in B$, we can evaluate f at a to obtain a complex number $f(a) = f(a_1, \ldots, a_n)$. Consider the binary relation $R = \{(a, f) \in A \times B \mid f(a) = 0\}$. Prove that if a subset $I \subset B$ is closed, then it is a radical ideal (an ideal J in a ring S is said to be radical if for all $f \in S$ and all $n > 0$, if $f^n \in J$ then $f \in J$).

The converse is also true and known as Hilbert's Nullstellensatz: see the book *Undergraduate algebraic geometry* by Miles Reid for a one-page proof.

4.2 The Galois correspondence

Definition 70. Let $K \subset M$ be fields. The **Galois group** $\mathrm{Gal}(M/K)$ is the group of field automorphisms of M which fix every element of K.

It is not hard to show that $\mathrm{Gal}(M/K)$ is a group under composition.

Example 71. Here are some examples of Galois groups $\mathrm{Gal}(M/K)$.

(a). If $K = M$ then the Galois group is trivial.

(b). Suppose $K = \mathbb{R}$, $M = \mathbb{C}$. Then the Galois group has order 2, and consists of the trivial element and complex conjugation.

(c). Suppose $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. Again the Galois group has order 2 as we proved in example 51.

(d). Suppose $K = \mathbb{Q}$ and $M = \mathbb{Q}(\alpha)$ where $\alpha = 2^{1/3}$ is the real cube root of 2. We claim that $\mathrm{Gal}(M/K)$ is trivial. Let $s \in \mathrm{Gal}(M/K)$. Then $s(\alpha)$ is a cube root of 2 and is in $\mathbb{R}$ becaus $M \subset \mathbb{R}$. But α is the only cube root of 2 in $\mathbb{R}$ so $s(\alpha) = \alpha$. It follows that $s = 1$ because M is generated by α.

(e). Let $n \geq 1$. Then the Galois group $\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(X^n))$ is cyclic of order n and generated by s: $X \mapsto \exp(2\pi i/n)\, X$.

(f). Let K be a field. It can be shown that $\mathrm{Gal}(K(X)/K)$ consists of those K-automorphisms of $K(X)$ taking X to a rational function of the form

$$\frac{aX + b}{cX + d}$$

with $a, b, c, d \in K$, $ad - bc \neq 0$. This group is usually denoted $\mathrm{PGL}(2, K)$.

For the rest of this section, we fix a field extension N/K and write $G = \mathrm{Gal}(N/K)$. We now introduce some notation that we use nearly always when considering a field extension.

We define a binary relation $R \subset G \times N$ by

$$R = \{(g, x) \in G \times N \mid g(x) = x\}.$$

Let $\dagger$: $P(G) \to P(N)$ and $*$: $P(N) \to P(G)$ be the maps as in (66). Explicitly: for $H \subset G$ and $L \subset N$ we define

$$H^\dagger := \{x \in N \mid g(x) = x \quad \text{for all } g \in H\},$$
$$L^* := \{g \in G \mid g(x) = x \quad \text{for all } x \in L\}.$$

Definition 72. As in section 4.1, we can talk about closed subsets of G and closed subsets of N. Let $\mathcal{F}$ denote the set of closed subsets of N and $\mathcal{G}$ the set of closed subsets of G.

As a particular case of proposition 69 we get:

Proposition 73. There exists a bijection $\mathcal{F} \to \mathcal{G}$ given by $H \mapsto H^\dagger$ and whose inverse is $L \mapsto L^*$. □

Of course, proposition 73 is virtually worthless unless we can determine which subsets of G or N are closed. Two easy restrictions are as follows:

Exercise (4.5) Prove that every element of $\mathcal{G}$ is a subgroup of G. Prove that every element of $\mathcal{F}$ is a subfield of N containing K.

Because of exercise 4.5, an element of $\mathcal{G}$ (that is, a closed subset of G) is called a **closed subgroup** of G. Also, an element of $\mathcal{F}$ is called a **closed intermediate field.** In general, if $P \subset Q \subset R$ are fields then we say that Q is an **intermediate field** of the extension $P \subset R$.

4.3 The closed fields and subgroups

Proposition 74. Let $K \subset L \subset M \subset N$ be fields. If $[M : L] = n < \infty$ then $[L^* : M^*] \leq n$.

Proof. Induction on n, the case $n = 1$ being trivial. If there exists a field L_0 properly between L and M, then the induction hypothesis tells us that $[L^* : L_0^*] \leq [L_0 : L]$ and $[L_0^* : M^*] \leq [M : L_0]$. Therefore

$$[L^* : M^*] = [L^* : L_0^*][L_0^* : M^*] \leq [L_0 : L][M : L_0] = [M : L].$$

So suppose now that there are no fields between L and M. Then M is of the form $L(\alpha)$ for some $\alpha \in M$. Let $f \in L[X]$ be the minimum polynomial for α over L. By proposition 56 we have $\deg(f) = [M : L] = n$. Consider the set Y of roots of f in M. Then $\#Y \leq n$. We define a map E: $L^*/M^* \to N$ (evaluation at α) by

$$E(gM^*) := g(\alpha).$$

We need to show that this is well-defined, that is, if $gM^* = hM^*$ then $g(\alpha) = h(\alpha)$. Indeed, if $g = hk$ with $k \in M^*$, then $E(g) = E(hk) = hk(\alpha) = h(k(\alpha)) = h(\alpha) = E(h)$ and we have shown that E is well-defined.

For all $g \in L^*$ we have

$$\begin{aligned} 0 &= g(0) && \text{because } g \text{ is a field automorphism} \\ &= g(f(\alpha)) && \text{because } f(\alpha) = 0 \\ &= f(g(\alpha)) && \text{because } g \in L^* \text{ and } f \in L[X] \end{aligned}$$

which proves that E takes values only in Y. If we can prove that E: $L^*/M^* \to Y$ is *injective* , then it follows that $[L^* : M^*] = \#(L^*/M^*) \leq \#Y \leq n$ and we will be done.

In order to prove that E is injective, assume that $E(gM^*) = E(hM^*)$, that is, $g(\alpha) = h(\alpha)$. Then $g^{-1}h(\alpha) = \alpha$. Now $g^{-1}h$ preserves L pointwise (as both g and h do) and it preserves α, so it preserves $L(\alpha) = M$ pointwise. So $g^{-1}h \in M^*$, that is, $gM^* = hM^*$. This proves that E is injective and the proof is finished. □

Proposition 75. Let $G = \mathrm{Gal}(N/K)$ and let $J \subset H \subset G$ be subgroups such that $[H : J] = n < \infty$. Then $[J^\dagger : H^\dagger] \leq n$.

Proof. Let $g \in H$ and $x \in J^\dagger$. Then $g(x)$ depends only on the coset $C := gJ$ (and x) and we shall write $C(x) := g(x)$ in the proof that follows.

Let $u_0, \ldots, u_n \in J^\dagger$. We need to prove that $u_0, \ldots, u_n$ are $H^\dagger$-dependent, that is, we need to find $a_0, \ldots, a_n \in H^\dagger$, not all zero, such that $\sum_i a_i u_i = 0$.

Write $H/J = \{C_1, \ldots, C_n\}$. Consider the equations

$$\sum_{i=0}^{n} a_i \cdot C_j(u_i) = 0 \qquad \text{for all } j \in \{1, \ldots, n\}. \tag{76}$$

These are n linear equations (with coefficients in $J^\dagger$) in $n+1$ unknowns a_i which for the moment are allowed to be in $J^\dagger$. By linear algebra, there is a nonzero solution $(a_i)_i$ to (76). Pick a nonzero solution with $\#\{i \mid a_i = 0\}$ maximal. After rescaling and renumbering we may suppose that $a_0 = 1$. The proof will be finished by proving that $a_i \in H^\dagger$ for all i. To this end, let $g \in H$. We need to show that $g(a_i) = a_i$ for all i.

Applying g to (76) gives

$$\sum_{i=0}^{n} g(a_i) \cdot g(C_j(u_i)) = 0 \qquad \text{for all } j \in \{1, \ldots, n\}.$$

Now $\{gC_1, \ldots, gC_n\} = \{C_1, \ldots, C_n\}$; only the order may be different. So

$$\sum_{i=0}^{n} g(a_i) \cdot C_j(u_i) = 0 \qquad \text{for all } j \in \{1, \ldots, n\}.$$

This means that $(g(a_i))_i$ is another solution to (76). Put $b_i := g(a_i) - a_i$. Then $(b_i)_i$ is a solution to (76) with more zero entries than $(a_i)_i$ because $b_0 = g(a_0) - a_0 = g(1) - 1 = 1 - 1 = 0$ (and $b_i = 0$ whenever $a_i = 0$). But we took $\{i \mid a_i = 0\}$ to be maximal, so $b_i = 0$ for all i. So $g(a_i) = a_i$ for all i and the proof is finished. □

4.4 The main theorem of Galois theory

For a group G acting on a field M we write

$$M^G := \{x \in M \mid g(x) = x \text{ for all } g \in G\}.$$

The automorphism group of a field M is written $\mathrm{Aut}(M)$.

Definition 77. The field extension M/K is said to be a **Galois extension** if there exists a subgroup $G \subset \mathrm{Aut}(M)$ such that $K = M^G$. We also say that M is Galois over K in this case.

Let us repeat this important definition in different words. The extension M/K is Galois if and only if, for all $x \in M$ not in K, there exists $g \in \mathrm{Gal}(M/K)$ such that $g(x) \neq x$. Also, M/K is Galois if and only if K is a closed intermediate field of the extension M/K.

Theorem 78. Let M/K be a finite Galois extension and let G, $\mathcal{F}$, $\mathcal{G}$, $\dagger$, $*$ be as usual, as explained in section 4.2.

(a) The set of subgroups of G is precisely $\mathcal{G}$. The set of intermediate fields of M/K is precisely $\mathcal{F}$.

(b) (Main theorem of Galois theory). There exists a bijection from the set of subgroups of G to the set of intermediate fields of M/K given by $H \mapsto H^\dagger$ and whose inverse is $L \mapsto L^*$.

(c) Let $H \subset J \subset G$ be subgroups. Then $[J : H] = [H^\dagger : J^\dagger]$.

Proof. Proof of (a). Recall that every element of $\mathcal{F}$ is an intermediate field of M/K by exercise 4.5. In order to prove the converse, let L be a subfield of M containing K. Note that $K = K^{*\dagger}$ because M/K is Galois. Therefore

$$\begin{aligned} [L^{*\dagger} : K] &= [L^{*\dagger} : K^{*\dagger}] \\ &\leq [L : K^*] \qquad \text{by proposition 75} \\ &\leq [L : K] \qquad \text{by proposition 74.} \end{aligned}$$

Also, $L \subset L^{*\dagger}$ by proposition 68b and $[L : K] < \infty$. Therefore $L = L^{*\dagger}$ and $L \in \mathcal{F}$. The proof that every subgroup of G is closed is similar. This finishes the proof of (a). Part (b) follows immediately from part (a) and proposition 73. Part (c) is an exercise. □

Remark 79. Theorem 78 can be extended to infinite field extensions but this is not on our syllabus. It turns out that again all intermediate fields are closed, but the subgroups of G are not necessarily closed. Instead, G becomes a topological group and a subgroup of G is closed in our sense if and only if it is closed in the topological sense.

There are three ways to obtain examples of field extensions M/K:

(a) Let M be a known field and let G be a subgroup of $\mathrm{Aut}(M)$. Then put $K = M^G$.

(b) Let N be a known field, for example $\mathbb{C}$. Define $M, K \subset N$ by specifying generators.

(c) Let K be a known field. Let M be obtained by adjoining a root of a specified irreducible polynomial in $K[X]$ as can be done in an essentially unique way by proposition 60. Make a tower of fields if necessary by repeating the process.

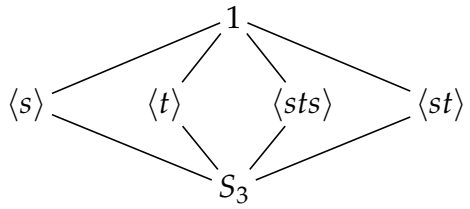
The techniques provided by this chapter suffice to deal with examples as in (a). Examples of (b) and (c) (which are essentially equivalent to each other) are best dealt with after the next two chapters though we shall already work out one such example in the next subsection.

4.5 Examples

Example 80: Subgroups of S_3. If you deal with a Galois extension whose Galois group isomorphic to S_3, the symmetric group on 3 objects, it may be useful to know its subgroups and some more properties which we collect here without proof.

Let G be a group generated by s, t and suppose that s, t have order 2 and st has order 3. Then G is isomorphic to S_3. An isomorphism is given by

ϕ: $G \to S_3$, $\phi(s) = (12)$, $\phi(t) = (23)$. Here are all subgroups of S_3.



Example 81. Let $K = \mathbb{C}(X)$ be the field of rational functions in z over $\mathbb{C}$. Let $\omega = \exp(2\pi i/3)$. Define $s, t \in \mathrm{Gal}(K/\mathbb{C})$ by

$$s(X) = X^{-1}, \qquad t(X) = \omega\, X^{-1}.$$

Put $G := \langle s, t\rangle$, the group generated by s and t. By theorem 78b, there exists a bijection between the subgroups of G and the fields between K and K^G: the intermediate field corresponding to a subgroup H of G is K^H.

(a) Prove $K^{\langle s\rangle} = \mathbb{C}(X + X^{-1})$.

(b) Prove $G \cong S_3$.

(c) List the subgroups of G and the corresponding fields between K, K^G.

Warning. The symbols s, t are not functions of one variable. If they were then one would have, for example,

$$s(1 + X) = (1 + X)^{-1} \qquad (???)$$

which is wrong. Correct is

$$s(1 + X) = s(1) + s(X) = 1 + X^{-1}$$

because s is a field automorphism.

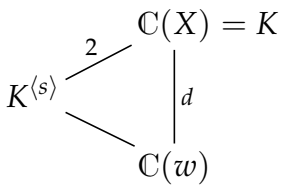
Solution. (a). Write $u = X + X^{-1}$. We have $\mathbb{C}(u) \subset K^{\langle s\rangle}$ because

$$s(u) = s(X + X^{-1}) = s(X) + s(X^{-1}) = X^{-1} + X = u.$$

By theorem 78c we have $[K : K^{\langle s\rangle}] = \#\langle s\rangle = 2$. On writing $d = [K : \mathbb{C}(u)]$ we have $d \leq 2$ because X is a root of the degree 2 polynomial

$$Y^2 - uY + 1$$

in $\mathbb{C}(u)[Y]$. By the tower law we must have $d = 2$ and $K^{\langle s\rangle} = \mathbb{C}(u)$.



(b). We have $st(X) = s(\omega X^{-1}) = \omega X$ so st has order 3. Now G is generated by s, t and the orders of s, t, st are $2, 2, 3$, so $G \cong S_3$.

(c). The subgroups of G were listed in example 80. Each subgroup $H \subset G$ corresponds to an intermediate field K^H by theorem 78. We claim that each intermediate fields is generated over $\mathbb{C}$ by a single function f as follows.

subgroup	1	$\langle s \rangle$	$\langle t \rangle$	$\langle sts \rangle$	$\langle st \rangle$	G
f	X	$X + X^{-1}$	$X + \omega X^{-1}$	$X + \omega^2 X^{-1}$	X^3	$X^3 + X^{-3}$

Let us explain how one finds K^H by the example of $H = G$. We immediately see that $\mathbb{C} \subset K^G$. But K^G is bigger than $\mathbb{C}$ and we need to find more elements in K^G.

Step 1. *Choose any element α of K.* Let us choose $\alpha = X$.

Step 2. *Compute the orbit $A = \{h(\alpha) \mid h \in H\}$.* In our case, this is

$$\{X, \quad \omega X, \quad \omega^2 X, \quad X^{-1}, \quad \omega X^{-1}, \quad \omega^2 X^{-1}\}.$$

Step 3. *Choose a symmetric function f in $\#A$ variables and substitute the elements of the orbit A for those variables. The result is an element of K^H.* In our example, let us choose $f = U_1 + \cdots + U_6$, the sum of six variables. Plugging the elements of A in gives $f(A) = 0$.

Step 4. *Find out if K^H is generated by the element(s) we found.* Well, K^G is not generated by $\mathbb{C} \cup \{0\}$.

In unsuccesful cases like this we go back to step 3 and repeat. Let us next take f to be the sum of the squares. The sum of the squares of the elements of A is again 0. Still no luck! But the sum of the cubes is $3(X^3 + X^3)$. Therefore we have $\mathbb{C}(X^3 + X^{-3}) \subset K^G$. In fact, these fields are equal. In part (a) we saw an example how to prove that two fields like this are equal. □

Example 82. Here is a baby example of things discussed at length in chapter 6. Let L/K be an extension of degree 2 and suppose that K has characteristic $\neq 2$. Prove that L/K is Galois and that its Galois group is of order 2.

Solution. Let α be an element of L but not of K. Then $L = K(\alpha)$ (by the tower law for example). Let $f \in K[X]$ be the minimum polynomial of α over K. Then $\deg f = 2$ by proposition 56. Since $X - \alpha$ divides f in $L[X]$ there exists $\beta \in L$ such that $f = (X - \alpha)(X - \beta)$. Therefore the minimum polynomial of β is also f. By uniqueness of field extensions (proposition 60b) there exists $h \in \mathrm{Gal}(L/K)$ such that $h(\alpha) = \beta$. We have $\alpha \neq \beta$ because otherwise $K[X] \ni f = (X - \alpha)^2 = X^2 - 2\alpha + \alpha^2$ so $\alpha \in K$ because 2 is invertible in K, a contradiction. It follows that L/K is Galois. The Galois group is of order 2 by theorem 78c. □

4.6 Exercises

(4.6) In this exercise you will fill some gaps in example 81.

(1) Prove that $K^{\langle st \rangle} = \mathbb{C}(X^3)$.

(2) Prove that $K^G = \mathbb{C}(v)$ where $v = X^3 + X^{-3}$.

(3) Compute the minimum polynomial of $u = X + X^{-1}$ over $\mathbb{C}(v)$.

(4.7) Let K be a field and $M = K(Z)$ the field of rational functions in a variable Z. Let $G \subset \mathrm{Gal}(M/K)$ be the subgroup generated by

$$s\colon Z \mapsto 1 - Z \qquad \text{and} \qquad t\colon Z \mapsto Z^{-1}$$

and $L = M^G$.

(a) Prove that the orders of (respectively) s, t, st are (respectively) $2, 2, 3$. [It follows that there is an isomorphism $G \to S_3$, $s \mapsto (12)$, $t \mapsto (23)$, don't prove this.]

(b) Write

$$y = \frac{Z^3 - 3Z + 1}{Z(Z-1)}.$$

Prove $M^{\langle st \rangle} = K(y)$.

(c) Prove $y + s(y) = 3$.

(d) Deduce from (c) that $L = K(w)$ where $w = y\,s(y)$. [This can be done without many calculations.]

(e) List all subgroups of G (by group generators) and the corresponding intermediate fields (by field generators). Proofs are not necessary.

(f) Let $P \subset Q$ be fields. Let $a \in P$ and write

$$f = (X^3 - 3X + 1) - a\,X(X-1) \in P[X].$$

Suppose that f has a root $u \in Q$. Prove that there are $v, w \in Q$ such that $f = (X-u)(X-v)(X-w)$. Prove also that if $\mathrm{char}\, P \neq 3$ then Q/P is Galois.

(4.8) Finish the proof of theorem 78a, that is, prove that every subgroup of G is closed.

(4.9) Prove theorem 78c, that is, $[J : H] = [H^\dagger : J^\dagger]$.

(4.10) Let M/K be an extension of degree $d < \infty$. Suppose that $\mathrm{Gal}(M/K)$ has t elements. Prove that $t \leq d$. Prove that $t = d$ if and only if M/K is Galois.

(4.11) Let $n \geq 1$. Prove that the extension $\mathbb{C}(X)/\mathbb{C}(X^n)$ is Galois. Prove that $\mathbb{Q}(X)/\mathbb{Q}(X^3)$ is not.

(4.12) In this exercise you prove that every finite group is (isomorphic to) a Galois group. Let G be a finite group.

(a) Suppose that G acts faithfully on a field M (recall that faithful means that if $g \in G$ is such that $g(x) = x$ for all $x \in M$ then $g = 1$). Let $K = M^G := \{x \in M \mid g(x) = x \text{ for all } g \in G\}$. Prove that M/K is Galois and that $\mathrm{Gal}(M/K) \cong G$.

(b) Prove that there exists a field M and a faithful G-action on it. Hint: Let G act on $\mathbb{Q}(X_1, \ldots, X_n)$ for appropriate n by permuting the variables.

(4.13) Let $K \subset N$ be fields and write $G = \mathrm{Gal}(N/K)$.

(a) Suppose that $K \subset L \subset M \subset N$ are fields. Suppose that L is closed and that $[M : L] = n < \infty$. Then M is also closed, and $[L^* : M^*] = n$

(b) Let $H \subset J \subset G$ be subgroups. Suppose that H is closed and that $[J : H] = n < \infty$. Then J is also closed, and $[H^\dagger : J^\dagger] = n$.

(4.14) Let $K \subset M$ be fields and write $G = \mathrm{Gal}(M/K)$.

(a) Prove that all finite subgroups of G are closed.

(b) Suppose that M/K is Galois and let L be an intermediate field of M/K with $[L : K]$ finite. Prove that M/L is Galois.

(4.15) Let K be an infinite field, $M = K(X)$, $G = \mathrm{Gal}(M/K)$.

(a) Prove that M is Galois over K.

(b) Prove that the only closed subgroups of G are the finite subgroups and G itself.

(4.16) Consider the field extension $\mathbb{Q}(X)/\mathbb{Q}$. Prove that the intermediate field $\mathbb{Q}(X^2)$ is closed but $\mathbb{Q}(X^3)$ is not.

(4.17) Let $K \subset L \subset M$ be fields with L/K and M/L Galois. Assume that any automorphism of L/K can be extended to M. Prove that M/K is Galois.

(4.18) Let M/K be a finite extension and let G, $\mathcal{F}$, $\mathcal{G}$, $\dagger$, $*$ be as usual. Prove that all subgroups of G are closed. Describe all closed intermediate fields.

(4.19) Let K be a field and $n \geq 1$. Let $\mathrm{GL}(n, K)$ be the group of invertible $n \times n$ matrices or equivalently, the group of invertible K-linear maps from K^n to itself.

(a) Prove that there exists a $\mathrm{GL}(2, K)$-action on the field $K(X)$ by K-automorphisms, defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(X) = \frac{aX + b}{cX + d}.$$

(b) Prove that an element of $\mathrm{GL}(2, K)$ acts trivially on $K(X)$ if and only if it is scalar. Notation: we let H denote the group of scalar elements and put

$$\mathrm{PGL}(2, K) := \mathrm{GL}(2, K)/H.$$

We have shown that $\mathrm{PGL}(2, K)$ is a subgroup of $\mathrm{Gal}(K(X), K)$.

(c) Prove that $\mathrm{PGL}(2, K) = \mathrm{Gal}(K(X)/K)$. Notation: as usual, $\mathrm{PGL}(2, K)$ acts on the set of 1-dimensional linear subspaces of K^2. Instead of the subspaces

$$K\tbinom{a}{1}, \text{ respectively, } K\tbinom{1}{0}$$

where $a \in K$ we simply write a, respectively, ∞. Thus we obtain a $\mathrm{Gal}(K(X)/K)$-action on $K \cup \{\infty\}$. Roughly, it is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(t) = \frac{at + b}{ct + d}$$

for all $t \in K \cup \{\infty\}$.

(4.20) Let K be a field. The **degree** of a rational function $r \in K(X)$ is defined to be $\max(\deg p, \deg q)$ where $p, q \in K[X]$ are any coprime polynomials such that $p/q = r$.

(a) Prove that if $r \in K(X)$ is not in K then $[K(X) : K(r)]$ is the degree of r in the above sense.

(b) Deduce that if $r, s \in K(X)$ then $\deg(r \circ s) = \deg(r)\deg(s)$ where $\circ$ denotes composition (s substituted for X in r).

(4.21) Let K be a field of characteristic $\neq 3$ and write $L = K(X)$. Let $\alpha \in K$ be a primitive cube root of unity. Define $s, t \in \mathrm{Gal}(K(X)/K)$ by

$$s(X) = \alpha X, \qquad t(X) = \frac{-X+1}{2X+1}$$

and write $G = \langle s, t \rangle$. (You may wish to skip parts (a) and (b) and instead simply assume that G has 12 elements).

(a) Prove: G preserves $\{0, 1, \alpha, \alpha^2\}$ where we use the $\mathrm{Gal}(K(X)/K)$-action on $K \cup \{\infty\}$ constructed in exercise 4.19.

(b) Prove that G is isomorphic to the alternating group A_4.

(c) Find $p, q \in K[X]$ of degree at most 12 such that $r := p/q$ is in L^G but not in K. Hint: why does the G-orbit of X^3 have at most 4 elements?

(d) Deduce that $L = K(r)$.

(4.22) Let K be a finite field of q elements. Recall that $G := \mathrm{Gal}(K(X)/K)$ consists of the elements taking X to

$$\frac{aX+b}{cX+d}$$

for some $a, b, c, d \in K$ with $ad - bc \neq 0$. Define $s \in G$ by $s(X) = X + 1$ and $H \subset G$ by

$$H = \left\{ X \mapsto aX + b \;\middle|\; a, b \in K,\ a \neq 0 \right\}.$$

(a) Prove $K(X)^{\langle s \rangle} = K(f)$ where $f = X^q - X$. Hint: either use that the characteristic of K is a prime number dividing q, or that $X^q - X = \prod_{a \in K}(X - a)$.

(b) Prove $K(X)^H = K(f^{q-1})$.

(c) Find g such that $K(X)^G = K(g)$.