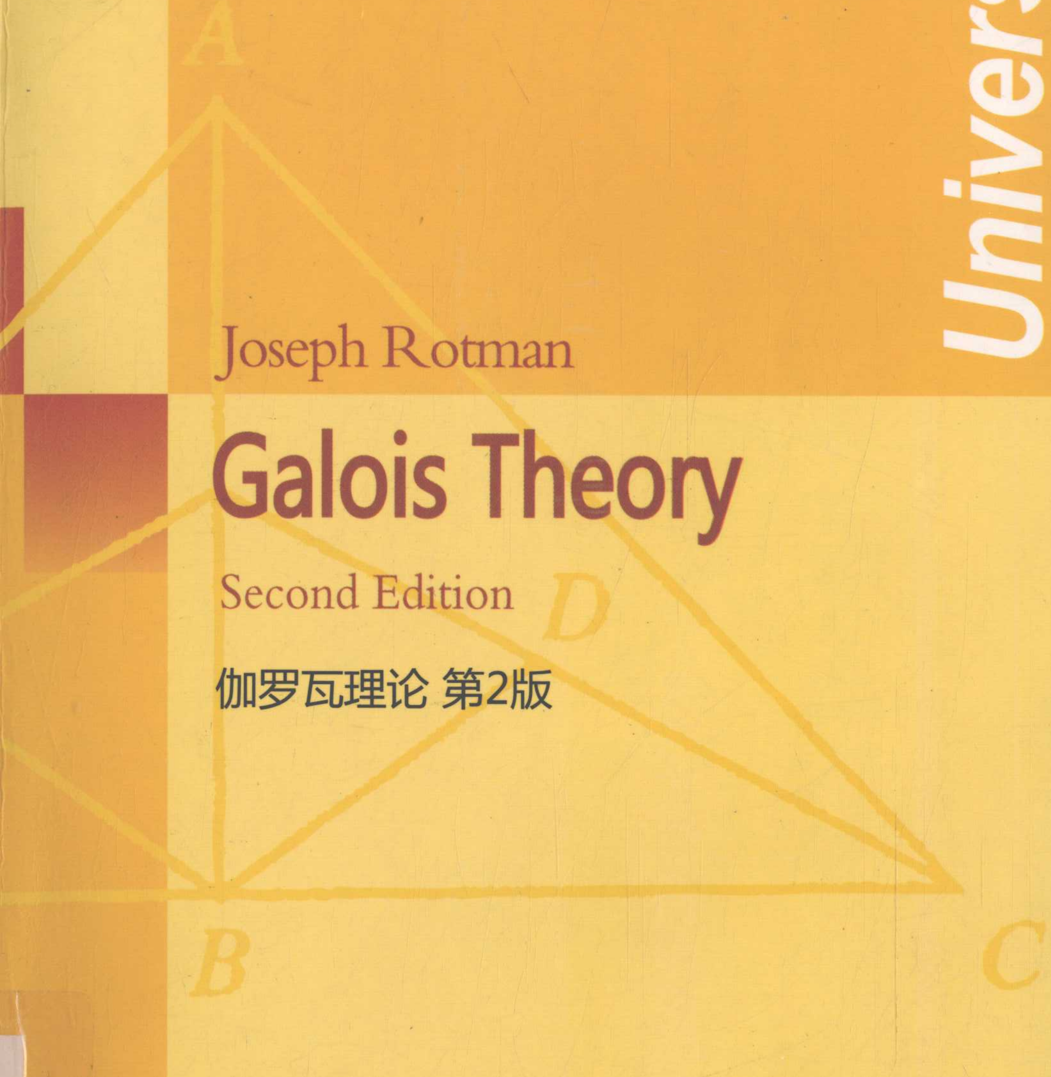
Universitext

Joseph Rotman

Galois Theory

Second Edition

伽罗瓦理论 第2版



Springer

世界图书出版公司
www.wpcbj.com.cn

Joseph Rotman

Galois Theory

Second Edition

Springer

图书在版编目（CIP）数据

伽罗瓦理论：第2版 = Galois Theory 2nd ed.：英文/（美）罗特曼（Rotman，J.）著. —影印本. —北京：世界图书出版公司北京公司，2010.2
ISBN 978-7-5100-0508-4

Ⅰ. ①伽… Ⅱ. ①罗… Ⅲ. ①伽罗瓦理论—英文
Ⅳ. ①O153.4

中国版本图书馆 CIP 数据核字（2010）第010705号

书　　名：	Galois Theory 2nd ed.
作　　者：	Joseph Rotman
中 译 名：	伽罗瓦理论 第2版
责任编辑：	高蓉　刘慧
出 版 者：	世界图书出版公司北京公司
印 刷 者：	三河国英印务有限公司
发　　行：	世界图书出版公司北京公司（北京朝内大街137号　100010）
联系电话：	010-64021602，010-64015659
电子信箱：	kjb@wpcbj.com.cn
开　　本：	24开
印　　张：	7.5
版　　次：	2010年01月
版权登记：	图字：01-2009-1084
书　　号：	978-7-5100-0508-4/O·724　　定　　价：25.00元

Joseph Rotman
Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801
USA
rotman@math.uiuc.edu

Mathematics Subject Classification (2000): 12-01, 12F10

With 9 Figures.

Library of Congress Cataloging-in-Publication Data
Rotman, Joseph J., 1934-
Galois theory / Joseph Rotman. — 2nd ed.
p. cm. — (Universitext)
Includes bibliographical references (p. –) and index.
ISBN 0-387-98541-7 (softcover : alk. paper)
1. Galois theory. I. Title.
QA214.R685 1998
512′.3—dc21 98-3967

9 8 7 6 5 4 3 2 (Corrected second printing)

ISBN 0-387-98541-7

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

Preface to the Second Edition

There are too many errors in the first edition, and so a "corrected nth printing" would have been appropriate. However, given the opportunity to make changes, I felt that a second edition would give me the flexibility to change any portion of the text that I felt I could improve. The first edition aimed to give a geodesic path to the Fundamental Theorem of Galois Theory, and I still think its brevity is valuable. Alas, the book is now a bit longer, but I feel that the changes are worthwhile. I began by rewriting almost all the text, trying to make proofs clearer, and often giving more details than before. Since many students find the road to the Fundamental Theorem an intricate one, the book now begins with a short section on symmetry groups of polygons in the plane; an analogy of polygons and their symmetry groups with polynomials and their Galois groups can serve as a guide by helping readers organize the various definitions and constructions. The exposition has been reorganized so that the discussion of solvability by radicals now appears later; this makes the proof of the Abel-Ruffini theorem easier to digest. I have also included several theorems not in the first edition. For example, the *Casus Irreducibilis* is now proved, in keeping with a historical interest lurking in these pages.

I am indebted to Gareth Jones at the University of Southampton who, after having taught a course with the first edition as text, sent me a detailed list of errata along with perspicacious comments and suggestions. I also thank Evan Houston, Adam Lewenberg, and Jack Shamash who made valuable comments as well. This new edition owes much to the generosity of these readers, and I am grateful to them.

Joseph Rotman
Urbana, Illinois, 1998

I thank everyone, especially Abe Seika and Bao Luong, who apprised me of errors in the first printing. I have corrected all mistakes that have been found.

Joseph Rotman
Urbana, Illinois, 2001

Preface to the First Edition

This little book is designed to teach the basic results of Galois theory—fundamental theorem; insolvability of the quintic; characterization of polynomials solvable by radicals; applications; Galois groups of polynomials of low degree—efficiently and lucidly. It is assumed that the reader has had introductory courses in linear algebra (the idea of the dimension of a vector space over an arbitrary field of scalars should be familiar) and "abstract algebra" (that is, a first course which mentions rings, groups, and homomorphisms). In spite of this, a discussion of commutative rings, starting from the definition, begins the text. This account is written in the spirit of a review of things past, and so, even though it is complete, it may be too rapid for one who has not seen any of it before. The high number of exercises accompanying this material permits a quicker exposition of it. When I teach this course, I usually begin with a leisurely account of group theory, also from the definition, which includes some theorems and examples that are not needed for this text. Here I have decided to relegate needed results of group theory to appendices: a glossary of terms; proofs of theorems. I have chosen this organization of the text to emphasize the fact that polynomials and fields are the natural setting, and that groups are called in to help.

A thorough discussion of field theory would have delayed the journey to Galois's Great Theorem. Therefore, some important topics receive only a passing nod (separability, cyclotomic polynomials, norms, infinite extensions, symmetric functions) and some are snubbed altogether (algebraic closure, transcendence degree, resultants, traces, normal bases, Kummer theory). My belief is that these subjects should be pursued only after the reader has digested the basics.

My favorite expositions of Galois theory are those of E. Artin, Kaplansky, and van der Waerden, and I owe much to them. For the appendix on "old-fashioned Galois theory," I relied on recent accounts, especially [Edwards], [Gaal], [Tignol], and [van der Waerden, 1985], and older books, especially [Dehn] (and [Burnside and Panton], [Dickson], and [Netto]). I thank my colleagues at the University of Illinois, Urbana, who, over the years, have clarified obscurities; I also thank Peter Braunfeld for suggestions that improved Appendix C and Peter M. Neumann for his learned comments on Appendix D.

I hope that this monograph will make both the learning and the teaching of Galois theory enjoyable, and that others will be as taken by its beauty as I am.

Joseph Rotman
Urbana, Illinois, 1990

To the Reader

Regard the exercises as part of the text; read their statements and do attempt to solve them all. A result labeled Theorem 1 is the first theorem in the text; Theorem G1 is the first theorem in the appendix on group theory; Theorem R1 is the first theorem in the appendix on ruler-compass constructions; Theorem H1 is the first theorem in the appendix on history.

Contents

Galois Theory

Galois theory is the interplay between polynomials, fields, and groups. The quadratic formula giving the roots of a quadratic polynomial was essentially known by the Babylonians. By the middle of the sixteenth century, the cubic and quartic formulas were known. Almost three hundred years later, Abel (1824) proved, using ideas of Lagrange and Cauchy, that there is no analogous formula (involving only algebraic operations on the coefficients of the polynomial) giving the roots of a quintic polynomial (actually Ruffini (1799) outlined a proof of the same result, but his proof had gaps and it was not accepted by his contemporaries). In 1829, Abel gave a sufficient condition that a polynomial (of any degree) have such a formula for its roots (this theorem is the reason that, nowadays, commutative groups are called abelian). Shortly thereafter, Galois (1831) invented groups, associated a group to each polynomial, and used properties of this group to give, for any polynomial, a necessary and sufficient condition that there be a formula of the desired kind for its roots, thereby completely settling the problem. We prove these theorems here.

Symmetry

Although Galois invented groups because he needed them to describe the behavior of polynomials, we realize today that groups are the precise way to describe symmetry. The Greek roots of the word *symmetry* mean, roughly, measuring at the same time. In ordinary parlance, there are at least two meanings of the word, both involving an arrangement of parts somehow balanced with respect to the whole and to each other. One of these meanings attributes an aesthetic quality to the arrangement, implying that symmetry is harmonious and well-proportioned. This usage is common in many discussions of art, and one sees it in some mathematics books as well (e.g., Weyl's *Symmetry*). Here, however, we focus on arrangements without considering, for example, whether a square is more pleasing to the eye than a rectangle.

Before giving a formal definition of symmetry, we first consider mirror images.

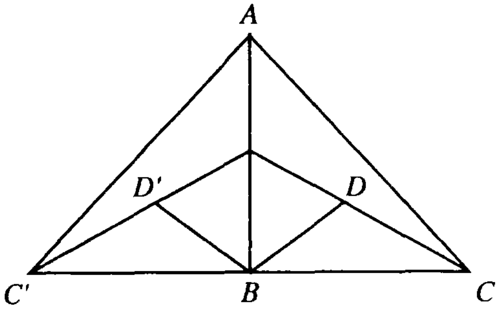


Figure 1

Let F denote the figure pictured in Figure 1. If one regards the line AB as a mirror, then the left half of F is the reflection of the right half. This figure is an example of ***bilateral symmetry***: each point P on one side of AB corresponds to a point P' (its mirror image) on the other side of AB; for example, C' corresponds to C and D' corresponds to D. We can describe this symmetry in another way. Regard the plane $\mathbb{R}^2$ as a flat transparent surface in space, having F (without the letters) drawn on it. Imagine turning over this surface by flipping it around the axis AB. If one's eyes were closed before the flip and then reopened after it, one could not know, merely by looking at F in its new position, whether the flip had occurred. Indeed, if F lies in the plane so that AB lies on the y-axis and CC' lies on the x-axis, then the linear transformation $r : \mathbb{R}^2 \to \mathbb{R}^2$, defined by $(x, y) \mapsto (-x, y)$ and called a *reflection*, carries the figure into itself; that is,

$$r(F) = F.$$

On the other hand, if T is some scalene triangle in the plane (say, with its center at the origin), then it is easy to see that there are points P in T whose mirror images $P' = r(P)$ do not lie in T; that is, $r(T) \neq T$.

Another type of symmetry is *rotational symmetry*. Picture an equilateral triangle Δ in the plane with its center at the origin. A (counterclockwise) rotation ρ by 120° carries Δ into itself; if one's eyes were closed before ρ takes place and then reopened, one could not detect that a motion had occurred.

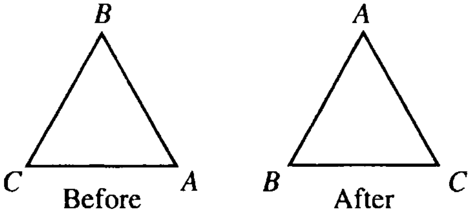


Figure 2

If we identify the plane with the complex numbers $\mathbb{C}$, then the rotation $\rho : \mathbb{C} \to \mathbb{C}$ can be described by $\rho : re^{i\theta} \mapsto re^{i(\theta+2\pi/3)}$, and

$$\rho(\Delta) = \Delta.$$

Definition. A linear transformation $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ is called ***orthogonal*** if it is distance preserving; that is, if $|U - V|$ denotes the distance between points U and V, then

$$|\sigma(U) - \sigma(V)| = |U - V|.$$

There are distance preserving functions that are not linear transformations; for example, a ***translation*** is defined by $(x, y) \mapsto (x + a, y + b)$ for fixed numbers a and b; geometrically, this translation sends any vector (x, y) into $(x, y) + (a, b)$. (It is a theorem that every distance preserving function is a composite of reflections, rotations, and translations and, if it fixes the origin, then it is a composite of reflections and rotations alone.)

It can be shown that every orthogonal transformation σ is a bijection,[1] so that its inverse function σ^{-1} exists; moreover, one can prove that σ^{-1} is also orthogonal. The set $O(2, \mathbb{R})$ of all orthogonal transformations is a group under composition, called the *real orthogonal group.*

[1] A function $f : X \to Y$ is an ***injection*** (one also says that f is *one-to-one*) if distinct points have distinct images; that is, if $x \neq x'$, then $f(x) \neq f(x')$; the contrapositive, $f(x) = f(x')$ implies $x = x'$, is often the more useful statement. A function f is a ***surjection*** (one also says f is *onto*) if, for each $y \in Y$, there exists $x \in X$ with $f(x) = y$. A function f is a ***bijection*** (one also says f is a *one-to-one correspondence*) if it is both an injection and a surjection. Finally, a function $f : X \to Y$ is a bijection if and only if it has an ***inverse***; that is, there is a function $g : Y \to X$ with both composites gf and fg identity functions.

Lemma 1. *Every orthogonal transformation σ preserves angles: if A, V and B are points, then $\angle AVB = \angle A'V'B'$, where $A' = \sigma(A)$, $V' = \sigma(V)$, and $B' = \sigma(B)$.*

Proof. We begin by proving the special case when V is the origin O. First, identify a point X with the vector starting at O and ending at X. Recall the formula relating lengths and dot product: $|X|^2 = (X, X)$, so that

$$|A - B|^2 = (A - B, A - B) = |A|^2 - 2(A, B) + |B|^2.$$

There is a similar equation for A' and B'. Since, by hypothesis, $|A' - B'| = |A - B|$, $|A'| = |A|$, and $|B'| = |B|$, it follows that $(A', B') = (A, B)$. But $(A, B) = |A||B| \cos\theta$, where $\theta = \angle AOB$. Therefore, $\angle AOB = \angle A'OB'$. But $O' = \sigma(O) = O$, because σ is a linear transformation, and so $\angle A'OB' = \angle A'O'B'$, as desired.

Now consider $\angle AVB$, where V need not be the origin O. If $\tau : W \mapsto W - V$ is the translation taking V to the origin, and if $\tau' : W \mapsto W + \sigma(V)$ is the translation taking the origin to $\sigma(V) = V'$, then the composite $\tau'\sigma\tau$ takes

$$\begin{aligned} W \mapsto W - V \mapsto \sigma(W - V) = \sigma(W) - \sigma(V) \mapsto \\ \sigma(W) - \sigma(V) + \sigma(V) = \sigma(W). \end{aligned}$$

Thus, $\sigma(W) = \tau'\sigma\tau(W)$ for all W, so that $\sigma = \tau'\sigma\tau$. Since the translations τ and τ' preserve all angles, not merely those with vertex at the origin, the composite preserves $\angle AVB$. •

The following definition of a *symmetry*, a common generalization of reflections and rotations, should now seem natural.

Definition. Given a figure F in the plane,[2] its ***symmetry group*** $\Sigma(F)$ is the family of all orthogonal transformations $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ for which

$$\sigma(F) = F.$$

The elements of $\Sigma(F)$ are called ***symmetries***.

[2] It is clear that these definitions can be generalized: for every $n \geq 1$, there is an n-dimensional real orthogonal group $O(n, \mathbb{R})$ consisting of all the distance preserving linear transformations of $\mathbb{R}^n$, and symmetry groups of figures in higher dimensional euclidean space are defined as for planar figures.

It is easy to prove that the symmetry group is a subgroup of the orthogonal group, and so it is a group in its own right.

The wonderful idea of Galois was to associate to each polynomial $f(x)$ a group, nowadays called its *Galois group*, whose properties reflect the behavior of $f(x)$. Our aim in this section is to set up an analogy between the symmetry group of a polygon and the Galois group of a polynomial.

Since our major interest is the Galois group, we merely state the fact that if σ is orthogonal and if U and V are points, then the image of the line segment UV is also a line segment, namely, $U'V'$, where $U' = \sigma(U)$ and $V' = \sigma(V)$. (The basic idea of the proof is a sharp form of the triangle inequality: if W is a point on the line segment UV, then $|UW| + |WV| = |UV|$, while if $W \notin UV$, then $|UW| + |WV| > |UV|$.)

Lemma 2. *If P is a (2-dimensional) polygon, then every orthogonal transformation $\sigma \in \Sigma(P)$ permutes* Vert(P), *the set of vertices of P.*

Proof. Let V be a vertex of P; if M, V, and N are consecutive vertices, then $\angle MVN \neq 180°$. If $V' = \sigma(V)$, then either V' lies on the perimeter of P or it lies in the interior of P.

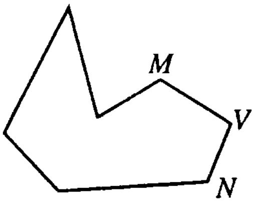


Figure 3

In the first case, Lemma 1 gives $\angle MVN = \angle M'V'N'$. But if V' is not a vertex, then $\angle M'V'N' = 180°$, a contradiction. Therefore, V' must be a vertex in this case.

In the second case, V' lies inside of P, and so there is a (2-dimensional) disk D with center V' lying wholly inside of P. Since $\sigma(P) = P$, every point in D lies in the image of σ. Now σ^{-1} is also an orthogonal transformation, and $\sigma^{-1}(V') = V$. In the disk D, every angle between 0° and 360° arises as $\angle JV'K$ for some points J and K in D. Now $\sigma^{-1}(\angle JV'K) = \angle J'VK'$ for some points J' and K' in P. But the only such angles satisfy

$$0 \leq \angle J'VK' \leq \angle MVN.$$

Therefore, there are angles that the orthogonal transformation σ^{-1} does not preserve, and this is a contradiction.

We conclude, for every vertex V, that $\sigma(V)$ is also a vertex; that is, the restriction σ_1 of σ maps Vert(P) to itself. Since σ is an injection, so is its restriction σ_1; since Vert(P) is finite, σ_1 must also be a bijection. Thus, if Vert$(P) = \{V_1, \ldots, V_n\}$, then

$$\{V_1, \ldots, V_n\} = \{\sigma(V_1), \ldots, \sigma(V_n)\} = \{\sigma_1(V_1), \ldots, \sigma_1(V_n)\},$$

and so σ_1 is a permutation of Vert(P). •

Theorem 3. *If P is a polygon with n vertices* Vert$(P) = \{V_1, \ldots, V_n\}$, *then $\Sigma(P)$ is isomorphic to a subgroup of the symmetric group S_n.*

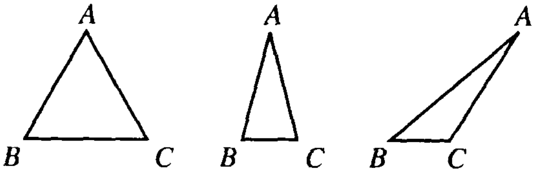


Figure 4

Proof. If $\sigma \in \Sigma(P)$, denote its restriction to Vert(P) by σ_1. By the lemma, σ_1 is a permutation of Vert(P); that is, $\sigma_1 \in S_{\text{Vert}(P)}$. It follows that the assignment $\sigma \mapsto \sigma_1$ is a well defined function $f : \Sigma(P) \to S_{\text{Vert}(P)}$.

To see that f is a homomorphism, suppose that $\sigma, \tau \in \Sigma(P)$. It is easy to see that if $V \in$ Vert(P), then $(\sigma\tau)_1$ and $\sigma_1\tau_1$ both have the same value on V, namely, $\sigma(\tau(V))$. Therefore, $(\sigma\tau)_1 = \sigma_1\tau_1$, and so f is a homomorphism:

$$f(\sigma\tau) = f(\sigma)f(\tau).$$

Finally, f is an injection, i.e., $\ker f = 1$, for if $f(\sigma) = \sigma_1 = 1$, then σ fixes every vertex $V \in$ Vert(P). But regarding the vertices as vectors in $\mathbb{R}^2$, there are two such that are linearly independent (neither is a scalar multiple of the other), and so these two vectors comprise a basis of $\mathbb{R}^2$. Since σ is a linear transformation fixing a basis of $\mathbb{R}^2$, it must be the identity. Therefore, f is an isomorphism between $\Sigma(P)$ and a subgroup of $S_{\text{Vert}(P)} \cong S_n$. •

Corollary 4. *Let Δ be a triangle with vertices A, B, and C. If Δ is equilateral, then $\Sigma(\Delta) \cong S_3$; if Δ is only isosceles, then $\Sigma(\Delta) \cong \mathbb{Z}_2$; if Δ is scalene, then $\Sigma(\Delta)$ has order* 1.

Proof. By the Theorem, $\Sigma(\Delta)$ is isomorphic to a subgroup of S_3. If Δ is equilateral, then we can exhibit 6 symmetries of it: the reflections about any of the 3 altitudes and the rotations of 0°, 120° and 240°. Since $|S_3| = 6$, it follows that $\Sigma(\Delta) \cong S_3$. If Δ is isosceles, say, $|AC| = |AB|$, then the reflection about the altitude through A is in $\Sigma(\Delta)$. This is the only non-identity symmetry, for every symmetry σ must fix A because the angle at A is different than the angles at B and C (lest Δ be equilateral). Thus, $\Sigma(\Delta) \cong \mathbb{Z}_2$. Finally, if Δ is scalene, then any symmetry fixes all the vertices, for no two angles are the same, and hence it is the identity. •

We shall see later that the Galois group of a polynomial having n distinct roots is also isomorphic to a subgroup of S_n. Moreover, there may be permutations of the roots that do not arise from the Galois group, just as there may be permutations of the vertices that do not arise from symmetries; for example, in Corollary 4 we saw that only two of the six permutations of the vertices of an isosceles triangle arise from symmetries.

Exercises

1. (i) If F is a square, prove that $\Sigma(F) \cong D_8$, the dihedral group of order 8.

   (ii) If F is a rectangle that is not a square, prove that $\Sigma(F) \cong V$, where V denotes the 4-group ($V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$).

   (iii) Give an example of quadrilaterals Q and Q' with $\Sigma(Q) \cong \mathbb{Z}_2$ and $\Sigma(Q') = 1$.

2. A polygon is ***regular*** if all the angles at its vertices are equal. Prove that a polygon P is regular if and only if $\Sigma(P)$ acts transitively on Vert(P).

3. Prove that if P_n is a regular polygon with n vertices, then $\Sigma(P_n) \cong D_{2n}$, where D_{2n} is the dihedral group of order $2n$.

4. Prove that if F is a circular disk, then $\Sigma(F)$ is infinite.

Rings

The algebraic system encompassing fields and polynomials is a commutative ring with 1. We assume that the reader has, at some time, heard the