Exercises supplementing those in Ian Stewart's *Galois Theory*, 3rd Edition

This is a collection of additional exercises that I put on homework sheets when I taught undergraduate Galois theory from this text in Spring 2005, supplementing those in the book. Some I included in assignments the students were to hand in; others I indicated were for ''students interested in further interesting and/or more challenging problems'' to think about.

I have given the exercises numbers indicating the relevant chapter of Stewart, and continuing the numeration where Stewart's exercises in each chapter leave off, except, occasionally, when I have numbered one of my exercises as a variant or an ''additional part'' of one of Stewart's. In all cases, the numbers I give my exercises are shown in quotation marks, to distinguish them from exercises actually in the text.

A number of these problems are adapted from a similar packet that I put together when I taught from the second edition of this text 4 years ago, renumbered to fit the current numbering of Stewart's chapters, and often improved in one or another way.

Many of my exercises have several parts. Often one may only want to assign or work some parts of an exercise.

Though I approve of Stewart's practice of marking with an asterisk more difficult exercises, I have not done so in this draft of this packet. The main reason is shortness of time, compounded by the fact that the difficulty of some exercises depends on whether the student has seen a discussion I gave in class, so that I would have had to go back and ponder the difficulty of each exercise without that background.

George M. Bergman
gbergman@math.berkeley.edu
14 June, 2005

This exercise-packet is accessible online at
`/~gbergman/ug.hndts/IStwrt_GalTh3_exs.ps`
See also the packet of errata to this edition of Stewart at
`/~gbergman/ug.hndts/IStwrt_GalTh3_err.ps`

– = ≡ ≡ = –

Chapter 1

''**Exercise 1.14**''. This exercise shows why I corrected the second display on p.13 to

$$(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2.$$

Consider the following expressions in four variables $\alpha_1, \alpha_2, \alpha_3, \alpha_4$:

$$p(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha_1 + i\alpha_2 - \alpha_3 - i\alpha_4, \qquad q(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = p(\alpha_1, \alpha_2, \alpha_3, \alpha_4)^4,$$

$$r(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4, \qquad s(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = r(\alpha_1, \alpha_2, \alpha_3, \alpha_4)^2.$$

Suppose we apply all 24 permutations of the variables $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ to each of these expressions. (For instance, applying these to $p(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, one of the 24 expression we get is $p(\alpha_4, \alpha_2, \alpha_1, \alpha_3)$. Another is, of course, the original expression, which we get from the identity permutation.) In some cases, when one expands two of the above expressions, they turn out to be equal; in other cases not.

For each of p, q, r and s, determine how many *distinct* expressions this procedure gives. (Your solution should not require you to list the 24 expansions in each case. Instead, you should use properties of these expressions to prove that some will be equal and others won't. To prove that two expressions are *not* equal you should find a way of assigning values for the α_i that give the expressions distinct values.)

''**Exercise 1.15**''. Given a cubic equation $y^3 + py + q = 0$ with real coefficients, suppose we solve it over the complex numbers using Cardano's formula, (1.7) on p.9, with the roots chosen as discussed at the bottom of that page. Show that if the square root occurring inside the cube roots in (1.7) is real and nonzero (i.e., is the square root of a positive real number) then only one of the three roots of the cubic is real, while if the square root is nonreal, all the roots of the cubic are real. Your proof should use only general properties of the arithmetic of complex numbers.

‘‘**Exercise 1.16**’’. In proving the existence of inverses in Exercise 1.5, we ran into the difficulty that the system of linear equations we had to solve had determinant $p^3 + 2q^3 + 4r^3 - 6pqr$, and we weren’t sure that would be nonzero. In this exercise you will prove that it must be so.

(i) Suppose there were rational numbers p, q, r, not all equal to zero, such that $p^3 + 2q^3 + 4r^3 - 6pqr = 0$. Show that there would also exist *integers* p, q, r not all zero satisfying this equation.

(ii) Suppose that p, q, r were integers not all equal to zero such that $p^3 + 2q^3 + 4r^3 - 6pqr = 0$. Show that if p is even, and we set $p' = q$, $q' = r$, $r' = p/2$, then these three integers would also satisfy that equation.

(iii) Deduce that if there were integers p, q, r not all zero that satisfied that equation, and we chose, from among all such 3-tuples of integers, one that made the positive integer $|p| + |q| + |r|$ as small as possible, then p would be odd.

(iv) Give an arithmetic reason why no 3-tuple of integers p, q, r with p odd can satisfy $p^3 + 2q^3 + 4r^3 - 6pqr = 0$. Conclude that for any three rational numbers p, q, r, not all zero, we have $p^3 + 2q^3 + 4r^3 - 6pqr \neq 0$.

This allows us prove, as desired, that every nonzero element of the form $p + \alpha q + \alpha^2 r$ has an inverse of the same form. But it in fact gives more:

(v) Deduce that if p, q, r are rational numbers, not all zero, then $p + \alpha q + \alpha^2 r \neq 0$.

‘‘**Exercise 1.17**’’. With notation as in Exercises 1.5 and 1.6, compute and simplify

$$(p + \alpha q + \alpha^2 r)(p + \omega\alpha q + \omega^2\alpha^2 r)(p + \omega^2\alpha q + \omega\alpha^2 r).$$

Chapter 2

Chapter 3

‘‘**Exercise 3.18**’’. Let n be a positive integer. This exercise will show that if we have, in an appropriate sense, a bound on the ‘‘size’’ of a polynomial f of degree n over $\mathbb{C}$, then we can bound the ‘‘sizes’’ of all factors of f. We begin with two results relating the size of a polynomial and the sizes of its zeros.

(a) For every positive real number r, find a positive real number $A(n,r)$ such that for any n complex numbers $\alpha_1, \dots, \alpha_n$ satisfying $|\alpha_n| \leq r$, the polynomial $(t - \alpha_1)\dots(t - \alpha_n)$ has all coefficients of absolute value $\leq A(n,r)$.

(b) For every positive real number s, find a positive real number $B(n,s)$ such that for any n complex numbers $c_0, \dots, c_{n-1}$ satisfying $|c_n| \leq s$, all the zeros of the polynomial $f = t^n + c_{n-1}t^{n-1} + \dots + c_1 t + c_0$ have absolute values $\leq B(n,s)$.

(Hint: For $|z|$ large, $f(z)$ is well approximated by z^n, hence if $|z|$ is large enough, $f(z)$ cannot be zero. Make this into a precise calculation that shows that no complex number of absolute value larger than a certain constant which you calculate in terms of n and s can be a zero of f. You are not required to find the smallest possible choice of $B(n,s)$, just one that you can prove works.)

The polynomials considered in (a) and (b) above have the property that the coefficient of the highest power of t is 1. A polynomial with this property is called *monic*. Stewart will introduce that term in Chapter 5 (p.58, last sentence). To simplify the statement of the next part I will use it here.

(c) For every positive real number s, find a positive real number $C(n,s)$ such that if $f(t)$ is a monic polynomial of degree n such that all coefficients of $f(t)$ are $\leq s$, and $g(t)$ is any monic polynomial dividing $f(t)$, then all coefficients of $g(t)$ must be $\leq C(n,s)$.

Suggestion: Combine the results of (a) and (b). You may take for granted the fact that every polynomial in $\mathbb{C}[t]$ is a product of linear factors. (A proof of this is sketched on pp.22-25 of the text, and another proof is developed in §23.)

‘‘**Exercise 3.19**’’. This exercise will justify Stewart’s statement on p.39, second paragraph, that the factorization of a polynomial over $\mathbb{Q}$ can always be reduced to testing a finite number of possibilities.

(a) Given a polynomial f over $\mathbb{Z}$, *not* necessarily monic, show with the help of Exercise ‘‘2.15’’ above how to compute a real constant D such that in every polynomial over $\mathbb{Z}$ dividing f, all coefficients have absolute value $\leq D$. (Hint: Given a polynomial g over $\mathbb{Z}$ dividing f, relate this to a *monic* polynomial over $\mathbb{Q}$ which divides a monic polynomial over $\mathbb{Q}$ obtained from f.)

(b) Conclude that given a polynomial f over $\mathbb{Z}$, one can list a finite set of polynomials over $\mathbb{Z}$, such that by testing whether each of these divides f, one can find a factor of f of smaller positive degree, if any exists. Why does this argument require that we work with polynomials over $\mathbb{Z}$, rather than over $\mathbb{Q}$?

(c) Deduce that the result of (b) holds with $\mathbb{Q}$ in place of $\mathbb{Z}$. Thus, with a finite amount of computation we can find all factors of any polynomial f over $\mathbb{Q}$.

We remark that the algorithm indicated above is *extremely* impractical, since the number of polynomials it requires one to test is enormous. But the more efficient an algorithm we want, the more work it is to describe it and prove its correctness. Since this exercise is a digression from the main topic of this course, we won’t go farther than showing the existence of an algorithm.

It is interesting that even though the result of this exercise concerns polynomials over $\mathbb{Z}$ and makes no mention of the field of complex numbers, we needed the complex numbers (called on in the preceding exercise) to prove it.

‘‘**Exercise 3.20**’’. Let p be a prime number.

(i) Show that if $n = p^2$, then in $\mathbb{Z}_n[t]$, the polynomial $pt + 1$ is invertible (i.e., has a multiplicative inverse in $\mathbb{Z}_n[t]$).

(ii) Is the same true if $n = p^k$ for arbitrary $k > 0$?

‘‘**Exercise 3.21**’’. Show by example that if hypothesis (1) is deleted from the statement of Eisenstein’s Criterion (Theorem 3.19, p.40), the resulting statement is false.

Chapter 4

‘‘**Exercise 4.11**’’. Let $K \subseteq L$ be fields, and let X and Y be subsets of L. It is not always true that $K(X \cap Y) = K(X) \cap K(Y)$. Prove that *one* of the two possible inclusions between these subfields of L always holds, and give an example in which the other inclusion fails.

‘‘**Exercise 4.12**’’. If $L:K$ is a field extension, and $f(t),\ g(t) \in K[t]$, show that f and g are coprime in $K[t]$ if and only if they are coprime in $L[t]$.

Chapter 5

Chapter 6

‘‘**Exercise 6.18**’’. In this exercise we shall determine the degrees of extensions of the form $F(x_1,\ldots,x_n):F(x_1^{d_1},\ldots,x_n^{d_n})$, where $x_1,\ldots,x_n$ are indeterminates over F and $d_1,\ldots,d_n$ are positive integers.

So let F be a field and $S = F[x_1,\ldots,x_n]$ be a polynomial ring in n indeterminates over F. We see that a basis for S over F is given by the set of all *monomials*, i.e., products of powers of our indeterminates:

$$\{x_1^{a_1}\ldots x_n^{a_n} \mid a_1,\ldots,a_n \text{ are nonnegative integers}\},$$

Let L denote $F(x_1,\ldots,x_n)$, the field of fractions of S, i.e., the field of rational functions in n indeterminates over F.

Now let $d_1,\ldots,d_n$ be positive integers and let $R = F[x_1^{d_1},\ldots,x_n^{d_n}]$, the subring of S generated over F by $x_1^{d_1}, \ldots, x_n^{d_n}$. (Warning: Don’t confuse monomials, i.e., expressions like $x_1^{a_1}\ldots x_n^{a_n}$ representing *products* of powers of indeterminates, with expression like ‘‘$x_1^{d_1},\ldots,x_n^{d_n}$’’ in the preceding sentence, which represent *lists* of powers of our indeterminates. The commas show the distinction.) This subring R thus has for F-basis the subset

$$\{x_1^{a_1 d_1}\ldots x_n^{a_n d_n} \mid a_1,\ldots,a_n \text{ are nonnegative integers}\}.$$

Let K denote the subfield of L generated by R.

Finally, let

$$B = \{x_1^{a_1}\ldots x_n^{a_n} \mid 0 \le a_i < d_i \text{ for } i = 1,\ldots,n\}.$$

Thus, B has $d_1\ldots d_n$ members.

(a) Show that L is spanned over K by B, and hence that $[L:K] \le d_1\ldots d_n$. (Hint: Regard L as $K(x_1,\ldots,x_n)$, and note that $x_1,\ldots,x_n$ are algebraic over K.)

(b) Show that every element of R can be represented in a unique way as a linear combination of elements of B with coefficients in the subring S. (You may be a little hand-wavy here, as long as you indicate clearly why the result is true.)

(c) Deduce from (b) that as a subset of L, B is linearly independent over K, hence is a basis of L over K, hence that $[L:K] = d_1\ldots d_n$.

The above result is useful in giving examples of extensions with specified properties.

There is a curious consequence of (a) above, which we shall illustrate in the case $n = 1$. Since in that case, our set of subscripts $\{1,\ldots,n\}$ is just $\{1\}$, let us drop subscripts and write $L:K$ as $F(x):F(x^d)$.

(e) Deduce from (a) that for any field F and any positive integer d, every element $\alpha\in F(x)$ can be written f/g with $f\in F[x]$, $g\in F[x^d]$. Taking $\alpha = 1/h$ ($h\in F[x]$), deduce that every nonzero polynomial $h\in F[x]$ has a nonzero multiple that lies in $F[x^d]$.

‘‘**Exercise 6.19**’’. Let $L:K$ be an algebraic extension, and f a nonzero element of $L[t]$. Show that there exists a nonzero $g\in L[t]$ such that $fg\in K[t]$. (Hint: Reduce the problem to the case where f is irreducible. In that case, note that f is the minimal polynomial of an element of an extension of L, and consider the minimal polynomial of the same element over K.)

Does your proof allow you to bound the degree of fg in terms of $[L:K]$ and the degree of f, assuming the former is finite?

‘‘**Exercise 6.20**’’. Show that every subextension of a simple algebraic extension of an infinite field is simple. You may make use of the result of Exercise 6.16.

(The corresponding statement is also true of simple transcendental extensions, but the proof is entirely different. I generally make it a full week’s assignment in Math 250A; cf. /~gbergman/grad .hndts/Luroth.ps .)

Chapter 7

‘‘**Exercise 7.18**’’. Show that if you are given a circle C and a square S of equal areas, then you can square any circle. (That C is ‘‘given’’ will be understood to mean that our given set P_0 includes the center of C and at least one point on its circumference. Similarly, understand S to be given by giving its four vertices. What you are asked to prove means that if P_0 also contains the center and a point on the radius of some other circle C', then from P_0 one can construct a square whose area equals that of C'.)

‘‘**Exercise 7.19**’’. Suppose P_0 consists of the single point $(1, 2^{1/3})$. Can one construct from P_0 a line segment of length $2^{1/3}$?

Chapter 8

‘‘**Exercise 8.13**’’. Let L be any field, and $\mathrm{Aut}(L)$ the group of *all* automorphisms of L as a field. Let P be the prime subfield of L. Show that $\mathrm{Aut}(L) = \Gamma(L:P)$.

‘‘**Exercise 8.14**’’. Let $L:K$ be any field extension.

(a) Suppose H_1 and H_2 are subgroups of $\Gamma(L:K)$, and let $H_1 \vee H_2$ denote the subgroup of $\Gamma(L:K)$ generated by the union of these two groups. Show that $(H_1 \vee H_2)^\dagger = H_1^\dagger \cap H_2^\dagger$.

(b) Suppose M_1 and M_2 are intermediate fields of $L:K$, and let $M_1 M_2$ denote the intermediate field generated by the union of these two fields. (In the notation introduced in Definition 4.7, p.31, this could be written as $M_1(M_2)$ or as $M_2(M_1)$.) Show that $(M_1 M_2)^* = M_1{}^* \cap M_2{}^*$.

‘‘**Exercise 8.15**’’. Deduce from the result of Exercise 8.4 that the field of symmetric rational functions in $t_1, \ldots, t_n$ is generated over K as a field by $s_1, \ldots, s_n$.

‘‘**Exercise 8.16**’’. Let $L:K$ and $E:F$ be field extensions.

(i) Show that if $L:K$ and $E:F$ are isomorphic extensions, then $\Gamma(L:K)$ and $\Gamma(E:F)$ are isomorphic groups.

(ii) Show by example that the converse to (i) is false.

Chapter 9

‘‘**Exercise 9.10**’’. The one example Stewart has shown us of a *non-normal* extension, $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ (p.111, top), is also the one example he has shown us of an extension of degree 3. It is not hard to modify this example to get a *normal* extension of degree 3, namely $\mathbb{Q}(\omega, \sqrt[3]{2}):\mathbb{Q}(\omega)$, where $\omega = e^{2\pi i/3}$. But one may wonder whether $\mathbb{Q}$ itself has any normal extensions of degree 3. The first time I taught this course, a student asked that question. This exercise answers it.

(a) Let $\zeta_7 = e^{2\pi i/7}$. Show that ζ_7 is algebraic over $\mathbb{Q}$, with minimal polynomial $p(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$. (Hint: Calculate $(t-1)\,p(t)$ and show that ζ_7 is a zero of that product but not a zero of $t - 1$. You showed in Exercise 3.5 that $p(t)$ was irreducible.)

(b) Deduce that $[\mathbb{Q}(\zeta_7):\mathbb{Q}] = 6$, and that a basis of $\mathbb{Q}(\zeta_7)$ over $\mathbb{Q}$ is given by *any six* of $1, \zeta_7, \zeta_7^2, \ldots, \zeta_7^6$. Write down the linear dependence relation satisfied by these seven elements.

For any integer r, let θ_r denote $\zeta_7^r + \zeta_7^{-r}$. You will show below that $\mathbb{Q}(\theta_1):\mathbb{Q}$ is a normal extension of degree 3. In the computations you make, I recommend expressing elements in terms of all 7 of the elements listed in (b), using the linear dependence relation when it seems appropriate.

(c) Show by computation that for any r, $\theta_{2r} \in \mathbb{Q}(\theta_r)$. What does this imply about the relation between $\mathbb{Q}(\theta_r)$ and $\mathbb{Q}(\theta_{2r})$?

(d) Verify that $\theta_4 = \theta_3$ and $\theta_8 = \theta_1$, and deduce with the help of (c) that $\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2) = \mathbb{Q}(\theta_3)$.

(e) Show by computation that the polynomial $(t - \theta_1)(t - \theta_2)(t - \theta_3)$ has coefficients in $\mathbb{Z}$. Deduce that $\mathbb{Q}(\theta_1):\mathbb{Q}$ is a splitting field, and conclude that it is normal.

(f) Show that ζ_7 satisfies a quadratic equation over $\mathbb{Q}(\theta_1)$.

(g) Deduce the relations

$$6 = [\mathbb{Q}(\zeta_7):\mathbb{Q}] = [\mathbb{Q}(\zeta_7):\mathbb{Q}(\theta_1)] \cdot [\mathbb{Q}(\theta_1):\mathbb{Q}] \leq 2 \cdot 3 = 6.$$

At each nontrivial step, it is enough to point to one of the results (a)-(f) and/or a result in Stewart from which the conclusion follows. In getting the ''≤'' step, actually show the corresponding inequality for each factor; this will be needed for the next part of this exercise.

(h) Deduce from (g) that $[\mathbb{Q}(\theta_1):\mathbb{Q}] = 3$. This and the last part of (f) give the desired example.

Chapter 10

''**Exercise 10.6**''. Show that if G is an infinite group of automorphisms of a field K, and K_0 its fixed field, then $[K:K_0]$ is infinite.

''**Exercise 10.7**''. In this exercise we will see that from the results of Chapter 10 alone, it is not hard to prove a version of the Fundamental Theorem of Galois Theory (Theorem 12.1) in which the ''finite separable normal'' hypothesis is replaced by the assumption that K is the fixed field of a finite group of automorphisms of L.

Let L be a field, G a finite group of automorphisms of L, K the fixed field of G, and M any field with $K \subseteq M \subseteq L$.

(a) Show, simply from the logic of the way ''fixed field'' and ''$\Gamma(L:K)$'' are defined, that G and $\Gamma(L:K)$ have the same fixed field.

(b) Deduce from (a) and Theorem 10.5 that $G = \Gamma(L:K)$.

Hence we may use the symbols $*$ and $\dagger$ introduced by Stewart to relate subgroups of G and fields between K and L. Now, using only results from Chapter 10 and earlier –

(c) Show that $[G:M^*] \leq [M:K]$. (Hint: Show that elements of G in different cosets of M^* act differently on M. You need to decide whether ''coset'' should here mean ''left coset'' or ''right coset'' for this to be true. Then apply a result in Chapter 10.)

(d) Show that $[G:M^*] \geq [M:K]$. (Hint: Apply Theorem 10.5, first for the given group G, and then with M^* in place of that group. What do we know at this point about inclusion relations between M and the fixed field of M^*?)

Combining the inequalities of (c) and (d), we conclude that $[G:M^*] = [M:K]$.

(e) Deduce that the operators $*$ and $\dagger$ relating intermediate fields of the extension $L:K$ and subgroups of G are inverse to one another. (Suggestion for showing $M = M^{*\dagger}$: Prove that $[L:M] = [L:M^{*\dagger}]$, and apply the Tower Law to $M \subseteq M^{*\dagger} \subseteq L$. The method for proving $H = H^{\dagger *}$ is similar, but in place of the equation gotten by combining parts (c) and (d), you can use a result proved in Chapter 10.)

''**Exercise 10.8**''. Using Corollary 10.6 and the Tower Laws for groups and for field extensions, we see that the result $[G:M^*] \leq [M:K]$ of part (c) of the preceding exercise is equivalent to $|M^*| \geq [L:M]$, and that the result $[G:M^*] \geq [M:K]$ of part (d) is likewise equivalent to $|M^*| \leq [L:M]$.

Now if we remove from the hypotheses of that exercise the assumption that G is finite, the Tower Law arguments are no longer applicable, so we can no longer say a priori that these pairs of conditions are equivalent. Investigate what subset of these four inequalities you can prove in this more general case, assuming only that one or the other side of the given inequality is finite.

(So four inequalities and two possibilities for which side to assume finite gives eight possible statements. Notice that ‘‘$[G:M^*] \leq [M:K]$ if $[M:K]$ is finite’’ would imply ‘‘$[G:M^*] \leq [M:K]$ if $[G:M^*]$ is finite’’ but not vice versa; and similarly for the other three inequalities.)

More generally, you might let $M \subseteq M'$ be intermediate fields, and consider the relation between $[M^*:M'^*]$ and $[M':M]$. Any equality or inequality concerning these would imply two results of the sort mentioned above, by taking $M = K$ on the one hand, and $M' = L$ on the other.

Chapter 11

‘‘**Exercise 11.8**’’. (a) Suppose $L:K$ is a normal algebraic extension, E any field containing L, and A any subset of E. Show that $\Gamma(L(A):K(A))$ is isomorphic to a subgroup of $\Gamma(L:K)$, the isomorphism being given by restricting elements of $\Gamma(L(A):K(A))$ to L. (You should begin by indicating why this restriction operation takes elements of $\Gamma(L(A):K(A))$ to elements of $\Gamma(L:K)$.)

(b) Show by example that the above result becomes false if $L:K$ is not assumed normal.

‘‘**Exercise 11.9**’’. Let $L:K$ be a finite normal algebraic extension.

(a) Suppose $f \in K[t]$ is monic, and irreducible over K, and let its factorization into monic irreducible polynomials over L be $f = g_1 \ldots g_n$. Show that for any $i, j \in \{1, \ldots, n\}$ there exists $\sigma \in \Gamma(L:K)$ such that $\sigma(g_i) = g_j$, where σ is defined to act on polynomials by acting on each coefficient, and fixing t.

(In the language that will be introduced on the bottom of p.251, this result says σ acts *transitively* on the set of monic irreducible factors of f in $L[t]$.)

(b) Deduce that if E is an extension field of L and $\alpha \in E$, then the degree of α over L divides the degree of α over K.

(c) Show by example that the results of (a) and (b) both fail if the assumption that $L:K$ is normal is removed.

Chapter 12

‘‘**Exercise 12.7**’’. Let L, K, G, $\mathcal{F}$, $\mathcal{G}$, $*$ and $\dagger$ be as in Theorem 12.1. Show that fields M, $M' \in \mathcal{F}$ are isomorphic by an isomorphism that is the identity on K if and only if M^* and M'^* are *conjugate*, meaning that there exists $\tau \in G$ such that $M'^* = \tau M^* \tau^{-1}$.

‘‘**Exercise 12.8**’’. Let L, K, G, $\mathcal{F}$, $\mathcal{G}$, $*$ and $\dagger$ be as in Theorem 12.1, and let $M \in \mathcal{F}$. We wish to determine $\Gamma(M:K)$ purely in terms of the group G and its subgroup M^*. This was done in part 5 of that theorem in the case where M is normal; we shall do it here for arbitrary M.

Let $H = \{\tau \in G \mid \tau M^* \tau^{-1} = M^* = \tau^{-1} M^* \tau\}$. For every $\tau \in H$, let $\varphi(\tau)$ denote $\tau|_M$.

(a) Show that H is a subgroup of G and contains M^*.

(b) Show that for every $\tau \in H$, $\varphi(\tau) \in \Gamma(M:K)$, and show that φ is a homomorphism $H \to \Gamma(M:K)$.

(c) Show that the homomorphism φ is onto, and that its kernel is M^*, and conclude that $\Gamma(M:K) \cong H/M^*$.

This is what we wanted. Let us note one further fact.

(d) Show that the fixed field of $\Gamma(M:K)$ is $H^\dagger$. (Note that ‘‘the fixed field of $\Gamma(M:K)$’’ means the subfield of M that it fixes, while $H^\dagger$ means the subfield of the whole field L that H fixes.)

Here is some relevant terminology: If E is a subgroup of any group G, then $\{\tau \in G \mid$

$\tau E \tau^{-1} = E = \tau^{-1} E \tau\}$ is the largest subgroup H of G such that E is *normal* in H, and is therefore called the *normalizer* of E in G, often written $N_G(E)$. The final result of (c) above thus says that for an intermediate field M of a finite separable normal field extension $L:K$, one has

$$\Gamma(M:K) \;\cong\; N_{\Gamma(L:K)}(M^*)/M^*.$$

‘‘**Exercise 12.9**’’. We saw in ‘‘Exercise 11.8’’ that if $L:K$ is a normal algebraic extension, E a field containing L, and A a subset of E, then $\Gamma(L(A):K(A))$ is isomorphic to a subgroup of $\Gamma(L:K)$, via restriction of isomorphisms. Now let us assume $L:K$ not only normal but also finite and separable. Then the Fundamental Theorem of Galois Theory tells us that subgroups of $\Gamma(L:K)$ correspond to fields between K and L, and is natural to ask what field between K and L the above subgroup corresponds to. Show that it corresponds to the field $L \cap K(A)$.

(This is the result that I find in other texts called the Theorem of Natural Irrationalities. That seems a reasonable name if we understand ‘‘irrationality’’ to mean ‘‘algebraic element’’, since the result says that $K(A)$ has to contain those algebraic elements of L that are suggested by the failure of some members of $\Gamma(L:K)$ to extend to elements of $\Gamma(L(A):K(A))$. But the connection with the result Stewart calls the Theorem of Natural Irrationalities is not clear to me.)

‘‘**Exercise 12.10**’’. Show that every finite separable field extension is simple. (You may make use of the result of Exercise 6.16.)

Chapter 13

‘‘**Exercise 13.13**’’. Let us apply ‘‘Exercise 12.8’’ to the separable normal field extension $\mathbb{Q}(\xi, i):\mathbb{Q}$ of Chapter 13, taking $M = \mathbb{Q}(\xi)$.

What is M^*? Determine the normalizer H of M^* in G, describe H/M^* as a group of automorphisms of M, and verify that its fixed field is $H^\dagger$.

‘‘**Exercise 13.14**’’. In this exercise, we will study the Galois theory of the splitting field of the polynomial $t^3 - 2$ over $\mathbb{Q}$, as Stewart does in Chapter 13 for $t^4 - 2$. Let us begin by naming the zeros of $t^3 - 2$. Letting $\sqrt[3]{2}$ denote the real cube root of 2, and $\omega = e^{2\pi i/3} = (-1+\sqrt{-3})/2$, we set

$$\rho_1 \;=\; \sqrt[3]{2}, \qquad \rho_2 \;=\; \omega\sqrt[3]{2}, \qquad \rho_3 \;=\; \omega^2\sqrt[3]{2} \;=\; \bar{\omega}\sqrt[3]{2}.$$

Thus our splitting field is

$$L \;=\; \mathbb{Q}(\rho_1, \rho_2, \rho_3) \;=\; \mathbb{Q}(\sqrt[3]{2},\, \omega).$$

Now for every automorphism σ of L, the elements $\sigma(\rho_1)$, $\sigma(\rho_2)$, $\sigma(\rho_3)$ will be some rearrangement of the three elements ρ_1, ρ_2, ρ_3; i.e., there will be some permutation $\bar{\sigma} \in \mathbb{S}_3$ such that $\sigma(\rho_i) = \rho_{\bar{\sigma}(i)}$ for $i = 1, 2, 3$. If we define $\bar{\sigma}$ in this way for each $\sigma \in \Gamma(L:\mathbb{Q})$, it is easy to verify that the map $\sigma \mapsto \bar{\sigma}$ is a group homomorphism.

Now for your tasks:

(a) Show that this homomorphism $\sigma \mapsto \bar{\sigma}$ is one-to-one.

(b) Deduce by comparing orders of groups that this homomorphism is an isomorphism $G \to \mathbb{S}_3$.

(c) Draw the lattice of subgroups of $\mathbb{S}_3$. Each subgroup other than $\mathbb{S}_3$ should be described by listing its elements. Write the nonidentity elements in cycle-notation (e.g., (13)), and the identity element as 1. You need not justify the statement that the subsets you list are subgroups (though of course, if some are not, you will lose credit), but you should say briefly how we can see that $\mathbb{S}_3$ has no *other* subgroups than those you list.

When two different subgroups in your picture are conjugate to one another (have the forms H and $\tau H \tau^{-1}$ for some $\tau \in G$), connect them with a dotted curve. Thus, the only subgroups not connected to any others by dotted curves will be the normal subgroups.

Since we found that the map $\sigma \mapsto \bar{\sigma}$ was an isomorphism, it has an inverse, an isomorphism $\mathbb{S}_3 \to G$, which we will write $\pi \mapsto \tilde{\pi}$. Thus, putting a $\tilde{}$ over each permutation in the above diagram of subgroups of $\mathbb{S}_3$ transforms that diagram into the diagram of all subgroups of G. Now

(d) List the *fixed field* of each subgroup of G. For *one* such subgroup other than $\{1\}$ or G, show explicitly that the set of elements fixed by that subgroup is precisely the fixed field you listed.

(e) Choose one pair of distinct conjugate subgroups, and verify Lemma 12.2 (p.134) for this case.

(f) The group $\mathbb{S}_3$ has one nontrivial proper normal subgroup N. List it, describe the factor-group $\mathbb{S}_3/N$, and describe the identification of this factor group with the Galois group of the corresponding subextension of L.

(Remark: Stewart says in the second paragraph of Chapter 13 (p.137) that an example simpler than the one of that chapter would be too small to illustrate the theory adequately. The example of this exercise comes close; the one feature of the theory that it does not adequately illustrate is the fact that inclusions of subgroups correspond to inclusions of intermediate fields, since there are no inclusions between distinct proper nontrivial subgroups of $\mathbb{S}_3$.)

‘‘**Exercise 13.15**’’. You may have noticed that when the intermediate fields of $\mathbb{Q}(\xi, i):\mathbb{Q}$ were determined in Chapter 13, two of them had generators that looked more complicated than the others: $\mathbb{Q}((1+i)\,\xi)$ and $\mathbb{Q}((1-i)\,\xi)$. Let us see what this is about.

(a) Show that $(1+i)\,\xi$ and $(1-i)\,\xi$ are fourth roots of -8.

(b) Deduce that $K = \mathbb{Q}(\xi, i)$ is also the splitting field of t^4+8 over $\mathbb{Q}$.

(c) Deduce from (a) that K is also the splitting field of t^4+2 over $\mathbb{Q}$.

(d) Let θ denote the fourth root of -2 in the first quadrant of $\mathbb{C}$. Express θ in terms of ξ and i in the form shown in the first displayed equation on p.140, and express ξ similarly in terms of θ and i.

(e) Sketch the set of zeros of t^4+2 in $\mathbb{C}$ as the vertices of a square in the plane, on a diagram that also shows the zeros of t^4-2. Show that the Galois group $\Gamma(K:\mathbb{Q})$ also acts on the zeros of t^4+2 as the group of symmetries of that square. Show, however, that there are elements of that group which act by a 2-cycle on the zeros of the former polynomial but as a product of two 2-cycles on the zeros of the latter, and vice versa.

‘‘**Exercise 13.16**’’. (a) Show that points 1-8 of Chapter 13 go over virtually unchanged if the given polynomial t^4-2 is replaced by t^4-a for any positive integer a which is divisible by some prime p but not by p^2. To do this, you must look carefully through Stewart’s arguments, note every point where he uses, explicitly or implicitly, properties of the final term ‘‘-2’’ of the given polynomial, and show that these remain valid for ‘‘$-a$’’.

(I don’t ask you to do the same for the remaining points, 9-13, because they are mostly hand-wavy or discursive, so it would be hard to pin down what was to be verified.)

In particular, the Galois group of the splitting field of any such polynomial is $\mathbb{D}_8$.

(b) Suppose b is a *rational* number which is not a square or the negative of a square. Show that a splitting field of t^4-b is also a splitting field of t^4-a for some positive integer a which is divisible by a prime p but not by p^2. Deduce that the Galois group of the splitting field of t^4-b is $\mathbb{D}_8$.

(Suggestion on how to think about the problem if you don’t see where to start: Begin with the two cases where b has the forms p^3 and p^5 for p a prime, show in each that $\mathbb{Q}(b^{1/4}) = \mathbb{Q}(p^{1/4})$, and deduce an equality of splitting fields. Generalize your method to the case where b is any positive rational number in which some prime p appears to an odd exponent. If b is the negative of such a rational number, use the idea of Exercise ‘‘13.15’’ above to find a *positive* rational number b' not a square such that the splitting fields of $t^4 - b$ and of $t^4 - b'$ are the same.)

(c) On the other hand, show that if $b \in \mathbb{Q}$ is a square or the negative of a square, then the splitting field of $t^4 - b$ over $\mathbb{Q}$ has degree ≤ 4, hence its Galois group is not $\mathbb{D}_8$. (The less straightforward case is where $b = -c^2$. I suggest reducing this to a case with positive b as in part (b) above.)

Chapter 14

‘‘**Exercise 14.1′**’’. Same as Stewart's Exercise 14.1 (p.151) except that, instead of Stewart's characterization of $\mathbb{D}_{2n}$ by generators and relations, use the definition

$$\mathbb{D}_{2n} = \{t_0, \ldots, t_{n-1}, r_0, \ldots, r_{n-1}\},$$

where these symbols denote the permutations of the elements of $\mathbb{Z}_n$ given by the formulas

$$t_i(m) = i + m, \qquad r_i(m) = i - m \qquad (m \in \mathbb{Z}_n, \text{ arithmetic done in } \mathbb{Z}_n).$$

(Here t stands for ‘‘translation’’ and r for ‘‘reflection’’. If you label the vertices of a regular n-gon with the elements of $\mathbb{Z}_n$, then $\mathbb{D}_{2n}$ becomes the group of symmetries of this n-gon. The a and b of Stewart's presentation correspond to the t_1 and r_0 respectively in our description.)

‘‘**Exercise 14.14**’’. (a) Show that any group G has a *least* normal subgroup N such that G/N is abelian; i.e., that among all normal subgroups N with G/N abelian, there is one which is contained in all the others. (Suggestion: Use the properties of commutators referred to in the first paragraph of the proof of Lemma 8.11, p.97.)

The standard symbol for the subgroup N of part (a) is G'. One writes G'' for $(G')'$, G''' for $(G'')'$, etc., and $G^{(n)}$ for G followed by n $'$s. (In particular, $G^{(0)} = G$.)

(b) Show that if H is a normal subgroup of a group G, then H' is also normal in G (even though in general, a normal subgroup of a normal subgroup need not be normal).

(c) Show that if we are given a chain of subgroups $G_0 \lhd G_1 \lhd \ldots \lhd G_t = G$ such that G_{i+1}/G_i is abelian for each i, then $G_{t-i} \supseteq G^{(i)}$ for each i.

(d) Deduce that a group G is solvable if and only if for some nonnegative integer i, one has $G^{(i)} = 1$.

(e) Deduce that a group G is solvable if and only if it has a chain of subgroups $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_t = G$, with all G_i normal in G (not merely in the next subgroup) and G_{i+1}/G_i abelian for each i.

‘‘**Exercise 14.15**’’. (a) Suppose G is a group, and H a subgroup. Show that $\bigcap_{g \in G} gHg^{-1}$ is a normal subgroup of G, and is the largest normal subgroup of G contained in H.

(b) Let G be a group, and H, E subgroups of G such that $H \lhd E$. Show that if E/H is abelian, then $(\bigcap_{g \in G} gEg^{-1})/(\bigcap_{g \in G} gHg^{-1})$ makes sense, and is also abelian.

(c) Use the result of (b) to get a proof of part (e) of Exercise ‘‘14.14’’ without the help of the earlier parts of that exercise.

‘‘**Exercise 14.16**’’. Suppose G is a simple group, and p a prime dividing the order of G. Show that G is generated by the set of its elements of order p. (Hint: Show that the subgroup generated by these elements is normal.)

‘‘**Exercise 14.17**’’. Let G be a finite group. Show that G is solvable if and only if every nontrivial subgroup H of G has a proper normal subgroup $N \lhd H$ such that H/N is abelian.

Chapter 15

‘‘**Exercise 15.13**’’. The examples we have seen so far of noncommutativity in Galois groups of radical extensions arise from the interaction of the way automorphisms move nth roots of unity and the way they move nth roots of other elements. In this exercise we shall see how a normal radical extension whose automorphisms do not move any roots of unity (for instance, an extension having all roots of unity in the base field) can still have noncommutative Galois group.

To get the desired extension field, we start with any field F of characteristic $\neq 2$ (e.g., $\mathbb{C}$), adjoin an indeterminate x, and then adjoin to $F(x)$ elements $\sqrt{1+x}$ and $\sqrt{1-x}$, i.e., zeros of $t^2-(1+x)$ and $t^2-(1-x)$ respectively. Let us call the resulting field

$$L \;=\; F(x, \sqrt{1+x}, \sqrt{1-x}).$$

We now consider L as an extension, not of F or $F(x)$, but of the field

$$K \;=\; F(x^2) \;\subseteq\; F(x).$$

However, we will not ignore $F(x)$; it will play a key role as intermediate field in our calculations.

(a) Show that the extension $F(x):K$ is separable and normal, determine its Galois group, and describe the action of this group on the zeros of a particular polynomial $f(t)$ over K of which $F(x)$ is the splitting field.

(b) Show that $\sqrt{1+x} \notin F(x, \sqrt{1-x})$ and that $\sqrt{1-x} \notin F(x, \sqrt{1+x})$. (Suggestion: Verify that $F(x, \sqrt{1-x}) = F(\sqrt{1-x})$ and that this is a simple transcendental extension of F, which we may write $F(y)$. Find a polynomial over $F(y)$ which has $\sqrt{1+x}$ as a zero, and prove that this polynomial has no zero in $F(y)$.)

(c) Show that the extension $L:F(x)$ is separable and normal, determine its degree and its Galois group, and describe the action of this group on the zeros of a particular polynomial $g(t)$ over $F(x)$ of which L is the splitting field.

(d) Now show that the extension $L:K$ is separable and normal, determine its Galois group, and describe the action of this group on the zeros of a particular polynomial $h(t)$ over K of which L is the splitting field. Show that this group is isomorphic to $\mathbb{D}_8$.

(d) Indicate (no proof necessary) the relationships between the Galois groups found in (a) and (b) and that found in (c), arising from the relationships among the field extensions.

(Remarks: Similar examples can be obtained with $\mathbb{Q}$ in the role of K; i.e., one can adjoin to $\mathbb{Q}$ the square root of a rational number r, then square roots of $1+\sqrt{r}$ and $1-\sqrt{r}$, and under appropriate conditions the Galois group will be $\mathbb{D}_8$. But to imitate the above proof, we need to know things about the arithmetic of $\mathbb{Q}(\sqrt{r})$, which we have not studied in this course. For a reduction of this question to arithmetic in $\mathbb{Q}$, and an explicit example, see Lang, *Algebra*, 3rd edition, Exercise 8, p.322. Modifying our example in a different direction, if m and n are positive integers, and F a field in which t^m-1 and t^n-1 split and have no multiple zeros, then in place of the quadratic extension $F(x):F(x^2)$ of the above exercise, we could use the extension $F(x):F(x^n)$, and instead of adjoining square roots of the two elements $1\pm x$ we could adjoin mth roots of the n elements $1+\zeta x$, where ζ runs over the nth roots of unity in F. In this case, we get for Galois group a noncommutative group of order $n\,m^n$.)

‘‘**Exercise 15.14**’’. Deduce from the existence of a polynomial with Galois group $\mathbb{S}_5$ an affirmative answer to Stewart’s Exercise 15.12(f) (p.162). (Note that that problem does not specify the base field; you are free to choose it to make your example work.)

‘‘**Exercise 15.15**’’. (a) Show that if $L:K$ is a normal radical extension, with $L \subseteq \mathbb{R}$, then $[L:K]$ is a power of 2. (Suggestion: Use ideas from the proof of Lemma 15.7.)

(b) Show by example that the statement of (a) becomes false if the condition ‘‘normal’’ is deleted.

(c) Also show by example that the statement of (a) becomes false if ‘‘normal’’ is kept, but ‘‘radical extension’’ is replaced by ‘‘extension which is contained in a radical extension $M \subseteq \mathbb{C}$’’. (Suggestion: Try the extension of Exercise ‘‘9.10’’. As discussed in class, that extension is an instance of the situation Stewart refers to on p.154, paragraph following Definition 15.2.)

Chapter 16

Chapter 17

‘‘**Exercise 17.15**’’. Let $E{:}K$ be a field extension, and let L, M be fields between K and E. Clearly, $L \cap M$ is the largest field contained in both L and M. The smallest subfield of E containing both L and M is the subfield generated by $L \cup M$. Let us (as in Exercise ‘‘8.14’’(b)) denote this LM.

(a) Show that if L and M are finite and normal over K, then so is $L \cap M$.

(b) Show that if L and M are finite and normal over K, then so is LM.

(c) Show that if L and M are finite and separable over K, then so is $L \cap M$.

(d) Show that if L and M are finite and separable over K, then so is LM.

‘‘**Exercise 17.16**’’. Let K be a field, G a finite group of automorphisms of K, and K_0 the fixed field of G. (In the notation of p.93, $K_0 = G^\dagger$.)

(a) Suppose $x \in K$, and let $x_1, \dots, x_n$ be the *distinct* elements gx as g ranges over the elements of G. (Thus, if different elements of G send x to the same element, say $gx = g'x$, this element still appears only once on this list.) Show that $(t - x_1) \dots (t - x_n) \in K_0[t]$.

(b) Deduce that $K{:}K_0$ is separable and normal.

‘‘**Exercise 17.17**’’. Let M_0, M_1 be subfields of a field L, such that $L{:}M_0$ and $L{:}M_1$ are both normal. In this exercise you will prove that $L{:}(M_0 \cap M_1)$ is normal.

To do this, suppose f is any monic irreducible polynomial over $M_0 \cap M_1$ which has a zero α in L. In $L[t]$, let us write $f(t) = (t - \alpha_1) \dots (t - \alpha_n)\, g(t)$, where the α_i are the zeros of $f(t)$ in L (possibly repeated if some of them are multiple zeros), and $g(t)$ is a polynomial having no zeros in L.

(a) Show that $(t - \alpha_1) \dots (t - \alpha_n) \in M_0[t]$. (Hint: Consider the factorization of $f(t)$ over M_0, and separate it into the factors that have a root in L and factors that don’t.)

(b) Deduce that $(t - \alpha_1) \dots (t - \alpha_n) \in (M_0 \cap M_1)[t]$, and hence that $g(t) \in (M_0 \cap M_1)[t]$.

(c) Deduce that $g(t) = 1$ and thus that $f(t)$ splits over $M_0 \cap M_1$.

(d) Conclude that $L{:}(M_0 \cap M_1)$ is normal, as desired.

(Remark: Even if $L{:}M_0$ and $L{:}M_1$ are both algebraic, $L{:}(M_0 \cap M_1)$ may not be; this is shown in ‘‘Exercise 17.18’’ below. Many authors restrict the term ‘‘normal’’ to algebraic extensions. If one makes that restriction, one can adjust this exercise to start with the assumption that M_0 and M_1 are intermediate fields in an algebraic extension $L{:}K$, so as to guarantee that $L{:}(M_0 \cap M_1)$ is algebraic. The rest of the proof would remain unchanged.)

‘‘**Exercise 17.18**’’. Let L be the field $\mathbb{C}(x)$ of rational functions in one indeterminate over the complex numbers, let $\sigma\colon L \to L$ be the map sending each rational function $f(x) \in L$ to $f(-x)$, and let $\tau\colon L \to L$ be the map sending $f(x)$ to $f(1-x)$. You may take for granted in this exercise that σ and τ are both well-defined homomorphisms. (It is not hard to show that they give homomorphisms on the polynomial ring $\mathbb{C}[x]$, and Exercise 16.8 allows one to extend these from $\mathbb{C}[x]$ to its field of fractions $\mathbb{C}(x)$.) We see that σ^2 and τ^2 are both the identity map of L, so both σ and τ are automorphisms of L.

Let M_0 denote the fixed field of σ, and M_1 the fixed field of τ. (In the notation of p.93 these are $\{1,\sigma\}^\dagger$ and $\{1,\tau\}^\dagger$, where 1 denotes the identity automorphism of L; since σ and τ each have order 2, $\{1,\sigma\}$ and $\{1,\tau\}$ are subgroups.)

(a) Show that $L:M_0$ and $L:M_1$ are finite algebraic extensions. (Hint: Show $L = M_0(x)$.)

(b) Show that $M_0 \cap M_1 = \mathbb{C}$, and deduce that $L:(M_0 \cap M_1)$ is transcendental. (Suggestion: For $f(x) \in M_0 \cap M_1 = \mathbb{C}$, show that if f is written in ''lowest terms'', then the set of zeroes in $\mathbb{C}$ of its numerator is closed under the maps $z \mapsto -z$ and $z \mapsto 1-z$, and the same is true of the set of zeroes of its denominator. Deduce that these sets are closed under the composite of those two maps. What form does that composite have?)

''**Exercise 17.19**''. Show that if $f(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0$ is an irreducible polynomial over a finite field K of characteristic p, then there is some m not divisible by p such that $a_m \neq 0$.

''**Exercise 17.20**''. Let $L:K$ be a finite separable extension that is *not* normal, and N a normal closure of L over K. Show that $\Gamma(N:K)$ is noncommutative.

''**Exercise 17.21**''. Suppose $L:K$ is a finite inseparable extension of characteristic p.

(a) Show that there exist fields M, M' with $K \subseteq M \subset M' \subseteq L$ such that M' is obtained from M by adjoining a pth root of an element which is not a pth power in M.

(b) Deduce that $|\Gamma(L:K)| < [L:K]$. (Suggestion: Apply the Tower Law to the fields of part (a), and modify the reasoning of Theorem 11.10 to take account of the case where the zeroes of a polynomial are *not* distinct.)

''**Exercise 17.22**''. Let $L:K$ be an algebraic extension, and N, N' intermediate fields such that L is normal over both N and N'. Exercise ''17.17'' above outlined a lengthy proof that L is normal over $N \cap N'$. However, when $L:K$ is finite and separable there is a much quicker proof using the Fundamental Theorem of Galois Theory. Give such a proof.

Chapter 18

''**Exercise 18.13′**''. (Clarification of Stewart's Exercise 18.13.) (i) If f in Exercise 18.12 is irreducible over K, show that the Galois group of L is cyclic.

(ii) Conversely, if K is a field of positive characteristic p and L is a separable normal extension whose degree is this same prime p (which necessarily has cyclic Galois group), show that L is the splitting field of a polynomial of the form $t^p - t - a$ over K. (Hint: Exercise 18.7.)

(iii) Deduce a characterization of finite extensions with solvable Galois group in characteristic p.

''**Exercise 18.15**''. Let us write ''tr.deg$(L:K)$'' for the transcendence degree of a finitely generated field extension $L:K$. Prove the following ''tower law'' for transcendence degrees: If $K \subseteq L \subseteq M$, with L and M each finitely generated over K, then

$$\text{tr.deg}(M:K) = \text{tr.deg}(M:L) + \text{tr.deg}(L:K).$$

''**Exercise 18.16**''. Let K be a field, let n be a positive integer not divisible by the characteristic of K, and let $M = K(u_2, \ldots, u_n)$ be an extension of K gotten by adjoining $n-1$ independent transcendentals $u_2, \ldots, u_n$. Let g be the polynomial $t^n + u_2 t^{n-2} - u_3 t^{n-3} + \ldots \pm u_n$ over M (i.e., like the ''general polynomial'' of this chapter, but with no t^{n-1} term, and with coefficients called u_i instead of s_i). Deduce from the results of this chapter that the Galois group of g is isomorphic to $\mathbb{S}_n$. (Hint: Apply a Tschirnhaus transformation to the ''general polynomial'' over K.)

''**Exercise 18.17**''. (This is based on Exercise 14.9 in Stewart's second edition, which Stewart attributes to Ramanujan. I give more details than Stewart did, and drop some unnecessary assumptions.)

Let K be a field, and $a \in K$. Below, when no additional conditions are stated, ''L'' will denote an arbitrary extension field of K. For any such L, let X_L denote the set of all 3-tuples (x, y, z) of elements of L satisfying

$$x^2 = y + a$$
$$y^2 = z + a$$
$$z^2 = x + a\,.$$

(a) Show that if $(x, y, z) \in X_L$, then $K(x) = K(y) = K(z)$. (Hint: Use the above equations to express each component of the given 3-tuple in terms of another by field operations.)

(b) Write down a polynomial f over K such that an element x of an extension field L of K is the first member of a 3-tuple in X_L if and only if it is a zero of f. (Hint: As noted in (a), the components of such a 3-tuple are expressible in a cyclic manner in terms of each other. By substitution, you can get an expression for one of them in terms of itself, which is a polynomial relation.) You do not have to ''expand this polynomial out'', but you should show why it has the property asserted, and should note its degree.

(c) Similarly write down a polynomial $g(t)$ over K whose zeros in any extension L are all elements of L which are first components of members of X_L having the special form (x, x, x). Show that $g \mid f$.

(d) Let us call a set of elements of an extension field L of K a ''cluster'' if it is the set of entries of some 3-tuple $(x, y, z) \in X_L$. (Thus, a cluster will contain between one and three elements, depending on the number of repetitions in the 3-tuple in question.) Show that over any extension L of K, there are at most two 1-element clusters, at most two 3-element clusters, and no 2-element clusters.

(e) Show that if $\alpha \in \Gamma(L{:}K)$, and if $\{x, y, z\}$ is a cluster, then so is $\{\alpha(x), \alpha(y), \alpha(z)\}$.

(f) Using the result of (e), obtain a homomorphism φ from $\Gamma(L{:}K)$ into the group of all permutations of the set of clusters in L. (Do not confuse the *set of clusters* with the set of those elements of L which are *members* of clusters!) Show from the result of (d) that the image of φ is an abelian group of order dividing 4.

(g) Now suppose that L is a splitting field of the polynomial f of (b). Thus, each element of $\Gamma(L{:}K)$ is determined by the permutation it induces on the set of zeros of f. Show that for φ defined as in (f), $\mathrm{Ker}(\varphi)$ is an abelian group of order dividing 9, and deduce using the series

$$1 \lhd \mathrm{Ker}(\varphi) \lhd \Gamma(L{:}K)$$

that $\Gamma(L{:}K)$ is solvable, of order dividing 36.

(h) Assuming the characteristic of K is not 2 or 3, find expressions in radicals for the zeroes of the polynomial f of (b).

''**Exercise 18.18**''. In the second display on p.203, Stewart lists three ''natural'' expressions that are fixed by the Klein four-group $\mathbb{V}$, and permuted by $\mathbb{S}_4$. But other equally natural expressions with these properties are easy to give; for instance

$$x_1 = t_1 t_2 + t_3 t_4 \qquad\qquad z_1 = (t_1 + t_2 - t_3 - t_4)^2$$

$$x_2 = t_1 t_3 + t_2 t_4 \qquad \text{or} \qquad z_2 = (t_1 - t_2 + t_3 - t_4)^2$$
$$x_3 = t_1 t_4 + t_2 t_3 \qquad\qquad\quad z_3 = (t_1 - t_2 - t_3 + t_4)^2$$

Show, however, that these are ''essentially the same'' as the expressions Stewart gives, by obtaining linear relations between s_1^2, x_i, y_i, and z_i (where s_1 is the elementary symmetric polynomial $t_1 + t_2 + t_3 + t_4$) which hold for $i = 1, 2, 3$. Conclude that after application of a Tschirnhaus transformation as on p.204 bottom, for each i the expressions x_i, y_i, and z_i differ only by a constant factor.

''**Exercise 18.19**''. Given positive integers $j \leq n$, let $s_j^{(n)}(t_1, \ldots, t_n)$ denote the elementary symmetric polynomial of degree j in n indeterminates $t_1, \ldots, t_n$. (For example, in the 3rd-from-last display on p.194, s_j denotes $s_j^{(n)}$, while s_j' denotes $s_j^{(n-1)}$).

For arbitrary positive integers $m \leq n$, find and prove a formula expressing the elementary symmetric polynomials $s_j^{(n)}(t_1, \ldots, t_n)$ $(0 \leq j \leq n)$ in terms of the polynomials $s_h^{(m)}(t_1, \ldots, t_m)$ $(0 \leq h \leq m)$ and the polynomials $s_i^{(n-m)}(t_{m+1}, \ldots, t_n)$ $(0 \leq i \leq n-m)$.

(Hint: In a given elementary symmetric polynomial $s_j^{(n)}(t_1, \ldots, t_n)$, each monomial occurring can be written as the product of some subset of $\{t_1, \ldots, t_m\}$ and some subset of $\{t_{m+1}, \ldots, t_n\}$. Which subsets of $\{t_1, \ldots, t_m\}$ get multiplied by which subsets of $\{t_{m+1}, \ldots, t_n\}$? The equation on p.195 mentioned above can be looked at as such a formula for $m = n-1$.)

''**Exercise 18.20**''. This exercise will show how the norm and trace functions can be defined for not necessarily normal extensions.

Let $L{:}K$ be a finite separable extension, and M the normal closure of L over K. Let $\tau_1, \ldots, \tau_n$ be the K-monomorphisms of L into M. For $\alpha \in L$, define

$$N_{L:K}(\alpha) = \tau_1(\alpha) \ldots \tau_n(\alpha), \qquad\qquad T_{L:K}(\alpha) = \tau_1(\alpha) + \ldots + \tau_n(\alpha).$$

(a) Show that $N_{L:K}$ and $T_{L:K}$ are functions $L \to K$, that $N_{L:K}$ respects multiplication (i.e., satisfies $N_{L:K}(\alpha\beta) = N_{L:K}(\alpha)\, N_{L:K}(\beta)$) and that $T_{L:K}$ is K-linear and nonzero.

Since $M{:}K$ is also a finite separable extension, we can similarly define maps $N_{M:K}$ and $T_{M:K}$ from M to K.

(b) Show that $N_{M:K}$ and $T_{M:K}$ are the norm and trace functions called N and T in the text.

(c) Prove simple formulas for the restrictions of $N_{M:K}$ and $T_{M:K}$ to L in terms of $N_{L:K}$ and $T_{L:K}$.

Finally, we have the analogous maps $N_{M:L}$, $T_{M:L}$: $M \to L$. (These are again instances of the definition of the text, since $M{:}L$ is also normal.)

(d) Show that $N_{M:K}(\alpha) = N_{L:K}(N_{M:L}(\alpha))$ and that $T_{M:K}(\alpha) = T_{L:K}(T_{M:L}(\alpha))$ for all $\alpha \in M$.

Chapter 19

''**Exercise 19.12**''. Let us call a separable algebraic extension $E{:}K$ *constructible* if there exists a finite chain of subextensions

(*) $$K = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_r = E$$

such that

$$[E_{i+1} : E_i] = 2 \qquad (i = 0, \ldots, r-1).$$

(This is the condition used in Theorem 19.4, p.214, with a slight change of notation. However we are not assuming, as that theorem does, that our fields are subfields of $\mathbb{R}$.)

(a) Suppose E, F are intermediate fields in an extension $L{:}K$, and let us write EF for the field they generate. Show that if $E{:}K$ and $F{:}K$ are both constructible, then so is $EF{:}K$.

(b) Deduce that if $E:K$ is a constructible extension, and L is the normal closure of $E:K$, then $L:K$ is a constructible extension.

(c) Deduce that not every separable field extension of degree a power of 2 is constructible. (Suggestion: Let $f \in K[t]$ be a polynomial of degree 4 with Galois group $\mathbb{S}_4$, and $E:K$ the extension obtained by adjoining to K a zero of f.)

(d) Show that every subextension of a constructible extension is constructible. (Suggestion: look at Galois groups, and imitate the proof of Theorem 14.4(i).)

(e) Deduce that the following conditions on a separable extension $E:K$ are equivalent:

(i) $E:K$ is constructible.

(ii) E is contained in a constructible extension of K.

(iii) The normal closure of $E:K$ has degree a power of 2.

‘‘**Exercise 19.13**’’. Although the prime 2 has a special significance in connection with ruler-and-compass constructions, we may ask whether the purely field-theoretic results of Exercise ‘‘19.12’’ are restricted to this prime, or are true for other primes, e.g., 3. To investigate this, let us call an extension $E:K$ ‘‘3-constructible’’ if there exists a chain (*) (see Exercise ‘‘19.12’’) such that each degree $[E_{i+1}:E_i]$ is 3. Let us likewise call $E:K$ ‘‘$\{2,3\}$-constructible’’ if there exists a chain (*) such that each degree $[E_{i+1}:E_i]$ is 2 or 3, and finally, let us call it ‘‘strongly 3-constructible’’ if there exists a chain (*) such that each step $E_{i+1}:E_i$ is *normal* of degree 3. In each part below, you should either show the result is true by indicating how to modify the appropriate step of Exercise ‘‘19.12’’(a) to get the proof, or show that it is not true by a counterexample.

(i) Is the analog of Exercise ‘‘19.12’’(a) true for 3-constructible extensions?

(ii) Is the analog of Exercise ‘‘19.12’’(a) true for $\{2,3\}$-constructible extensions?

(iii) Is the analog of Exercise ‘‘19.12’’(a) true for strongly 3-constructible extensions?

For brevity, I won’t ask about analogs of parts (b)-(d) of that exercise.

Chapter 20

‘‘**Exercise 20.13**’’. Deduce from the result of Exercise 20.5 that every polynomial over a finite field has cyclic, hence abelian, Galois group.

‘‘**Exercise 20.14**’’. Let p be a prime and n a positive integer. Show that the irreducible factors of $t^{p^n} - t$ in $\mathbb{Z}_p[t]$ are precisely all the irreducible polynomials over $\mathbb{Z}_p$ of degrees dividing n. (Hint: Apply Exercise 20.5 to the extension of $\mathbb{Z}_p$ generated by a zero of an irreducible factor of this polynomial.)

‘‘**Exercise 20.15**’’. Recall that the *Fibonacci numbers* are the sequence of integers f_0, f_1, ... defined by the conditions $f_0 = 0$, $f_1 = 1$, $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$.

(a) For any field F, let α_F and β_F denote the zeros of the polynomial $t^2 - t - 1$ in the splitting field of that polynomial over F. Show that if F has characteristic $\neq 5$, then the equation

$$f_n = (\alpha_F^n - \beta_F^n)/(\alpha_F - \beta_F)$$

holds in F for all nonnegative integers n. What goes wrong in characteristic 5?

(b) Now let p be a prime other than 5, let $F = \mathbb{GF}(p)$, and let a_p = the order of the element β_F/α_F in the multiplicative group of nonzero elements of $\mathbb{GF}(p^2)$. Show that the positive integers n such that the nth Fibonacci number is divisible by p are precisely the multiples of a_p.

(c) Show that for all primes $p \neq 5$, a_p is a divisor of $p^2 - 1$,

(d) Show that if the polynomial $t^2 - t - 1$ splits in $\mathbb{Z}_p$, then a_p is in fact a divisor of $p-1$.

(e) Show that if the polynomial $t^2 - t - 1$ does not split in $\mathbb{Z}_p$, then a_p is a divisor of $p+1$. (Hint: Let φ be the Frobenius automorphism of $\mathbb{GF}(p^2)$. Recalling the result of Exercise 20.5, conclude that $\varphi(\alpha_F / \beta_F)$ is the multiplicative inverse of α_F / β_F. Combine this result with the definition of φ.)

(f) Is there an integer a_5 such that the values of n for which f_n is divisible by 5 are precisely the multiples of a_5? If so, what is it?

Chapter 21

‘‘**Exercise 21.13**’’. Let p, a and k positive integers, with p prime and a coprime to p, and let K be a field of characteristic different from p.

(a) Show that an element $\varepsilon \in K$ is a primitive $p^k a$th root of unity if and only if $\varepsilon^{p^{k-1}}$ is a primitive path root of unity.

(b) Show by example that for an element $\varepsilon \in K$, being a primitive $p^k a$th root of unity is not equivalent to ε^{p^k} being a primitive ath root of unity. Does an implication hold in one direction?

‘‘**Exercise 21.14**’’. On p.126 we saw the structure of the splitting field of the polynomial $t^3 - 2$ over $\mathbb{Q}$. This exercise will determine, more generally, the structure of the splitting field of a polynomial $t^p - q$ over $\mathbb{Q}$, and show that if $p > 2$, its Galois group is noncommutative. Let p and q be prime numbers (which may be equal or distinct), let α be the pth root of q in $\mathbb{R}$, and let N be the normal closure of $\mathbb{Q}(\alpha):\mathbb{Q}$ in $\mathbb{C}$.

(a) Show that $[N:\mathbb{Q}] = p(p-1)$. (Suggestion: Show that $N = \mathbb{Q}(\alpha, \zeta_p)$. Deduce that $[N:\mathbb{Q}]$ is at most $p(p-1)$, and also that it is divisible by both p and $p-1$.)

(b) Deduce from (a) that α has degree p over $\mathbb{Q}(\zeta_p)$, and that ζ_p has degree $p-1$ over $\mathbb{Q}(\alpha)$, and describe a basis for N over $\mathbb{Q}$.

(c) Deduce from (b) that for each $j \in \mathbb{Z}_p^*$, the group $\Gamma(N:\mathbb{Q})$ contains an element ρ_j which fixes α and sends ζ_p to ζ_p^j, and also that it contains an element τ which fixes ζ_p and sends α to $\zeta_p \alpha$.

(d) Show that for $j \neq 1$ in $\mathbb{Z}_p^*$, the elements ρ_j and τ of part (c) do not commute: $\rho_j \tau \neq \tau \rho_j$. Conclude that for $p \neq 2$, $\Gamma(N:\mathbb{Q})$ is non-commutative.

‘‘**Exercise 21.15**’’. (a) Suppose L is a field of characteristic not equal to 2, in which the polynomial $t^4 + 1$ splits. Show that the subgroup of the multiplicative group of L generated by the zeros of that polynomial is cyclic of order 8. If we let α be a generator of that group, which elements α^j $(0 \leq j < 8)$ are the zeros of $t^4 + 1$?

(b) Suppose K is a field of characteristic not equal to 2, in which the polynomial $t^4 + 1$ is irreducible. Determine the Galois group of $t^4 + 1$ over K precisely, writing out its multiplication table, and verify that this group is not cyclic. (In writing this table, specify the meanings of the symbols you use for the group elements. Your discussion should show why the Galois group must have this table, though you don’t have to show all arithmetic calculations. Hint: If α is one zero of the given polynomial, part (a) shows what elements a member of the Galois group can take α to.)

‘‘**Exercise 21.16**’’. Deduce from the results of Exercises ‘‘21.15’’ and 20.5 that $t^4 + 1$ is reducible over $\mathbb{Z}_p$ for every prime p. (Exercise ‘‘21.15’’ is not applicable to the case $p = 2$, but that case can be done very easily.) Deduce that this polynomial is reducible over every field of nonzero characteristic. On the other hand, show that it is irreducible over $\mathbb{Q}$.

Chapter 22

‘‘**Exercise 22.10**’’. Let f be a polynomial over a field K, which has no multiple zeros in its splitting field Σ. Prove the converse of Proposition 22.3 (p.252): If the Galois group of f is transitive on the set of zeros of f in Σ, then f is irreducible.

‘‘**Exercise 22.11**’’. (a) Show that if p is a prime, X is a set of p elements, and G a subgroup of the group of permutations of X, then G is transitive if and only if its order is divisible by p. (You may use the fact that for any element $x \in X$, if we let Gx denote $\{gx \mid g \in G\}$, and G_x denote $\{g \in G \mid gx = x\}$, then $|Gx| = [G : G_x]$.)

(b) Deduce from (a) and the result of Exercise ‘‘22.10’’ above that if f is a separable irreducible polynomial of prime degree p, Σ its splitting field, and M an intermediate field of $\Sigma : K$, then f remains irreducible over M if and only if $[M : K]$ is not divisible by p.

(c) Find another proof of the result of (b), which only requires the results of Chapters 1-6, and does not need the assumption of separability.

‘‘**Exercise 22.12**’’. This exercise gives a little practice with the concept of transitive subgroup (p.251); it involves no field theory.

Let us regard the dihedral group $\mathbb{D}_8$ as the group of symmetries of the square, and in particular as a group of permutations of the vertices of the square, which we will label successively 0, 1, 2, 3. (For instance, the transposition (02), which interchanges a pair of opposite vertices, belongs to $\mathbb{D}_8$, but the transposition (01) does not.) We shall regard $\mathbb{D}_8$ as also acting on the set of edges of the square, $\{\overline{01}, \overline{12}, \overline{23}, \overline{30}\}$. (For instance, the transposition (02) sends $\overline{01}$ to $\overline{12}$.)

You can answer parts (a) and (b) below simply by listing the required subgroups, since the verification of the properties asked for is completely straightforward. In parts (c) and (d), you should give some reasoning, but it can be quite brief if you find a concise argument.

(a) Show that $\mathbb{D}_8$ has subgroups A and B each of which is transitive on the set of vertices of the square, but such that $A \cap B$ is not transitive on that set.

(b) Show that $\mathbb{D}_8$ has a subgroup E which is transitive on the set of vertices of the square but not on the set of edges, and a subgroup F which is transitive on the set of edges but not on the set of vertices. (You saw a similar fact in ‘‘Exercise 13.15(e)’’.)

(c) Let S denote the set of all ordered pairs (v, e) such that v is a vertex of the square and e an edge. We will consider $\mathbb{D}_8$ to act on S by letting each group element α send each pair (v, e) to the pair $(\alpha(v), \alpha(e))$. Show that $\mathbb{D}_8$ is not transitive on S.

(d) Let $T \subseteq S$ denote the set of those pairs (v, e) such that v is a vertex of the edge e. Show that $\mathbb{D}_8$ is transitive on T.

Chapter 23