

GALOIS THEORY

NOTES FOR MATH338

by Dr C.D.H. Cooper
Macquarie University

4th Edition 2010

CONTENTS

CHAPTER 0: PREPARATION FOR GALOIS THEORY

0.1 Sets and Functions	5
0.2 Complex Numbers	5
0.3 Coordinate Geometry	5
0.4 Fields and Rings	6
0.5 Vector Spaces	6
0.6 Polynomials	7
0.7 Groups	8
0.8 Permutations	9
0.9 Calculus	9
Exercises for Chapter 0	9
Solutions for Chapter 0	11

CHAPTER 1: POLYNOMIALS

1.1 Prime Polynomials	15
1.2 Prime Polynomials over \mathbf{Z}_p	16
1.3 Integer Polynomials	17
1.4 Tests for Primeness over \mathbf{Q}	18
1.5 Minimum Polynomials	22
1.6 Numbers of Real Zeros	25
Exercises for Chapter 1	28
Solutions for Chapter 1	29

CHAPTER 2: FIELD EXTENSIONS

2.1 Ruler and Compass Constructions	33
2.2 Examples of Ruler and Compass Constructions	35
2.3 Constructible Numbers	37
2.4 Number Fields and Field Extensions	38
2.5 Fields as Vector Spaces	39
2.6 Dimensions of Field Extensions	40
2.7 Degree of the Minimum Polynomial	41
Exercise for Chapter 2	42
Solutions for Chapter 2	43

CHAPTER 3: SOLUBILITY BY RADICALS

3.1 The Quadratic Equation From An Advanced Standpoint	49
3.2 The Cubic Equation	50
3.3 A Short History of the Problem	52
3.4 Radical Extensions of Fields.....	53
3.5 A Precise Statement of the Problem	54
3.6 Galois Groups of Field Extensions	56
3.7 Extending Automorphisms	57
3.8 Restricting Automorphisms	59
3.9 Galois Groups and Radical Extensions	59
3.10 Solubility	60
3.11 Permutations on the Zeros of a Polynomial	61
Exercises for Chapter 3	63
Solutions for Chapter 3	64

CHAPTER 4: EXAMPLES OF GALOIS GROUPS

4.1 Overview of Galois Theory	69
4.2 $f(x) = x^4 - x^2 - 2$	69
4.3 $f(x) = x^3 - 2$	71
4.4 $f(x) = x^4 - 2$	72
4.5 $f(x) = x^5 - 2$	74
4.6 $f(x) = x^4 - 6x^2 + 3$	74
4.7 $f(x) = x^6 - 18x^3 + 6$	76
4.8 $f(x) = x^6 - 6x^3 + 6$	77
4.9 $f(x) = x^{15} - 1$	78
4.10 $f(x) = x^8 - 5x^5 - 7x^3 + 35$	78
4.11 $f(x) = x^{30} - 30x^{15} + 216$	78
4.12 $f(x) = x^3 - 3x + 1$	79
4.13 $f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	79

CHAPTER 5: THE FUNDAMENTAL THEOREM OF ALGEBRA

5.1 Algebraically Closed Fields	83
5.2 Fixed Fields	83
5.3 Automorphisms as Linear Transformations.....	83
5.4 Fixed Fields of Polynomial Extensions	85
5.5 Finite-dimensional Extensions of the Real and Complex Fields	86
5.6 The Proof of the Fundamental Theorem of Algebra	86

CHAPTER 6: FINITE FIELDS

6.1 The Field $GF(4)$	89
6.2 Fields as Quotient Rings	90
6.3 Prime Subfields	92

APPENDIX A: The Life of Galois	95
APPENDIX B: An Overview of Galois Theory	97
APPENDIX C: Cubic Equation Worksheet	101

0. PREPARATION FOR GALOIS THEORY

0.1 Sets and Functions

A **set** is a collection of “things” called elements with $x \in S$ indicating that x is an **element** of the set S ($x \notin S$ if it is not).

A set can be described by listing its elements $\{a, b, \dots\}$ or by specifying a defining property $\{x \in S \mid Px\}$ meaning the set of all $x \in S$ for which Px is true. We often omit the “ $\in S$ ” if it is understood). S is a **subset** of T if $x \in S$ implies that $x \in T$ and we denote this by $S \subseteq T$. It is a **proper subset** ($S \subset T$) if as well $S \neq T$. Two sets are defined to be **equal** if each is a subset of the other. The **empty set** is \emptyset . The **intersection** $S \cap T = \{x \mid x \in S \text{ and } x \in T\}$ and the **union** $S \cup T = \{x \mid x \in S \text{ or } x \in T\}$.

A **map** (function) $\theta: S \rightarrow T$ is a pair of sets S (= **domain**) and T (= **codomain**) together with a rule that associates with every $x \in S$ a unique **image** $x^\theta \in T$. (It is more common to write this as $\theta(x)$ but we shall reserve that notation for polynomials.) The set of all the images of the elements of S is called the **image** of θ and is written $\text{im } \theta = \{x^\theta \mid x \in S\}$. The map is **1-1** if $x^\theta = y^\theta$ implies that $x = y$ and **onto** if $\text{im } \theta = T$. We say that θ **fixes** x if $x^\theta = x$. The **identity map** on a set S is the map $1: S \rightarrow S$ which fixes every element. If $\alpha: X \rightarrow Y$ and $\beta: Y \rightarrow Z$ are maps we define their **product** $\alpha\beta: X \rightarrow Z$ by $x^{\alpha\beta} = (x^\alpha)^\beta$, that is apply α first, then β . (Note $\alpha\beta$ would often be written as $\beta \circ \alpha$.)

0.2 Complex Numbers

Complex numbers are of the form $z = x + iy$ where $x, y \in \mathbf{R}$, and i is an “imaginary” number satisfying $i^2 = -1$. They are added and multiplied in the usual way. Writing z in the **polar form** $r(\cos \theta + i \sin \theta)$ with $r > 0$ and $0 \leq \theta < 2\pi$ (unique if $z \neq 0$) we define the **modulus** of z , to be $|z| = r = \sqrt{x^2 + y^2}$ and the **argument** of z to be $\arg z = \theta$. The **conjugate** of z is $\bar{z} = x - iy$, so a complex number is real if and only if it is equal to its conjugate.

For $z \neq 0$, $z^{-1} = \frac{\bar{z}}{|z|^2}$. In particular, for complex numbers with modulus 1 (on the **unit circle**), $z^{-1} = \bar{z}$.

De Moivre's Theorem says that $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$, the first step towards justifying $e^{i\theta} = \cos \theta + i \sin \theta$. The n 'th roots of 1, $\varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$ where $\varepsilon = e^{2\pi i/n}$ and for $n \geq 2$ their sum is 0 (the sum of the zeros of $z^n - 1$). In particular the cube roots of 1 are 1, ω, ω^2 where $\omega = e^{2\pi i/3} = \frac{-1 + \sqrt{3}i}{2}$ and $1 + \omega + \omega^2 = 0$.

0.3 Coordinate Geometry

The equation of the **line** passing through (x_1, y_1) and (x_2, y_2) is:

$$(y - y_1)(x_2 - x_1) = (x - x_1)(y_2 - y_1).$$

and the equation of the **circle** with centre (x_1, y_1) that passes through (x_2, y_2) is:

$$(x - x_1)^2 + (y - y_1)^2 = (x_2 - x_1)^2 + (y_2 - y_1)^2.$$

0.4 Fields and Rings

The modern view of Galois Theory is that it is the study of fields using group theory as a tool, though the concept of a field came much later than Evaristé Galois (1811-1832). A **field** is an algebraic system which consists of a set F , together with two binary operations $+$ and \times . In addition F is closed under each of these operations each operation is both associative and commutative and \times is distributive over $+$. Also for each operation, there is an identity element. The additive identity is written 0 and the multiplicative identity is written 1 . The axioms of a field insist that $1 \neq 0$ thereby ruling out fields with just one element. Finally for each operation there are inverses. Every element $x \in F$ has an additive inverse $-x \in F$ and every non-zero $x \in F$ has a multiplicative inverse, x^{-1} .

The familiar examples of field are the field of rational numbers \mathbf{Q} , the field of real numbers \mathbf{R} and the field of complex numbers \mathbf{C} . There are also finite fields, of which the simplest are the fields, \mathbf{Z}_p , of integers modulo a prime. A **subfield** of a field is a subset which is a field under the same operations, so \mathbf{Q} and \mathbf{R} are examples of subfields of \mathbf{C} .

A **ring** is a more general structure, again with two operations of addition and multiplication, but where multiplication need not be commutative and where elements need not have inverses under multiplication. Sometimes even the existence of an identity under multiplication is not required. The ring of integers, \mathbf{Z} , is a commutative ring and the ring $M_n(F)$ of all $n \times n$ matrices over F is an example of a non-commutative ring.

0.5 Vector Spaces

A **vector space** over a field F is a set V together with two operations: addition and multiplication by a **scalar** (element of F). Under addition a vector space must be an abelian group. Additional axioms involving scalar multiplication are:

$$\lambda v \in V, (\lambda + \mu)v = \lambda v + \mu v, \lambda(u + v) = \lambda u + \lambda v, (\lambda\mu)v = \lambda(\mu v) \text{ and } 1v = v.$$

A **subspace** is a subset that is a vector space under the same operations. Notation: $U \leq V$.

We tend to think of vectors as having components, such as (x, y, z) and as such are quite distinct from scalars. However the axioms don't insist on this. By comparing the axioms for fields and vector spaces we can see that fields can be viewed as vector spaces over subfields, in which case the elements of the subfield will be both a vector and a scalar.

A **linear combination** of vectors is an expression of the form $\lambda_1 v_1 + \dots + \lambda_n v_n$ where the λ 's are scalars and the v 's are vectors. It is **non-trivial** if at least one $\lambda_i \neq 0$. A set of vectors X **spans** a vector space if every vector in the space is a linear combination of the vectors in X and it is **linearly independent** if no non-trivial linear combination is zero (otherwise it is **linearly dependent**). A **basis** for V is a linearly independent subset which also spans V . A vector space is finite-dimensional if it has a finite spanning set. Every finite-dimensional vector space V has a basis and all bases have the same size, called the **dimension** of V (or **dim** V). Any subset smaller than $\dim V$ can't span V and any set bigger than $\dim V$ must be linearly dependent.

A **linear transformation** $f: U \rightarrow V$, from one vector space over F to another, is a map which preserves addition and scalar multiplication. The **kernel** of f (**ker** f) = $\{v \in V \mid v^f = 0\}$ and the **image** (**im** f) = $\{v^f \mid v \in V\}$ are subspaces of U, V respectively and the sum of their dimensions is $\dim U$ (rank + nullity = ...).

0.6 Polynomials

In the middle ages, solving polynomial equations was the main problem of algebra and the quintic was what inspired Galois. A **polynomial** over a field F is an expression of the form $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ where the coefficients $a_0, \dots, a_n \in F$ and where x is an “indeterminate”. (coefficients of higher powers are assumed to be zero.) It is usually written in the form $f(x)$ and if α is substituted for x the value obtained is written $f(\alpha)$. Polynomials are regarded as equal if corresponding coefficients are equal. The set of all polynomials over F is denoted by $F[x]$. Polynomials can be added and multiplied in the usual way and under these operations $F[x]$ is a commutative ring, though not a field.

The above polynomial is said to have **degree** n if $a_n \neq 0$, in which case a_n is called the **leading coefficient**. (The degree of the zero polynomial is undefined.) A polynomial is **monic** if its leading coefficient is 1. A polynomial of degree 0 is a non-zero **constant polynomial**. There are special names for polynomials of low degree (**linear polynomials** have degree 1, **quadratics** have degree 2, and the list extends to **cubics, quartics, quintics, ...**). When polynomials multiply their degrees add, so degree is like a crude sort of logarithm.

The so-called **Division Algorithm** is actually a theorem which states that every polynomial $a(x) \in F[x]$ can be divided by a non-zero polynomial $b(x)$, giving a **quotient** $q(x)$ and a **remainder** $r(x)$ (both in $F[x]$) where the remainder is either zero or has lower degree than $b(x)$. A simple consequence is the **Remainder Theorem** which states that the remainder on dividing $f(x)$ by $x - \alpha$ is $f(\alpha)$.

A **zero** of a polynomial $f(x)$ is a number α for which $f(\alpha) = 0$. Any non-real zeros of a real polynomial come in conjugate pairs. Real polynomials of odd degree have at least one real zero (by continuity). More generally, the **Fundamental Theorem of Algebra** states that every non-constant polynomial over \mathbf{C} has a zero in \mathbf{C} (proved in chapter 3).

If the remainder on dividing $a(x)$ by $b(x)$ is zero we say that $b(x)$ **divides** $a(x)$. Divisibility properties of polynomials are very similar to those of integers. In particular we define a non-constant polynomial to be **prime** if it cannot be factored as a product of polynomials of lower degree. (The constant polynomials are excluded for technical reasons similar to those that exclude the number 1 from being called a prime.)

We define the **greatest common divisor** of two non-zero polynomials $a(x), b(x)$ to be the monic polynomial of highest degree which divides both of them. We denote it by $\mathbf{GCD}(a(x), b(x))$ and if the GCD is 1 we say that the polynomials are **coprime**. As with integers there is a method for computing the GCD called **the Euclidean Algorithm**. This involves dividing one polynomial by another and then repeatedly dividing the most recent remainder by the one before. Eventually we get a zero remainder and the last non-zero remainder, made monic, is the GCD. A consequence of this algorithm is the fact that the GCD of $a(x)$ and $b(x)$ can be expressed in the form $a(x)h(x) + b(x)k(x)$ for some polynomials $h(x), k(x)$ over the same field.

The quadratic formula, $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ for the quadratic $ax^2 + bx + c$ expresses the zeros in terms of its coefficients using the operations $+, -, \times, \div$ and extraction of roots (radicals). There are similar (though more complicated) formulae for the cubic and quartic but not for most quintics and beyond.

0.7 Groups

Galois invented group theory for the purpose of answering the question “which polynomials have zeros that can be expressed in terms of its coefficients using the operations $+$, $-$, \times , \div and extraction of roots?” A **group** is an algebraic structure G with an associative operation (which we shall usually call multiplication) under which G is closed, and where there is an identity element, denoted by 1 , with respect to which every element of G has an inverse. The **trivial group** is $\{1\}$. An **abelian group** is one which satisfies the commutative law.

A **subgroup** is a non-empty subset which is closed under multiplication and inverses. Notation: $H \leq G$. Powers are defined in the usual way and the **cyclic subgroup generated by g** is $\langle g \rangle = \{g^n \mid n \in \mathbf{Z}\}$. A group is **cyclic** if it is $\langle g \rangle$ for some $g \in G$, called a **generator**. Cyclic groups are abelian. The **order of a group G** is its size $|G|$ and the **order of an element g** is the order of the subgroup $\langle g \rangle$.

If $H \leq G$ a **coset** (left/right) is a set of the form $xH = \{xh \mid h \in H\}$ or $Hx = \{hx \mid h \in H\}$. The group G decomposes into a disjoint union of cosets of either type from which it follows that the order of a subgroup (and hence the order of an element) of a finite group G divides $|G|$.

If $Hx = xH$ for all $x \in G$ we say that H is a **normal subgroup** of G and in such cases we can form a group, called the **quotient group G/H** , from these cosets with the coset H as its identity. A **simple group** is one with no proper non-trivial normal subgroup.

The **cyclic group of order n** is denoted by C_n . The **dihedral group D_{2n}** (of order $2n$) can be expressed in terms of generators and relations by $\langle A, B \mid A^n = B^2 = 1, BA = A^{-1}B \rangle$ with D_4 more usually written V_4 . D_{2n} is non-abelian iff $n > 2$. Groups of prime order are cyclic and groups of order $2p$ must be cyclic or dihedral.

A group **homomorphism** is a map $f: G \rightarrow H$, from one group to another which preserves products and an **isomorphism** is a 1-1 and onto homomorphism. If an isomorphism exists between G and H we say that G, H are **isomorphic** and we write $G \cong H$. The **kernel** of a homomorphism $f = \ker f = \{g \in G \mid g^f = 1\}$ and the **image** of f is $\text{im } f = \{g^f \mid g \in G\}$.

The First Isomorphism Theorem states that $\ker f$ is a normal subgroup of G , $\text{im } f$ is a subgroup of H and $G/\ker f \cong \text{im } f$. Consequences are:

Second Isomorphism Theorem: if $H, K \leq G$ with K being normal, then $HK/K \cong H/(H \cap K)$;

Third Isomorphism Theorem: if $H \leq K \leq G$ with both H, K being normal in G , then $(G/H)/(G/K) \cong K/H$.

A **commutator** is an element of the form $[x, y] = x^{-1}y^{-1}xy$. The **derived subgroup** of a group G is $G' =$ subgroup generated by all the commutators. A useful characterisation of G' is that it is the smallest normal subgroup for which the quotient is abelian. The **derived series** is $G \geq G' \geq G'' \geq \dots$ and if this series reaches 1 we say that G is **soluble**.

If p^n divides $|G|$, where p is prime and G is a finite group, then G has a subgroup of order p^n . In particular if p^n is the largest power of p which divides $|G|$ then such a subgroup is called a **Sylow p -subgroup**.

The direct sum of abelian groups G_1, \dots, G_k is $G_1 \oplus \dots \oplus G_k = \{(x_1, \dots, x_k) \mid \text{each } x_i \in G_i\}$ with point-wise addition. Every finite abelian group is a direct sum of cyclic groups of prime power order.

0.8 Permutations

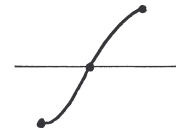
For Galois, all groups were groups of permutations on the zeros of polynomials. A **permutation** on a set X is a 1-1 map from X to itself. The most efficient notation is **cycle notation**: $(x_1 x_2 \dots x_r)(y_1 \dots y_s) \dots$ where each symbol maps to the one on its right, except for the last in each cycle which maps to the first. Cycles of length 1 are omitted, except for the identity permutation which is denoted by I . The **symmetric group** S_n is the set of all $n!$ permutations on $\{1, 2, \dots, n\}$ under multiplication of **maps**.

An **n-cycle** is a permutation of the form $(x_1 \dots x_n)$ and a **transposition** is a 2-cycle. Every permutation is a product of cycles and each **n-cycle** is a product of $n - 1$ **transpositions** so every permutation is a product of transpositions. An **even (odd)** permutation is one which is a product of an even (odd) number of transpositions and no permutation can be both, so cycles of odd length are even. Permutations satisfy the rules even \times even = even, even \times odd = odd, odd \times odd = even. The **alternating group** A_n is the subgroup of S_n consisting of the even permutations. For $n \geq 5$, A_n is simple and so A_n and S_n are not soluble for these n .

0.9 Calculus

If $f: \mathbb{R} \rightarrow \mathbb{R}$ we say that L is the limit of $f(x)$ as $x \rightarrow a$ if, for all $\epsilon > 0$ there exists $\delta > 0$ such that $|x - a| < \delta$ implies that $|f(x) - L| < \epsilon$. We say that f is continuous at $x = a$ if the limit of $f(x)$ as $x \rightarrow a$ is $f(a)$ and that f is differentiable at $x = a$ if the limit of $\frac{f(x) - f(a)}{x - a}$ as $x \rightarrow a$, exists. We call this limit $f'(x)$ and the function f' is called the derivative. We say that f is continuous or differentiable if it has the property at every point. Differentiability implies continuity and polynomials have both properties.

Intermediate Value Theorem: If $f(x)$ is a continuous function on the closed interval $[a, b]$ then if $f(a) < 0 < f(b)$ we must have $f(c) = 0$ for some c with $a < c < b$.
(Of course a similar result holds if $f(a) > 0 > f(b)$.)



Rolle's Theorem: If $f(x)$ is differentiable on the open interval (a, b) and continuous on the closed interval $[a, b]$ then if $f(a) = 0 = f(b)$ we must have $f'(c) = 0$ for some c with $a < c < b$.



EXERCISES FOR CHAPTER 0

Exercise 1: If $S = \{1, 2, 4, 5\}$ and $T = \{1, 3, 4, 6\}$ write down $S \cap T$.

Exercise 2: How many proper non-empty subsets are there of $\{1, 3, 4\}$.

Exercise 3: Is the map $\theta: \{x \in \mathbf{R} \mid x > 0\} \rightarrow \mathbf{Z}$ defined by $x^\theta = \text{INT}(\log x)$ a 1-1 function? Is it onto? Here INT means the integer part.

Exercise 4: If $f: \mathbf{R} \rightarrow \mathbf{R}$ and $g: \mathbf{R} \rightarrow \mathbf{R}$ are defined by $x^f = x^2$ and $x^g = 2^x$ find 3^{fg} and 3^{gf} .

Exercise 5: Write down the fixed points of $f: \mathbf{R} \rightarrow \mathbf{R}$ defined by $x^f = x^2 - 4x + 6$.

Exercise 6: Find the modulus, conjugate and inverse of the complex number $i - 2$.

Exercise 7: Simplify $\omega + \omega^2$.

Exercise 8: Write down all five fifth roots of 1 in terms of $\varepsilon = e^{2\pi i/5}$.

Exercise 9: If $\varepsilon = e^{2\pi i/7}$ find the conjugate of ε^3 as a power of ε .

Exercise 10: Which real number(s) can be expressed as a sum of two cube roots of 1?

Exercise 11: If $A = (1, -3)$ and $B = (3, 5)$ find the equations of the line through A, B and the circle with centre A which passes through B.

Exercise 12: Is $F = \{a + bi \mid a, b \in \mathbf{Q}\}$ a field?

Exercise 13: Is $F = \{a + b\sqrt[3]{2} \mid a, b \in \mathbf{Q}\}$ a field?

Exercise 14: Is $\{(2, 1), (4, 2)\}$ a basis for \mathbf{R}^2 ?

Exercise 15: Are the vectors $(1, 1), (2, 5), (3, 17)$ linearly independent?

Exercise 16: If $f: \mathbf{R}^7 \rightarrow \mathbf{R}^3$ is a linear transformation whose image is $\{(x, y, x + y) \mid x, y, z \in \mathbf{R}\}$ find the dimension of $\ker f$.

Exercise 17: Find the zeros, over \mathbf{Q} , of the polynomial $x^2 + 5x + 6$.

Exercise 18: “The polynomial $x^5 + 17x^4 - 33x + 2$ has exactly 2 real zeros and 3 non-real zeros.” Why must this statement be false?

Exercise 19: “The polynomial $x^4 - 3x^7 + 32$ has four non-real zeros and no real ones.” Why must this claim be false?

Exercise 20: If a real polynomial $f(x)$ has a non-real zero α , find a real quadratic factor.

Exercise 21: Which real polynomials over \mathbf{R} are prime over \mathbf{R} ?

Exercise 22: Find the $\text{GCD}(x^3 + 1, x^2 + 2x + 1)$ and express it in the form $(x^3 + 1)h(x) + (x^2 + 2x + 1)k(x)$ for suitable rational polynomials $h(x), k(x)$.

Exercise 23: If G is the group $\langle A, B \mid A^4 = B^2 = 1, BA = A^{-1}B \rangle$ what is $|G|$?

Exercise 24: What is the order of the complex number i under multiplication?

Exercise 25: Write down a proper non-trivial subgroup of the cyclic group generated, under multiplication, by the complex number i .

Exercise 26: “The group G has order 100 and has 5 subgroups of order 6”. Why must this statement be false?

Exercise 27: If $|G| = 17$, find all the subgroups of G .

Exercise 28: For which of the following values of n : 3, 4, 5, 6, 7, 8 is there a cyclic group of order n . For which of these values of n is there no other group of order n ?

Exercise 29: The group $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$ is a group under multiplication modulo 20 and $H = \{1, 11\}$ is a normal subgroup. Find the cosets of H in G . Which of the groups C_4 and $C_2 \times C_2$ is isomorphic to G/H ?

Exercise 30: Let $f: \mathbf{R}^\# \rightarrow \mathbf{R}$ be defined by $x^f = \log(x^2)$, where \mathbf{R} is the group of all real numbers under addition and $\mathbf{R}^\#$ is the group of all non-zero real numbers under multiplication. Show that f is a homomorphism and find $\ker f$ and $\text{im } f$. Hence find a quotient group of $\mathbf{R}^\#$ which is isomorphic to \mathbf{R} .

Exercise 31: Which abelian groups are soluble?

Exercise 32: If $|G'| = 4$, why must G be soluble?

Exercise 33: Why is D_{60} a soluble group?

Exercise 34: “The group G has order 80 and only 4 proper non-trivial subgroups.” Why must this statement be false?

Exercise 35: What are the orders of the Sylow subgroups of a group of order 1125?

Exercise 36: If $a = (1\ 2\ 3\ 4\ 5)$ and $b = (1\ 2)$, find $(ab)^{-2}b(ab)^2$.

Exercise 37: Is $(1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9) \in A_9$?

Exercise 38: A_4 has a normal abelian subgroup V_4 of order 4. Why does it follow that S_4 is soluble?

Exercise 39: For which values of n is S_n soluble?

Exercise 40: If $a = (1\ 4\ 5\ 2\ 3\ 7\ 6)$ and $b = (2\ 7)$ find the order of the group they generate.

SOLUTIONS FOR CHAPTER 0

Exercise 1: $S \cap T = \{1, 4\}$.

Exercise 2: 6.

Exercise 3: It is neither.

Exercise 4: $3^{fg} = 2^9$ and $3^{gf} = 2^6$.

Exercise 5: These are the values of x for which $x^2 - 4x + 6 = x$, namely 2, 3.

Exercise 6: The modulus is $\sqrt{5}$, the conjugate is $-i - 2$ and the inverse is $-\frac{2+i}{5}$.

Exercise 7: -1 .

Exercise 8: $1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$.

Exercise 9: ε^4 .

Exercise 10: 2 and -1 .

Exercise 11: The equation of AB is $\frac{y+3}{x-1} = \frac{5+3}{3-1} = \frac{8}{2} = 4$, which simplifies to $y = 4x - 7$.

The equation of the circle is $(x-1)^2 + (y+3)^2 = (3-1)^2 + (5+3)^2 = 68$.

This simplifies to $x^2 + y^2 - 2x + 6y - 58 = 0$.

Exercise 12: YES. Since $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} \in F$ if $a+bi \neq 0$, it satisfies the property that every non-zero element has a multiplicative inverse. The other field properties are obvious.

Exercise 13: NO because $(\sqrt[3]{2})^2 \notin F$.

Exercise 14: NO. They are not linearly independent.

Exercise 15: NO. The space of vectors (x, y) has dimension 2 and so any more than 2 vectors will be automatically linearly dependent.

Exercise 16: The rank of f is the dimension of the image. It is clearly 2. The nullity is therefore $7 - 2 = 5$. This is the dimension of $\ker f$.

Exercise 17: $-2, -3$.

Exercise 18: Non-real zeros of a real polynomial come in conjugate pairs and hence there must always be an even number of them.

Exercise 19: It has degree 7. Since 7 is odd the polynomial must have a real zero.

Exercise 20: The conjugate $\bar{\alpha}$ must also be a zero and hence $(x - \alpha)(x - \bar{\alpha})$ must be a real quadratic factor. This can be written as $x^2 - 2\operatorname{Re}(\alpha)x + |\alpha|^2$.

Exercise 21: Linear polynomials, of the form $ax + b$ (where $a \neq 0$) and quadratics of the form $ax^2 + bx + c$ where $b^2 < 4ac$. (Note that this automatically includes the condition that $a \neq 0$.)

Exercise 22:

$$\begin{array}{r} x^2 + 2x + 1 \overline{) x^3 + 2x^2 + x + 1} \\ \underline{x^3 + 2x^2 + x} \\ -2x^2 - x + 1 \\ \underline{-2x^2 - 4x - 2} \\ 3x + 3 \end{array}$$

Replace this by $x + 1$

Clearly $x^2 + 2x + 1 = (x + 1)^2$, with a remainder of zero, so the last non-zero remainder, made monic, is $x + 1$.

From the above, $3x + 3 = (x^3 + 1) - (x^2 + 2x + 1)(x - 2)$

Hence we can take $h(x) = \frac{1}{3}$ and $k(x) = \frac{1}{3}(x - 2)$.

Exercise 23: 8.

Exercise 24: 4.

Exercise 25: $\{1, -1\}$.

Exercise 26: 6 does not divide 100, so this contradicts Lagrange's Theorem.

Exercise 27: Just 1 and G because 17 is prime.

Exercise 28: All of them. None of them.

Exercise 29: $H = \{1, 11\}$, $3H = \{3, 13\}$, $7H = \{7, 17\}$, $9H = \{9, 19\}$.

$(3H)^2 = 9H \neq H$ so $3H$ has order 4. This means that $G/H \cong C_4$.

Exercise 30: $(xy)^f = \log((xy)^2) = \log(x^2y^2) = \log(x^2) + \log(y^2) = x^f + y^f$.

$\ker f = \{x \in \mathbf{R}^\# \mid \log(x^2) = 0\} = \{x \in \mathbf{R}^\# \mid x^2 = 1\} = \{1, -1\}$.

$\text{im } f = \mathbf{R}$.

Hence $\mathbf{R}^\#/\{1, -1\} \cong \mathbf{R}$.

Exercise 31: All of them.

Exercise 32: Groups of order 4 are abelian and so $G'' = 1$.

Exercise 33: $D_{60} = \langle a, b \mid a^{30} = b^2 = 1, b^{-1}ab = a^{-1} \rangle$.

Let $H = \langle a \rangle$. Then D_{60}/H has order 2 and so $D_{60}' \leq H$. But H is abelian, so $D_{60}'' = 1$.

Exercise 34: By Sylow's Theorem there exists a subgroup of order p^n when ever the prime power p^n divides the group order. Hence G has subgroups of orders 2, 4, 8, 16 and 5.

Exercise 35: $1125 = 3^2 \cdot 5^3$. So the Sylow 3-subgroups have order 9 and the Sylow 5-subgroups have order 125.

Exercise 36: $ab = (2\ 3\ 4\ 5)$ and so $(ab)^2 = (2\ 4)(3\ 5)$.

Hence $(ab)^{-2}b(ab)^2 = [(2\ 4)(3\ 5)]^{-1}(1\ 2)[(2\ 4)(3\ 5)] = (1\ 4)$.

Exercise 37: YES. It is an even permutation.

Exercise 38: $|S_4/A_4| = 2$ so $S_4' \leq A_4$.

$|A_4/V_4| = 3$ so A_4/V_4 is cyclic and hence abelian, so $S_4'' \leq A_4' \leq V_4$.

Since groups of order 4 are abelian, $S_4''' \leq V_4' = 1$.

Exercise 39: $n = 1, 2, 3$ and 4 .

Exercise 40: They generate S_7 , which has order $7! = 5040$.