c) Let $y \in G$. Show that the function from G to G which sends an element $x \in G$ to the element xy is one-to-one and onto. (That is, this function is a permutation of the elements of G.)

15. Symmetric groups

One family of groups will be particularly important to us. We start with an example. Consider any three objects, for instance, the integers 1, 2, 3. There are six possible ways of permuting these three objects, which we now list, giving each permutation a name.

$$\sigma_1: \begin{array}{ccc}1&2&3\\ \downarrow&\downarrow&\downarrow\\ 1&2&3\end{array} \quad \sigma_2: \begin{array}{ccc}1&2&3\\ \downarrow&\downarrow&\downarrow\\ 2&1&3\end{array} \quad \sigma_3: \begin{array}{ccc}1&2&3\\ \downarrow&\downarrow&\downarrow\\ 3&2&1\end{array} \quad \sigma_4: \begin{array}{ccc}1&2&3\\ \downarrow&\downarrow&\downarrow\\ 1&3&2\end{array} \quad \sigma_5: \begin{array}{ccc}1&2&3\\ \downarrow&\downarrow&\downarrow\\ 2&3&1\end{array} \quad \sigma_6: \begin{array}{ccc}1&2&3\\ \downarrow&\downarrow&\downarrow\\ 3&1&2\end{array}$$

Thus, by σ_3, we mean the permutation which takes 1 to 2, 2 to 1, and 3 to 3. (We say that it leaves 3 fixed.)

An alternate way of describing these σ_i would be in functional notation. For example, σ_3 is the function from the set $\{1, 2, 3\}$ to that same set, defined by $\sigma_3(1) = 3$, $\sigma_3(2) = 2$, and $\sigma_3(3) = 1$.

We will now give the set $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ a group structure. To do so, we must define an operation on this set. We take our operation to be composition. Thus, for $a \in \{1, 2, 3\}$, we define $(\sigma_i\sigma_k)(a) = \sigma_i(\sigma_k(a))$. Here is an example.

$(\sigma_3\sigma_5)(1) = \sigma_3(\sigma_5(1)) = \sigma_3(2) = 2.$
$(\sigma_3\sigma_5)(2) = \sigma_3(\sigma_5(2)) = \sigma_3(3) = 1.$
$(\sigma_3\sigma_5)(3) = \sigma_3(\sigma_5(3)) = \sigma_3(1) = 3.$
We see that $\sigma_3\sigma_5$ sends 1 to 2, 2 to 1, and 3 to 3. This is exactly what σ_2 does, and so $\sigma_3\sigma_5 = \sigma_2$.

(15.1) Exercise: Complete the following multiplication table, and verify that it turns the set $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ into a group. Find the identity element of this group. For each element in the group, identify the inverse of that element. Show that this group is not Abelian. (Note: In this table, the product $\sigma_3\sigma_5$ is given in the intersection of the row labeled σ_3 and the column labeled σ_5.)

S_3

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2					
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4					
σ_5	σ_5					
σ_6	σ_6					

.

Of course, if we consider the permutations of the k numbers 1, 2, ..., k, we can form those permutations into a group in the analogous way. It is denoted S_k, and is called the symmetric (or permutation) group on k elements.

For $k > 3$, it is convenient to have an efficient way of describing a given permutation on the set {1, 2, ..., k}, and we now develop such a description. For sake of example, let $k = 7$, so that we will be considering S_7, the group of permutations of 1, 2, 3, 4, 5, 6, 7. Let us use the symbol (1, 7, 3), to denote the following permutation.

$$(1,\ 7,\ 3) \text{ is the permutation } \quad \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 2 & 1 & 4 & 5 & 6 & 3 \end{array}$$

Note that this permutation leaves 2, 4, 5, and 6 all fixed. It sends 1 to 7, 7 to 3, and 3 to 1. All of this information is neatly encoded in the symbol (1, 7, 3). Since 2, 4, 5, and 6 do not appear, we know that they are fixed. Since 1 is followed by 7 in this symbol, we know that 1 is sent to 7. Since 7 is followed by 3, we know that 7 is sent to 3. Now 3 is at the end of the symbol, so we cycle back to the beginning of the symbol, and find a 1. That tells us that 7 is sent to 1. We call (1, 7, 3) a cycle, or to be more specific, a 3-cycle, since it involves three objects.

The 2-cycle (4, 6) is the following permutation.

(4, 6) is the permutation $\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 6 & 5 & 4 & 7 \end{array}$.

Remarks: a) 2-cycles are usually called transpositions.

b) The identity permutation, which fixes everything, will be denoted by (1).

Now consider (1, 7, 3)(4, 6). You should have no trouble seeing that this is the permutation

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 2 & 1 & 6 & 5 & 4 & 3 \end{array}.$$

Furthermore, you can easily verify that the above permutation also equals (4, 6)(1, 7, 3). In fact, we have a lemma whose easy proof we leave to the reader.

(15.2) Lemma: If $(a_1, a_2, \dots a_m)$ and $(b_1, b_2, \dots, b_k)$ are disjoint cycles (i.e., if $\{a_1, a_2, \dots a_m\} \cap \{b_1, b_2, \dots, b_k\}$ is empty), then $(a_1, a_2, \dots a_m)(b_1, b_2, \dots, b_k) = (b_1, b_2, \dots, b_k)(a_1, a_2, \dots a_k)$.

Of course, we can work backwards. Starting with a random permutation, such as

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 6 & 4 & 7 & 1 & 2 \end{array},$$

we can write it as a product of disjoint cycles. Since 1 → 3, and 3 → 6, and 6 → 1, we get the cycle (1, 3, 6). Now 2 → 5, and 5 → 7, and 7 → 2, so we get the cycle (2, 5, 7). We then note that 4 → 4, giving the cycle (4). Thus, the above permutation is seen to equal (1, 3, 6)(2, 5, 7)(4). Since the cycle (4) really just tells us that 4 → 4, it does no harm to leave it out, and simply write (1, 3, 6)(2, 5, 7).

(15.3) Exercises: a) Write the permutation

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 7 & 6 & 1 & 2 & 3 & 5 \end{array}$$

as a product of disjoint cycles.

b) Show that (1, 7, 3, 5) = (5, 1, 7, 3) = (3, 5, 1, 7) = (7, 3, 5, 1).

c) $(1, 2)^{-1} = ?$ $(1, 2, 3)^{-1} = ?$ (In S_k, $k \geq 4$.)

d) Rewrite the table in exercise (15.1), expressing each element as a product of disjoint cycles.

e) Convince yourself that the permutation group on 4 elements, S_4, contains the following 24 permutations.

(1);
(1, 2); (1, 3); (1, 4); (2, 3); (2, 4); (3, 4);
(1, 2)(3, 4); (1, 3)(2, 4); (1, 4)(2, 3)
(1, 2, 3); (1, 3, 2); (1, 2, 4); (1, 4, 2)
(1, 3, 4); (1, 4, 3); (2, 3, 4); (2, 4, 3);
(1, 2, 3, 4); (1, 2, 4, 3); (1, 3, 2, 4);
(1, 3, 4, 2); (1, 4, 2, 3); (1, 4, 3, 2).

f) Find all the distict 5-cycles in S_5. (Avoid repetitions!)

g) Let $\sigma = (1, 2, 3)$. Find σ^2, σ^3, σ^4, and σ^5, writing each as a product of disjoint cycles. Now do the same for

$\sigma = (1, 2, 3, 4)$, and for $\sigma = (1, 2, 3, 4, 5)$.

h) Let σ be the m-cycle $(a_1, a_2, \ldots, a_m)$. What is the smallest positive power of σ which equals (1), the identity element?

i) Let σ be an m-cycle, and τ be a k-cycle. Suppose that σ and τ are disjoint. If m and k are relatively prime, then what is the smallest positive power of $\sigma\tau$ which equals (1)? Now answer that question without assuming that m and k are relatively prime.

(15.4) Exercise: Show that any permutation can be written as a product of transpositions. (Hint: Argue that it is enough to show that any cycle can be writen as a product of transpositions. Then show that $(a_1, a_2, \ldots, a_m) = (a_1, a_m)(a_1, a_{m-1}) \ldots (a_1, a_2)$.

We present a final lemma, which will be useful later.

(15.5) Lemma: Let (a, b) be a transposition in S_k, and let Θ be some permutation in S_k. Then $\Theta(a, b)\Theta^{-1} = (\Theta(a), \Theta(b))$.

Proof: Let $1 \le c \le k$. We must show that $\Theta(a, b)\Theta^{-1}$ fixes c unless c equals $\Theta(a)$ or $\Theta(b)$, and that $\Theta(a, b)\Theta^{-1}$ sends $\Theta(a)$ to $\Theta(b)$ and $\Theta(b)$ to $\Theta(a)$. Now since Θ is a permutation of the integers 1, 2, ..., k, we know that $c = \Theta(d)$ for some $1 \le d \le k$. Suppose first that d = a, so that $c = \Theta(a)$. Then $\Theta(a, b)\Theta^{-1}$ applied to c is the same as $\Theta(a, b)\Theta^{-1}$ applied to $\Theta(a)$. However,

Θ^{-1} sends $\Theta(a)$ to a, (a, b) sends a to b, and Θ sends b to $\Theta(b)$. Thus $\Theta(a, b)\Theta^{-1}$ sends c to $\Theta(b)$, as desired. Similarly, when d = b, so that c = $\Theta(b)$, we see that $\Theta(a, b)\Theta^{-1}$ sends c to $\Theta(a)$, as desired. Finally, suppose that d is neither a nor b, so that c is neither $\Theta(a)$ nor $\Theta(b)$. Then Θ^{-1} sends c = $\Theta(d)$ to d, (a, b) sends d to itself, and Θ sends d to $\Theta(d)$ = c. Thus $\Theta(a, b)\Theta^{-1}$ sends c to c, as desired.

(15.6) Exercise: Let $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_s)$ be disjoint cycles in S_k, and let $\Theta \in S_k$. What is $\Theta(a_1, \ldots, a_r)(b_1, \ldots, b_s)\Theta^{-1}$?

16. Subgroups

We will not belabor the issue. Consider the set **Q** with operation addition. This forms a group. Now **Q** has **Z** as a subset and if we take **Z** with addition, we again get a group. We say that the group (**Z**; +) is a subgroup of the group (**Q**; +), and we will write (**Z**; +) < (**Q**; +), or more simply **Z** < **Q** if it is understood that the operation we are considering is the standard addition.

Now if **E** represents the set of even integers, then (**E**; +) is clearly a subgroup of (**Z**; +), so **E** < **Z**. On the other hand, if **O** represents the set of odd integers, then (**O**; +) is not a subgroup of (**Z**; +), since **O** is not a group under the operation of addition.

We note that if G is a group, then G is always a subgroup of itself. Also, the set consisting of just the identity element of G is always a subgroup of G (called, as you might guess, the identity subgroup of G).

(16.1) Exercises: Consider the group described in Exercise (14.1)(e). Which of the following are subgroups of that group, using the same operation?

a) $\{(a, b) \mid a,b \in \mathbf{Z}$ with $a \neq 0$ and $b = 0\}$.

b) $\{(a, b) \mid a,b \in \mathbf{Z}$ with $a = 0$ and $b \neq 0\}$.

c) $\{(a, b) \mid a,b \in \mathbf{Z}$ with a and b not both zero, and with $a^2 + b^2 = 1\}$.

(16.2) Exercise: Working with the table you found in Exercise (15.1), find all of the subgroups of S_3.

(16.3) Exercise: The following multiplication table turns the set {a, b, c, d} into a group. (Trust me, or verify it yourself if you wish.) Note that {a, b} is a subgroup. Find all the other subgroups.

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(16.4) Exercise: The following table turns the set {a, b, c, d} into a group. Find all of its subgroups. (Note that the previous exercise gives a different group structure to that same set. This shows that when you are describing a group, it is not enough to name the set. You must also specify the operation.)

	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

The next result is an important piece of the puzzle we are putting together.

(16.5) Theorem: Let k be a prime integer. Suppose that H is a subgroup of S_k, that H contains a transposition, and that for any integers c and d with $1 \le c,d \le k$, H contains a permutation Θ such that $\Theta(d) = c$. Then $H = S_k$.

Proof: We first define an equivalence relation on the set of integers 1, 2, ..., k. For a and b two such integers, we will say that $a \sim b$ if $(a, b) \in H$. (Here, we allow the case that $a = b$, interpreting (a, a) to be the identity permutation.) Since the identity permutation is in H, we have $(a, a) \in H$, so that $a \sim a$. Thus, our relation is reflexive. Since $(a, b) = (b, a)$, if $a \sim b$, then $(a, b) \in H$, so $(b, a) \in H$, so $b \sim a$. Thus, our relation is symmetric. Now if $a \sim b$ and $b \sim c$, then $(a, b) \in H$ and $(b, c) \in H$. It follows that $(b, c)(a, b)(b, c) \in H$. However, $(b, c)(a, b)(b, c) = (a, c)$. Thus $(a, c) \in H$, so that $a \sim c$. This shows that our relation is transitive. We have now shown that $\sim$ is an equivalence relation.

We next show that any two equivalence classes under the relation $\sim$ have the same size. For this, let c and d both be integers between 1 and k. We must show that $\{a \mid a \sim c\}$ and $\{b \mid b \sim d\}$ have the same size. For this, we consider

$\Theta \in H$ such that $\Theta(d) = c$, the hypothesis assuring us that such a Θ exists in H. We claim that $\{\Theta(b) \mid b \sim d\} \subseteq \{a \mid a \sim c\}$. Suppose that b is in the equivalence class of d. Then $(d, b) \in H$. Thus $\Theta(d, b)\Theta^{-1} \in H$. However, by Lemma (15.5), $\Theta(d, b)\Theta^{-1} = (\Theta(d), \Theta(b)) = (c, \Theta(b))$. Thus, $\Theta(b)$ is in the equivalence class of c. This shows that $\{\Theta(b) \mid b \sim d\} \subseteq \{a \mid a \sim c\}$, as claimed. It follows that $\{a \mid a \sim c\}$ is at least as large as $\{\Theta(b) \mid b \sim d\}$, which (since Θ is one-to-one) is as large as $\{b \mid b \sim d\}$. Thus, $\{a \mid a \sim c\}$ is at least as large as $\{b \mid b \sim d\}$. However, the argument is perfectly symmetric, and so $\{b \mid b \sim d\}$ is also at least as large as $\{a \mid a \sim c\}$. This shows that $\{a \mid a \sim c\}$ and $\{b \mid b \sim d\}$ have the same size.

Suppose that there are r different equivalence classes. We just saw they all have the same size, which we will call s. Since these equivalence classes partition the set $\{1, 2, ..., k\}$, we see that $k = rs$. However, k is prime. Therefore, either $r = 1$ and $s = k$, or $r = k$ and $s = 1$. However, we also know that H contains some transposition, say (x, y). This tells us that the equivalence class of x contains both x and y, and so has size at least 2. Since all equivalence classes have the same size, namely s, we have $s \geq 2$. Thus the case $r = k$, $s = 1$ is eliminated, leaving only the case $r = 1$, $s = k$. This means there is only one equivalence class. Therefore, given any integers i and j with $1 \leq i,j \leq k$, we have $i \sim j$, so that $(i, j) \in H$. In particular, we see that H contains every transposition. By Exercise (15.4), $H = S_k$.

17. Solvable groups

Definition: The group G is solvable if there is a finite sequence of subgroups $\{1\} = G_0 < G_1 < G_2 < \dots < G_{n-1} < G_n = G$, such that for $1 \le i \le n$, and all elements x and y in G_i, $xyx^{-1}y^{-1}$ is in G_{i-1}.

Remark: Those readers familiar with group theory can see that the condition $xyx^{-1}y^{-1} \in G_{i-1}$ for all $x,y \in G_i$ is equivalent to saying that G_{i-1} is a normal subgroup of G_i, and $\frac{G_i}{G_{i-1}}$ is Abelian. The arguments below are made simplier by a knowledge of group theory. However, they can be done even without that knowledge, using rather boring calculations instead.

Example: We claim that S_3 is solvable. consider the sequence of subgroups $\{(1)\} = G_0 < G_1 < G_2 = S_3$, where $G_1 = \{(1), (1, 2, 3), (1, 3, 2)\}$ (which the reader can verify is a subgroup). We claim that this sequence satisfies the condition stated in the above definition. Thus, we must show for all x and y in G_1, that $xyx^{-1}y^{-1} \in G_0 = \{(1)\}$, and similarly for all x and y in $G_2 = S_3$, that $xyx^{-1}y^{-1} \in G_1$. First, let us pick any x and y in G_1. Since $\{(1)\}$ contains a single element, namely the identity permutation (1), to say that $xyx^{-1}y^{-1} \in \{(1)\}$ is the same as saying that $xyx^{-1}y^{-1} = (1)$, the identity. By multiplying (on the right) by yx, we see that this is the same as saying $xy = yx$. Therefore, we must first show that $xy = yx$ for all $x,y \in G_1$. That is, we must show that G_1 is Abelian. We leave it to the reader to check that this is true. We now must show for any x and y in S_3, that $xyx^{-1}y^{-1}$ is in G_1. For example, let $x = (1, 2)$ and $y = (1, 3)$. Then $x^{-1} = (1, 2)$ and $y^{-1} = (1, 3)$, so that $xyx^{-1}y^{-1} = (1, 2)(1, 3)(1, 2)(1, 3) = (1, 2, 3) \in G_1$. We leave it to the reader to check the other cases (there are 35 of them) necessary to verify that $xyx^{-1}y^{-1} \in G_1$ for all $x,y \in S_3$.

(17.1) Exercise: Complete the above verification that S_3 is solvable (or as much of it as you have patience for).

Example: We claim that S_4 is solvable. Consider the sequence of subgroups $\{(1)\} = G_0 < G_1 < G_2 < G_3 < G_4 = S_4$, where

$G_1 = \{(1), (1, 2)(3, 4)\}$,

$G_2 = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, and

$$G_3 = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3),$$
$$(1, 2, 3), (1, 3, 2), (1, 2, 4), (1, 4, 2),$$
$$(1, 3, 4), (1, 4, 3), (2, 3, 4), (2, 4, 3)\}.$$

We leave to the reader the arduous task of verifying that these are all subgroups, and that the sequence satisfies the condition needed to show that S_4 is solvable. (A knowledge of group theory makes this task much less arduous.)

(17.2) Exercise: Show that any Abelian group is solvable.

(17.3) Theorem: If $k \geq 5$, then S_k is not solvable.

Proof. Suppose to the contrary that S_k is solvable. We will derive a contradiction. We are supposing that there is a sequence of subgroups, $\{1\} = G_0 < G_1 < G_2 < \dots < G_{n-1} < G_n = S_k$, such that for $1 \leq i \leq n$, and all elements x and y in G_i, $xyx^{-1}y^{-1}$ is in G_{i-1}. Since $G_n = S_k$, every 3-cycle is in G_n. Since $G_0 = \{(1)\}$, no 3-cycles are in G_0. Therefore, we may suppose that i is the smallest index such that all 3-cycles are in G_i. Thus, G_{i-1} does not contain every 3-cycle. We will now show every 3-cycle is in G_{i-1} (a contradiction).

Let (a, b, c) represent any 3-cycle. Since $n \geq 5$, the set being permuted has at least five elements in it. In particular, besides a, b, and c, it contains at least two more elements, say d and e. Since G_i contains all 3-cycles, G_i contains $x = (a, b, e)$ and $y = (c, d, a)$. By assumption, $xyx^{-1}y^{-1} \in G_{i-1}$. However, $xyx^{-1}y^{-1} = (a, b, c)$ (verify!). Since (a, b, c) represents an arbitrary 3-cycle, we see that every 3-cycle is in G_{i-1}, giving our desired contradiction.

18. Galois Groups

We have already introduced the family of groups S_k, and told you that they will be important to us. We will now introduce the second family of groups which will be important to us in this work.

Let $F \subseteq K$ be fields. We wish to consider the set of all F-automorphisms of K, and make that set into a group. To do this, we must define an operation between two F-automormphisms of K. Let us use composition as our operation. Thus, if Θ and Φ are F-automorphisms of K, we define $\Theta\Phi$ to mean the composition of Θ with Φ, so that for any $\alpha \in K$, $(\Theta\Phi)(\alpha) = \Theta(\Phi(\alpha))$. We call the set of all F-automorphisms of K together with the operation of composition the Galois group of K over F, and denote this group by G(K/F). Of course, we must still show that it is indeed a group. We leave the argument that G(K/F) is closed under composition to the exercise below. Of course composition of functions is always associative, and it is obvious that the identity automorphism I, is the identity element of G(K/F). The existence of inverses follows from Exercise (10.4).

(18.1) Exercise: Complete the proof that G(K/F) is a group by showing that if Θ and Φ are F-automorphisms of K, then so is $\Theta\Phi$. (This shows that G(K/F) is closed under the operation.)

Definition. Let $F \subseteq K$ be fields. Then $G(K/F)$ is called the Galois group of K over F.

(18.2) Exercise: Let $F \subseteq K \subseteq L$ be fields. Show that $G(L/K)$ is a subgroup of $G(L/F)$.

Example: We will show that there are only two automorphisms in $G(\mathbf{Q}[i]/\mathbf{Q})$, the identity automorphism (which sends i to i), and another automorphism (which sends i to $-i$). First note that if Θ is a $\mathbf{Q}$-automorphism of $\mathbf{Q}[i]$, then since i is a root of $X^2 + 1$, Theorem (10.10) tells us that $\Theta(i)$ is also a root of $X^2 + 1$. Thus either $\Theta(i) = i$ or $\Theta(i) = -i$. Now since i and $-i$ are roots of $X^2 + 1$ which is irreducible in $\mathbf{Q}[X]$, Theorem (10.6) tells us that there is a unique $\mathbf{Q}$-isomorphism from $\mathbf{Q}[i]$ to $\mathbf{Q}[i]$ carrying i to i. (Obviously, it is the identity automorphism I of $\mathbf{Q}[i]$.) Therefore only one automorphism in $G(\mathbf{Q}[i]/\mathbf{Q})$ (namely, the identity) sends i to i. Now let us consider those $\Theta \in G(\mathbf{Q}[i]/\mathbf{Q})$ (if any) which send i to $-i$. Since i and $-i$ are both roots of $X^2 + 1$, Theorem (10.6) tells us that there is a unique $\mathbf{Q}$-isomorphism from $\mathbf{Q}[i]$ to $\mathbf{Q}[-i]$, which sends i to $-i$. However, Clearly $\mathbf{Q}[-i] = \mathbf{Q}[i]$, and so this isomorphism is in fact a $\mathbf{Q}$-automorphism of $\mathbf{Q}[i]$. Its uniqueness shows that it is the only $\mathbf{Q}$-automorphism of $\mathbf{Q}[i]$ sending i to $-i$.

In summary, we see that $G(\mathbf{Q}[i]/\mathbf{Q})$ contains two automorphisms. If $a + bi$ represents an arbitrary element in $\mathbf{Q}[i]$ (with a and b in $\mathbf{Q}$), then one of those automorphisms is the identity I, for which $I(a + bi) = a + bi$. The other automorphism in $G(\mathbf{Q}[i]/\mathbf{Q})$ (let us call it Θ) is such that $\Theta(a + bi) = \Theta(a) + \Theta(b)\Theta(i) = a + b(-i) = a - bi$. Note that Θ is really just conjugation restricted to $\mathbf{Q}[i]$.

(18.3) Exercise: Show that the Galois group $G(\mathbf{Q}[\sqrt[3]{2}]/\mathbf{Q})$ only contains the identity automorphism. (Use what you know about the three roots of $X^3 - 2$.)

(18.4) Exercise: Let $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Show that $G(\mathbf{Q}[\omega]/\mathbf{Q})$ contains exactly two automorphisms, the identity I, (which carries ω to ω) and another automorphism (which carries ω to $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$). Also show that $\mathbf{Q}[\omega]$ is the splitting field of $X^2 + X + 1$ over $\mathbf{Q}$. (Hint: It will be helpful to note that $X^2 + X + 1 = (X - \omega)(X - \beta)$, with $\beta = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, and $\mathbf{Q}[\omega] = \mathbf{Q}[\beta]$.)

Remark: In an earlier example, we dealt with $\mathbf{Q}[i]$, which is the splitting field of $X^2 + 1$ over $\mathbf{Q}$. In Exercise (18.4), you deal with $\mathbf{Q}[-\frac{1}{2} + \frac{\sqrt{3}}{2}i]$, which is the splitting field of $X^2 + X + 1$ over $\mathbf{Q}$. In general, when you wish to determine what automorphisms are in $G(K/F)$, the task is often easier if K is the splitting field of some polynomial over F, i.e., if K/F is Galois. We shall prove some powerful theorems about that case. We present the most important of them right now. It shows that when K is the splitting field of some polynomial f(X) over F, then the group G(K/F) is related to the group S_k, where k is the number of roots of f(X). In other words, we next show that the two families of groups we have introduced, are connected to each other.

(18.5) Theorem: Let $f(X) \in F[X]$, and let K be the splitting field of f(X) over F. Suppose that $\alpha_1, \ldots, \alpha_k$ are all of the (distinct) roots of f(X). Then the group G(K/F) can be thought of as a subgroup of S_k in a natural way.

Proof: Let $\Theta \in G(K/F)$. By Corollary (10.11), we know that the list $\Theta(\alpha_1), \ldots, \Theta(\alpha_k)$ is just a permutation of the list $\alpha_1, \ldots, \alpha_k$. Therefore, we can think of Θ as giving a permutation of the k elements $\alpha_1, \ldots, \alpha_k$. (In fact, ignoring the α's and just looking at the subscripts, we in fact can think of Θ as giving a permutation of 1, 2, ..., k.) Therefore, we will identify the automorphism Θ in G(K/F) with the following permutation in S_k.

$$\begin{array}{cccc} \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \downarrow & \downarrow & & \downarrow \\ \Theta(\alpha_1) & \Theta(\alpha_2) & & \Theta(\alpha_k) \end{array}$$

Let us call this permutation $\Theta^{\#}$. There is a subtle point to discuss. Suppose that Θ and Φ are two automorphisms in

$G(K/F)$. Might it happen that $\Theta \neq \Phi$, but $\Theta^{\#} = \Phi^{\#}$? The answer is no. If $\Theta^{\#} = \Phi^{\#}$, then we would have $\Theta(\alpha_i) = \Phi(\alpha_i)$ for $1 \leq i \leq k$. Since every element in K can be written as $g(\alpha_1, \ldots, \alpha_k)$, where $g(X_1, \ldots, X_k)$ is a polynomial with coefficients in F, and since both Θ and Φ fix elements in F, we see that $\Theta(g(\alpha_1, \ldots, \alpha_k)) = \Phi(g(\alpha_1, \ldots, \alpha_k))$. Therefore $\Theta = \Phi$. Finally, we easily see that $(\Theta\Phi)^{\#} = \Theta^{\#}\Phi^{\#}$. Therefore, identifying each Θ with the corresponding $\Theta^{\#}$, allows us to think of $G(K/F)$ as a subgroup of S_k.

Example: Let K be the splitting field of $X^2 + 1$ over $\mathbf{Q}$ (so that $K = \mathbf{Q}[i]$). Let $\alpha_1 = i$ and $\alpha_2 = -i$ be the two roots of $X^2 + 1$. In an earlier example, we saw that $G(K/\mathbf{Q})$ consisted of just two automorphisms, the identity auotmorphism, I, and another automorphism we called Θ. Now $I(\alpha_1) = \alpha_1$ and $I(\alpha_2) = \alpha_2$, while $\Theta(\alpha_1) = \alpha_2$ and $\Theta(\alpha_2) = \alpha_1$. Thus, with notation as in the preceding proof, $I^{\#}$ and $\Theta^{\#}$ are the permutations

$$I^{\#}: \begin{array}{cc} \alpha_1 & \alpha_2 \\ \downarrow & \downarrow \\ \alpha_1 & \alpha_1 \end{array} \qquad\qquad \Theta^{\#}: \begin{array}{cc} \alpha_1 & \alpha_2 \\ \downarrow & \downarrow \\ \alpha_2 & \alpha_1 \end{array}.$$

Surpressing the α's and only looking at the subscripts, we get

$$I^{\#} \quad \begin{array}{cc} 1 & 2 \\ \downarrow & \downarrow \\ 1 & 2 \end{array} \qquad\qquad \Theta^{\#} \quad \begin{array}{cc} 1 & 2 \\ \downarrow & \downarrow \\ 2 & 1 \end{array}.$$

Written as cycles, $I^\# = (1)$, and $\Theta^\# = (1, 2)$. We see that under this identification, $G(K/\mathbf{Q})$ identifies with all of S_2, since S_2 only contains the two permutations (1) and $(1, 2)$.

Let F be a field with $F \subseteq \mathbf{R}$, and let $f(X) \in F[X]$. Suppose that α is a root of $f(X)$. By Theorem (10.10) (with $K = L = \mathbf{C}$), we see that the complex conjugate $\overline{\alpha}$ is also a root of $f(X)$. Of course, if α is real, then $\overline{\alpha} = \alpha$, while if α is not real, then $\overline{\alpha} \neq \alpha$. Thus, the nonreal roots of $f(X)$ come in pairs. We use this in the statement of the next result.

(18.6) Lemma: Let F be a field with $F \subseteq \mathbf{R}$, and let $f(X) \in F[X]$. Let K be the splitting field of $f(X)$ over F. Let Θ be the restriction of complex conjugation to K. Then $\Theta \in G(K/F)$. Furthermore, suppose that the (distinct) roots of $f(X)$ are $\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_{r+1}, \cdots \alpha_k$. Suppose also that these are ordered so that $\alpha_1, \ldots, \alpha_r$ are nonreal, while $\alpha_{r+1}, \ldots, \alpha_k$ be real. Also, (using the preceding paragraph, which shows that r must be even), let $\alpha_2 = \overline{\alpha_1} = \Theta(\alpha_1)$, $\alpha_4 = \overline{\alpha_3} = \Theta(\alpha_3)$, ..., $\alpha_r = \overline{\alpha_{r-1}} = \Theta(\alpha_{r-1})$. Then under the identification of $G(K/F)$ with a subgroup of S_k, the automorphism Θ identifies with the permutation $(1, 2)(3, 4) \ldots (r-1, r)$.

Remark: If all the roots of $f(X)$ are real, then $r = 0$. In this case, we will interprete the above theorem to say that Θ identifies with the permutation (1). This is consistent, since if $r = 0$, then $K \subseteq \mathbf{R}$, so that conjugation restricted to K is just the identity automorphism, i.e., $\Theta = I$, and I does identitfy with (1).

Proof: We have $K = F[\alpha_1, ... \alpha_k]$. Since $F \subseteq \mathbf{R}$, conjugation fixes everything in F. Thus, $\Theta|F$ is the identity. Therefore, $\Theta(K) = F[\Theta({}_1), ..., \Theta(\alpha_k)]$. However, Corollary (10.11) shows that $\Theta(\alpha_1), ..., \Theta(\alpha_k)$ is just a permutation of $\alpha_1, ..., \alpha_k$, and so $\Theta(K) = F[\alpha_1, ..., \alpha_k] = K$. This shows that $\Theta \in G(K/F)$. Next, (using the notation of the proof of Theorem (18.5)) we note that

$$\begin{array}{ccccccccccc}
 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \;\cdots & \alpha_{r-1} & \alpha_r & \alpha_{r+1} \;\cdots & \alpha_k \\
\Theta^{\#}: & \downarrow^{-} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & \Theta(\alpha_1) & \Theta(\alpha_2) & \Theta(\alpha_3) & \Theta(\alpha_4) & ...\Theta(\alpha_{r-1}) & \Theta(\alpha_r) & \Theta(\alpha_{r+1}) & ...\Theta(\alpha_k)
\end{array}$$

For $r + 1 \leq i \leq k$, α_i is real, and so $\Theta(\alpha_i) = \alpha_i$. For $1 \leq i \leq r$, the value of $\Theta(\alpha_i)$ is given in the statement in the theorem. Thus

$$\begin{array}{ccccccccccc}
 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \;\cdots & \alpha_{r-1} & \alpha_r & \alpha_{r+1} \;\cdots & \alpha_k \\
\Theta^{\#}: & \downarrow^{-} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 \;\cdots & \alpha_r & \alpha_{r-1} & \alpha_{r+1} \;\cdots & \alpha_k
\end{array}$$

Just considering subscripts, this becomes

$$\begin{array}{ccccccccc}
 & 1 & 2 & 3 & 4 & r-1 & r & r+1 & k \\
\Theta^{\#}: & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
 & 2 & 1 & 4 & 3 & r & r-1 & r+1 & k
\end{array}$$

Written in terms of cycles, we get $\Theta^{\#} = (1, 2)(3, 4) \ldots (r-1, r)$.

Let $f(X) \in F[X]$ and let K be the splitting field of $f(X)$ over F. If $f(X)$ has k distinct roots, then Theorem (18.5) tells us that we may think of $G(K/F)$ as a subgroup of S_k. Since the size $|S_k|$ of the group S_k is k!, we have an upper bound to how large $G(K/F)$ can be. (Those readers who know Lagrange's Theorem from group theory will see that we can in fact say that the size of $G(K/F)$ divides the size of S_k.) If $f(X)$ is irreducible, we can get more information about the size of $G(K/F)$.

(18.7) Theorem: Let $f(X) \in F[X]$ be irreducible with degree k, and let K be the splitting field of $f(X)$ over F. Then the size $|G(K/F)|$ of the group $G(K/F)$ is a multiple of k.

Proof: Suppose that $\alpha_1, \ldots, \alpha_k$ are all of the roots of $f(X)$. Since $f(X)$ is irreducible, by Theorem (7.10) we know that these roots are all distinct. Fix any one root α of $f(X)$. If $\Theta \in G(K/F)$, then we know that $\Theta(\alpha)$ is also a root of $f(X)$, so that $\Theta(\alpha) = \alpha_i$ for some $i = 1, 2, \ldots, k$. We will now partition $G(K/F)$ into k subsets. For each $1 \leq i \leq k$, let $W_i = \{\Theta \in G(K/F) \mid \Theta(\alpha) = \alpha_i\}$. Note that each $\Theta \in G(K/F)$ is in exactly one W_i, $1 \leq i \leq k$. (Here, we are using that $\alpha_1, \alpha_2, \ldots, \alpha_k$ are all distinct.) Thus

$G(K/F) = W_1 \cup W_2 \cup \dots \cup W_k$ is a partition of $G(K/F)$. If we can show that all of these sets W_i have the same size, say size m, then we will have that $|G(K/F)| = km$. Thus, we must only show that all the W_i have the same size. Consider W_r and W_s for arbitrary integers r and s between 1 and k. We will show that $|W_r| = |W_s|$. This will suffice to prove the result. Actually, it will suffice to prove that $|W_r| \leq |W_s|$, since then by symmetry we will also have $|W_s| \leq |W_r|$. These two inequalities together will show that $|W_r| = |W_s|$, as desired.

We now show that $|W_r| \leq |W_s|$. Since α_r and α_s are both roots of the irreducible polynomial $f(X) \in F[X]$, Corollary (12.3) tells us that there is a $\Phi \in G(K/F)$ with $\Phi(\alpha_r) = \alpha_s$. Now suppose that $W_r = \{\Theta_1, \Theta_2, \dots, \Theta_t\}$ (so that $|W_r| = t$). Consider the set $\{\Phi\Theta_1, \Phi\Theta_2, \dots, \Phi\Theta_t\}$. This set contains t distinct objects (since if $\Phi\Theta_u = \Phi\Theta_v$, the multiplying on the left by Φ^{-1} would show that $\Theta_u = \Theta_v$). We will show that $\{\Phi\Theta_1, \Phi\Theta_2, \dots, \Phi\Theta_t\} \subseteq W_s$. This will show that $|W_r| = t \leq |W_s|$, and complete the proof. Pick any $\Phi\Theta_u$, with $1 \leq u \leq t$. Since $\Theta_u \in W_r$, we know (by definition of W_r) that $\Theta_u(\alpha) = \alpha_r$. Thus $\Phi\Theta_u(\alpha) = \Phi(\Theta_u(\alpha)) = \Phi_u(\alpha_r) = \alpha_s$. Since $\Phi\Theta_u(\alpha) = \alpha_s$, the definition of Ws tells us that $\Phi\Theta_u \in W_s$. This completes the proof.

Example. Let K be the splitting field of $X^3 - 2$ over **Q**. We will determine what $G(K/\mathbf{Q})$ is. We know that the roots of $X^3 - 2$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$, and $\sqrt[3]{2}\,\omega^2$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$.

By Theorem (18.5), G(K/**Q**) can be thought of as a subgroup of S_3, and by Theorem (18.7) we know that 3 divides $|G(K/\mathbf{Q})|$. Now S_3 has only two subgroups whose sizes are divisible by three, namely {(1), (1, 2, 3), (1, 3, 2)} and S_3 itself. However, since $\sqrt[3]{2}$ is real, while $\sqrt[3]{2}\ \omega$ and its complex conjugate $\sqrt[3]{2}\ \omega^2$ are not real, by Lemma (18.6), (2, 3) $\in$ G(K/**Q**). Thus G(K/**Q**) = S_3.

(18.8) Exercises: With notation as in the previous example, note that $\omega = \dfrac{\sqrt[3]{2}\,\omega}{\sqrt[3]{2}} \in K$. Suppose that $\Theta \in G(K/\mathbf{Q})$.

a) Show that $\Theta(\sqrt[3]{2})$ is either $\sqrt[3]{2}$, or $\sqrt[3]{2}\omega$, or $\sqrt[3]{2}\omega^2$.

b) Show that $\Theta(\omega)$ is either ω or ω^2. (Hint: ω and ω^2 are the roots of $X^2 + X + 1$.)

Subtle question: Is there a $\Theta \in G(K/\mathbf{Q})$ such that (for example) $\Theta(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, and $\Theta(\omega) = \omega^2$? How about any other choices of one possibility from part (a) and one possibility from part (b)? In part (d), we answer this question. For now, try to understand why it is a significant question.

c) Suppose you know what $\Theta(\sqrt[3]{2})$ is, and what $\Theta(\omega)$ is. Show that these two values determine what each of $\Theta(\sqrt[3]{2})$, $\Theta(\sqrt[3]{2}\omega)$, and $\Theta(\sqrt[3]{2}\omega^2)$ are, and so determine what Θ is.

d) Let α be any one of $\sqrt[3]{2}$, or $\sqrt[3]{2}\omega$, or $\sqrt[3]{2}\omega^2$, and let β be either of ω or ω^2. Show that there is a $\Theta \in G(K/\mathbf{Q})$ with $\Theta(\sqrt[3]{2}) = \alpha$ and $\Theta(\omega) = \beta$. (Hint: By the previous example, we know that $G(K/\mathbf{Q}) = S_3$, and so $G(K/\mathbf{Q})$ contains 6 elements. Also note that part (a) allows 3 choices, and part (b) allows 2 choices.)

Example: We continue with the notation of the preceeding example and exercise. By part (d) of the last exercise, there is a $\Theta \in G(K/Q)$ such that $\Theta(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, and $\Theta(\omega) = \omega^2$. We can see that $\Theta(\sqrt[3]{2}\omega) = \Theta(\sqrt[3]{2})\Theta(\omega) = (\sqrt[3]{2}\omega)(\omega^2) = \sqrt[3]{2}\omega^3 = \sqrt[3]{2}$. Also, $\Theta(\sqrt[3]{2}\omega^2) = \Theta(\sqrt[3]{2})(\Theta(\omega))^2 = (\sqrt[3]{2}\omega)(\omega^2)^2 = \sqrt[3]{2}\omega^5 = \sqrt[3]{2}\omega^2$. Thus, if $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\omega$, and $\alpha_3 = \sqrt[3]{2}\omega^2$, then we have $\Theta(\alpha_1) = \alpha_2$, $\Theta(\alpha_2) = \alpha_1$, and $\Theta(\alpha_3) = \alpha_3$. Thus when we think of Θ as being a permutation in S_3, it is the permutation which sends 1 to 2, and 2 to 1, and leaves 3 fixed. That is, it is the permutation (1, 2).

(18.9) Exercises: a) For each of the other 5 possible Θ's given by Exercise (18.8)(d), find out what permutation in S_3 Θ corresponds to. (We did one case in the above example.)

Example: We continue the above notation. We saw above that the element $\Theta \in G(K/\mathbf{Q})$ defined by saying $\Theta(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, and $\Theta(\omega) = \omega^2$, identifies with the permutation (1, 2) in S_3. Now $G(K/\mathbf{Q}[\omega])$ is a subgroup of $G(K/\mathbf{Q})$, and so $G(K/\mathbf{Q}[\omega])$ identifies with a subgroup of S_3. Let us call that subgroup H.

Question: is (1, 2) in H? Answer: No. Since (1, 2) identifies with Θ, and since $\Theta(\omega) = \omega^2$, Θ does not fix ω, and so $\Theta \notin G(K/\mathbf{Q}[\omega])$. Therefore, $(1, 2) \notin H$.

(18.10) Exercises: Determine the subgroup of S_3 which identifies with each of the following subgroups of $G(K/\mathbf{Q})$.

a) $G(K/\mathbf{Q}[\omega])$ b) $G(K/\mathbf{Q}[\sqrt[3]{2}])$ c) $G(K/\mathbf{Q}[\sqrt[3]{2}\omega])$ d) $G(K/\mathbf{Q}[\sqrt[3]{2}\omega^2])$.