תוכנית רוטשילד - ויצמן למצוינות בהוראת המדעים
במימונה של קרן קיסריה אדמונד בנימין דה רוטשילד

קרן קיסריה
אדמונד בנימין דה רוטשילד

המחלקה להוראת המדעים

קורס
Algebra:
From Equations to Structures

המרצה:
ד"ר ג'וזי שמש

תשע"ב

תוכן עניינים:

1. Introduction and definitions of algebraic structures: rings, fields, groups, vector spaces.

Introduction:

Starting point: Discussion regarding $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ as historical motivation for entire course.

The search for a formula for the roots of the polynomial equation of degree *n*, using the coefficients of the formula, the four arithmetic operations, and extraction of roots. The work of Galois and Abel and their insights which led to them looking at number fields, permutations of roots of polynomials, and groups of permutations.

Note: All topics were connected to this basic goal throughout the course.

Definitions:

Rings, fields, groups, vector spaces – using tables to compare the sets of axioms (see attachments).

Usual basic examples of fields and counterexamples:
Including $Q(\sqrt{2})$, construction of finite fields of order 2, 3, 5 (order 4 in homework)

Usual basic examples of rings and counterexamples:
Including Cartesian products of rings, rings of polynomials in one and 2 variable over Z, and over fields. Z_n.

Usual basic examples of groups and counterexamples:
Including additive and multiplicative groups of a field, definition of S_3, $\{\pm 1, \pm i\}$, and group of rotations of the plane.

Usual basic examples of vector spaces and counterexamples:
Including vector spaces of functions.

Substructures: definitions and usual basic examples and counterexamples.

Some basic claims – e.g.: In a subfield, the zero and identity element are the same as in the field.

סיכום השיעור

נתחיל בביטוי מוכר:

$$\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

מהו בעצם מבטא?
שורשי המשוואה הריבועית $ax^2+bx+c=0,\quad a\neq 0$ מבוטאים בעזרת המקדמים של הפולינום במשוואה תוך שימוש ב-4 פעולות החשבון (+, -, *, /) ופעולת השורש הריבועי.

תחום האלגברה: עסקו מתמטיקאים במשך מאות שנים בחיפוש דרכים לפתרון משוואות –

בפרט המטרה המרכזית החל מהמאה ה-16 פתרון של המשוואה הפולינומיאלית:
$$x^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0=0$$
ומציאת נוסחאות באמצעות 4 פעולות החשבון והצוצאת שורשים.

דוגמא:
המשוואה $5x^3-2=0$ ניתנת לפתרון בעזרת חיבור, חילוק והצאת שורש מסדר 3:
$x=\sqrt[3]{\frac{2}{5}}$.
מטרה נוספת:
דרכי פתרון למערכות משוואות ליניאריות שגם עליהם נדבר עליהן בהמשך – שמתחבר גם לבעיה הראשונה.

שני שמות החשובים ביותר בהקשר לבעיה הראשונה: Galois, Abel.

- יש לעיין בפרק בספר של מריו ליביו, ובפרק 2.

במטרה המרכזית –
היתה התקדמות רבה במשך 300 שנה:
משוואות ממעלה 2, 3, 4 נפתרו בעזרת נוסחאות.
החשיבות של Galois היא שבנסיונותיו לפל במשוואה ממעלה 5 הוא הצליח להכליל ולפתור את המקרה הכללי (ממעלה n) – והפך לגמרי את כל דרך ההתסכלות על הבעיה.
הוא הבחין בשני דברים חשובים מאוד:
1. חשובה **<u>קבוצת המספרים</u>** עליה ואיתה אנו עובדים ותכונותיה האלגבריות.
2. חשוב להסתכל בתכוניתהם של שורשי המשוואה (בהנחה שיש כאלה) והקשרים ביניהם.

נתייחס תחילה למשוואה הריבועית.
נתחיל בקבוצת המספרים:
1. אנו חייבים לעבוד עם קבוצת מספרים עליה מוגדרות חיבור, כפל, נגדיים והופכיים כדי לפתור את המשוואות.

למשל:
את המשוואה $4x^2-4x+1=0$ לא ניתן לפתור בקבוצת המספרים השלמים:
$0,\pm1,\pm2,\cdots$

אף על פי שמוגדרות בה פעולות חיבור וכפל (ולפעמים גם חיסור וחילוק) כי שורש המשוואה הוא:

$\frac{4\pm\sqrt{16-16}}{8}=\frac{1}{2}$ שורש יחיד והוא אינו שלם!

את המשוואה ניתן לפתור "מעל" המספרים הרציונליים.

2. יש משוואות ריבועיות שלא נוכל לפתור גם כאשר כל פעולות החשבון מוגדרות בה משום שאין שורש ריבועי לכל מספר.

למשל:

$x^2-2=0$ לא ניתנת לפתרון בקבוצת המספרים הרציונליים כי שורשים: $\pm\sqrt{2}$ אינם רציונליים.

יש לו פתרונות בקבוצת המספרים הממשיים.

$x^2+16=0$ לא ניתנת לפתרון בקבוצת המספרים הממשיים כי שורשים: $\pm 4i$ אינם ממשיים.

יש לו פתרונות בקבוצת המספרים המרוכבים.

נשים לבי כי קבוצות המספרים שהזכרנו עד כה מקיימים: $Z\subset Q\subset R\subset C$.

בעצם מספיק לקחת את קבוצת המספרים: $\left\{a+b\sqrt{2}\mid a,b\in Q\right\}$ נכדי לפתור בה את המשוואה

$x^2-2=0$ במקום את כל קבוצת המספרים הממשיים. מסתבר שהסתכלות כזאת חשובה ומרכזית.

נגדיר קבוצת אברים (מבנה אלגברי) שרצוי שנעבוד איתו: שדה.

<u>האכסיומות של שדה</u>

קבוצה F היא שדה אם מוגדרות עליה שתי פעולות בינריות, חיבור וכפל, כך שהיא סגורה תחת הפעולות ולכל a, b, c ב- F.

שם	חיבור	כפל
קומוטטיביות (חילוף)	$a+b=b+a$	$ab=ba$
אסוציאטיביות (צרוף)	$(a+b)+c=a+(b+c)$	$(ab)c=a(bc)$
קיום אבר נייטרלי	$a+0=a=0+a$	$a\cdot 1=a=1\cdot a$
קיום הופכיים	$a+(-a)=0=(-a)+a$	$aa^{-1}=1=a^{-1}a$ if $a\neq 0$

אכסיומה המקשרת בין כפל וחיבור

שם	
דיסטריבוטיביות (פילוג)	$a(b+c)=ab+ac$, $(a+b)c=ac+bc$

ומוסיפים גם את האכסיומה: $1\neq 0$

דוגמאות:

Q, R, C אך לא **N, Z**.

גם: $Q\left(\sqrt{2}\right)=\left\{a+b\sqrt{2}\,\middle|\, a,b\in Q\right\}$ שמוכלת בקבוצת המספרים הממשיים הוא שדה!

בדיקה חלקית של תכונות:

עבור אבר שונה מ-0 יש אבר הופכי בקבוצה כי:

$$\left(a+b\sqrt{2}\right)^{-1}=\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\left(\frac{a}{a^2-2b^2}\right)-\left(\frac{b}{a^2-2b^2}\right)\sqrt{2}$$

שתי הערות:

החישוב נעשה בקבוצת הממשיים שם כל הפעולות מוגדרות.

יש לציין כי אם $a+b\sqrt{2}\neq 0$ הרי גם $a^2-2b^2\neq 0$ כאשר המקדמים הם רציונליים.

כאמור קודם, מעל השדה הזה ניתן לפתור את המשוואה $x^2-2=0$ ולמעשה נראה בהמשך שזהו השדה הקטן ביותר שמכיל את שדה הרציונליים שמעליו ניתן לפתור אותה.

<u>הברקה נוספת של Galois:</u> ההתכלות בתכונות שורשי המשוואה.

נסתכל במשוואה הריבועית $ax^2+bx+c=0,\quad a\neq 0$. אם שורשיו הם x_1, x_2 אז:

$$ax^2+bx+c=a(x-x_1)(x-x_2)=a\left(x^2-(x_1+x_2)+x_1x_2\right)$$

נסתכל בביטויים: x_1+x_2 , x_1x_2.

אם נבצע תמורה על השורשים: $x_1\leftrightarrow x_2$ נקבל: x_2+x_1 ו- x_2x_1. אך בגלל חוקי השדה הם שווים לביטויים המקוריים – כלומר יש לביטויים הללו תוכנות סימטריות.

כעת נסתכל על פולינום ממעלה שלישית ששורשיו x_1, x_2, x_3:

$$ax^3+bx^2+cx+d=a(x-x_1)(x-x_2)(x-x_3)=a\left(x^3-x^2(x_1+x_2+x_3)+x(x_1x_2+x_2x_3+x_1x_3)-x_1x_2x_3\right)$$

שוב הביטויים שקיבלנו בשורשים כמקדמים אינם משתנים תחת תמורות על x_1, x_2, x_3:

למשל החלפת: $x_1\leftrightarrow x_2$ תתן:

$$x_1+x_2+x_3\leftrightarrow x_2+x_1+x_3$$

$$x_1x_2+x_2x_3+x_1x_3\leftrightarrow x_2x_1+x_1x_3+x_2x_3$$

$$x_1x_2x_3\leftrightarrow x_2x_1x_3$$

שוב – חוקי השדה מבטיחים שאלה שווים למקוריים.

מסתבר אם כך שחשוב להתסכל על קבוצות התמורות על שורשים ותכנותיהן.

זוהי דוגמא של מבנה אלגברי נוסף: החבורה, אליה נגיע בהמשך:

<u>האכסיומות של חבורה</u>

קבוצה G היא חבורה חיבורית אם מוגדרות עליה פעולה בינרית, חיבור, כך שהיא סגורה תחת הפעולות ולכל a, b, c ב- G .

שם	חיבור	כפל
קומוטטיביות (חילוף)		
אסוציאטיביות (צרוף)	$(a+b)+c=a+(b+c)$	
קיום אבר נייטרלי	$a+0=a=0+a$	
קיום הופכיים	$a+(-a)=0=(-a)+a$	

קבוצה G היא חבורה כפלית אם מוגדרות עליה פעולה בינרית,כפל, כך שהיא סגורה תחת הפעולות ולכל a, b, c ב- G .

שם	חיבור	כפל
קומוטטיביות (חילוף)		
אסוציאטיביות (צרוף)		$(a\,b)\,c=a\,(b\,c)$
קיום אבר נייטרלי		$a\cdot 1=a=1\cdot a$
קיום הופכיים		$a\cdot a^{-1}=1=a^{-1}\cdot a$

האכסיומות של חוג

קבוצה R היא חוג אם מוגדרות עליה שתי פעולות בינריות, חיבור וכפל, כך שהיא סגורה תחת הפעולות ולכל a, b, c ב- R .

שם	חיבור	כפל
קומוטטיביות (חילוף)	$a+b=b+a$	
אסוציאטיביות (צרוף)	$(a+b)+c=a+(b+c)$	$(ab)c=a(bc)$
קיום אבר נייטרלי	$a+0=a=0+a$	$a\cdot 1=a=1\cdot a$
קיום הופכיים	$a+(-a)=0=(-a)+a$	

אכסיומה המקשרת בין כפל וחיבור

דיסטריבוטיביות (פילוג)	$a(b+c)=ab+ac$, $(a+b)c=ac+bc$

ומוסיפים גם את האכסיומה : $0\neq 1$

האכסיומות של מרחב וקטורי

קבוצה V היא מרחב וקטורי מעל השדה F, אם היא חבורה חיבורית אבלית ומוגדרת פעולת בין אברי V ואברי השדה, כפל בסקלר שתוצאתה אבר ב- V שמקיימת שלכל a,b ב-F ו-v,w ב-V :

$a(v+w)=av+aw$
$(a+b)v=av+bv$
$(ab)v=a(bv)$
$1_F\cdot v=v$

יש לציין כי ההגדרות הנ"ל בנות בערך 150 שנה.

נתן דוגמאות ראשונית בלבד :

חבורות : Z כחבורה חיבורית, כל שדה ביחס לחיבור, כל שדה ללא אבר האפס – חבורה כפלית, $\{\pm 1\}$ ביחס לכפל , $\{\pm 1,\pm i\}$ - עם לוח כפל, חבורת התמורות S_3 ביחס לפעולת ההרכבה, חבורת הסיבובים של המישור דרך זוית כלשהי.

<u>חוגים</u>: Z, כל שדה, $Z \times Z$ וכל מכפלה קרטזית של שני חוגים הוא חוג.
$Z[x]$, $Z[x, y]$, $F[x]$ כאשר F הוא שדה.

<u>מרחבים וקטוריים</u>: F^n, R^n, R^2 , מרחב הפונקציות הממשיות.

<u>דוגמאות של שדות סופיים</u>: Z_2, Z_3, Z_5, Z_p אך לא Z_4, Z_6 שהם חוגים אך לא שדות - ולתת את המשפט להכליל.

להראות שבכל שדה: $0 \cdot a = 0$ $-1 \cdot a = -a$

ואחר-כך בניית שדה כלשהו בן 3 אברים (בניית לוח כפל תחילה, ואחר-כך חיבור...):

בניית שדה בן 4 אברים – בתרגיל בלבד!

<u>תת-מבנים</u>:

ראינו כי $Q(\sqrt{2}) \subset R$ ושניהם שדות ביחס לפעולות החשבון ב-R.

הגדרה:
אם F שדה, $K \subset F$ נקרא תת-שדה אם K שדה ביחס לאותן הפעולות שמוגדרות ב-F.

הערה חשובה:
במקרה זה אבר ה-0 ואבר ה-1 בתת-שדה יהיו אבר ה-0 ואבר ה-1 בשדה הגדול.

להוכיח ביחס לאבר ה-0.

באופן דומה: ההופכי והנגדי של אברים בתת-שדה יהיו זהים לאלה שבשה הגדול.

לכן **<u>טענה</u>**: אם F שדה, ואם $K \subset F$ תת-קבוצה לא ריקה שסגורה תחת חיבור וכפל, מכילה את 0 ו-1 ולכל $a \in K$ קיים שגם: $-a \in K$ ואם $a \neq 0$ גם $a^{-1} \in K$ - אז K הוא תת-שדה של F.

באופן דומה נגדיר:
תת-חוג (יש <u>לדרוש</u> גם כי אבר היחידה תת-חוג יהיה אבר היחידה של החוג הגדול!)
תת-חבורה
תת-מרחב.

דוגמאות:
$Z[x^2] \subset Z[x], \quad S_3 \subset S_5, \quad \{\pm 1, \pm i\} \subset C^*,$
תת-מרחב של R^3 ועוד.

2. Ring Theory: Ideals, homomorphisms, quotient structures. Detailed examples.

The most important kind of substructure for a ring is not a subring but an ideal:

Ideal:

Definition: Let R be a ring. A subset I of R is an **ideal** if it is an additive subgroup such that: $ax, xa \in I$ for all a in R and x in I.

Examples:

1. In P[x]:
   - set of polynomials with 0 constant term = x P[x]
   - set of polynomials divisible by x- 3 (notation: <x – 3>)
   - trivial ideals.

   But not: set of polynomials with rational coefficients

   And not: set of pynomials with integer constant term.
2. In Z:
   - $2Z,,nZ$
   - but not the set of odd integers.

Note: A field has no nontrivial ideals.

Claim: For in ideal I in a ring R: $1 \in I \Leftrightarrow I = R$

Definition: Let R be a ring. A subset I of R is a **left (right) ideal** if it is an additive subgroup such that: $ax \in R$ ($xa \in R$) for all a in R and x in I.

Clearly in a commutative ring, all left/right ideals are ideals.

Example: $R = M_2(Q)$

Recall – matrix multiplication.

$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \, a,b \in Q \right\}$ is a right ideal in R but not as left ideal.

(Check multiplication with a matrix of 1s!)

Quotient rings:

Definition: Let R be a ring, I an ideal.

For an element a in R, we define the **coset** of I determined by a to be the set:

$I + a = \{x + a \mid x \in R\}$.

Let $R/I = \{I + a \mid a \in R\} = R(\mathrm{mod}\, I)$.

Note that this is a set of sets.

We note first that:
$I+a=I+b \Leftrightarrow a-b\in I$

Claim: Cosets are equal or disjoint.
In other words: $I+a\cap I+b\neq\phi \Rightarrow I+a=I+b$
With proof.

We conclude that *R*/*I* in fact is a partition of *R*. Note of course that every element in the ring is in some coset!

Quotient rings:
We define operations on *R*/*I* :

Addition: $(I+a)+(I+b)=I+(a+b)$
Multiplication: $(I+a)\cdot(I+b)=I+(a\cdot b)$

We claim that with respect to these operations, *R*/*I* is a ring.
We need to show first that the definitions are independent of the choice of coset representatives.
Then examples to verify the axioms.

Examples of quotient rings:
$Z/3Z,\quad Z/4Z,\quad R[x]/<x-3>,\quad R[x]/<(x^2-x-2)>$ (in detail, note here that $(J+(x+1))(J+(x-2))=J,\quad J=<(x^2-x-2)>$.)

Homomorphisms and isomorphisms of rings, kernel and image.

Definition: Let *R* and *S* be rings. $\varphi: R\to S$ is a ring homomorphism if it is additive and multiplicative and satisfies: $\varphi(1)=1$.

Examples:
- Inclusion function of *Q*[*x*] in *R*[*x*].
- $\varphi: Z\to M_n(Z)$ defined by: $\varphi(n)=\begin{pmatrix} n & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & n \end{pmatrix}$ but not $\varphi(n)=\begin{pmatrix} n & \cdots & 0 \\ 0 & \ddots & 0 \\ 0 & \cdots & 0 \end{pmatrix}$.
- $\varphi: Z\to Z/6Z,\quad \varphi(n)=n+6Z.$

$\varphi: Q[x] \to Q(\sqrt{3}), \quad \varphi(g(x)) = g(\sqrt{3})$.

- $\varphi: R[x] \to C, \quad \varphi(g(x)) = g(i)$.

$\varphi: Z \times Z \to Z, \quad \varphi(x, y) = x$.

Definitions: Let R and S be rings. $\varphi: R \to S$ a homomorphism:

$\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$

$\mathrm{Im}\varphi = \{\varphi(a) \mid a \in R\}$

Claim: The kernel of a homomorphism is an ideal in R.
Claim: The kernel of a homomorphism is trivial if and only if the homomorphism is one-to-one.

Note that the Image of a homomorphism is an additive subgroup of S.

A homomorphism that is 1-1 and onto S is called an isomorphism.
In such a case we write: $R \cong S$.

The Homomorphism theorem for rings.
Let R and S be rings. $\varphi: R \to S$ a homomorphism onto S. Then $R/\ker\varphi \cong S$.

Example: $R[x]/<x^2+1> \cong C$ as $<x^2+1>$ is the kernel of the homomorphism we had above.

3. Commutative rings and detailed examples, Principal ideal domains, Special commutative rings, polynomial rings. Unique factorization domains

Special properties of the ring of integers:

- **The Euclidean property:**

For any integers *a* and *b* there exist integers *q* and *r* such that:

$a = bq + r, \quad 0 \le r < |b|$

Example: 17 = 5*3 + 2

- **Every ideal of *Z* is principal** – proof in assignment 2.

- **Unique factorization into primes in *Z*.**

Every integer has a factorization into primes. The factorization is unique up to order of factors and signs.

Example: 30 = 3*5*2 = (-5)*(-3)*2 = (-2)*5*(-3) etc.

- **Every two nonzero integers have a greatest common divisor, and it is unique up to a sign.**

Note: By "greatest" common divisor we mean that if d is a gcd of *a* and *b* then for any *d'* dividing *a* and *b* we have *d'* dividing *d*.

All these properties can be generalized.
We shall start with some definitions:

Commutative Domains.

Definition: A ring *R* is a commutative domain if it is commutative and for and *a* and *b*
in *R:* $ab = 0 \Rightarrow a = o \quad or \quad b = 0.$

Examples: *Z*, *Z*[*x*], but not $Z \times Z, \; Z/_{6Z}$.

Primes and irreducibles in rings.

Definition: For a ring *R*, *p* in *R* is a prime element if it is nonzero, not invertible
and if for any *a*, *b* in *R:* $p|ab \Rightarrow p|a \quad or \quad p|b.$

Definition: For a ring *R*, *x* in *R* is an irreducible element if it is nonzero, not invertible
and if for *a*, *b* in *R:* $x = ab \Rightarrow a \quad or \quad b$ is invertible.

Examples.

Prime numbers in *Z* are prime elements and irreducibles.
Irreducible polynomials over a field are both prime and irreducible.

Claim: Prime elements in a domain are irreducible.

Proof: Let *p* be a prime and assume $p = ab$.
Then $p|ab$ so we have $p|a \quad or \quad p|b$. Wlog (=Without loss of generality) we assume
$p|a$. So there exists some element *u* in the the ring such that $pu = a$.

This gives us: $pub = ab = p$ and so $p(ub - 1) = 0$.
Since *R* is a domain this implies that $ub = 1$ (as *p* is nonzero), so that the factorization of *p* is trivial.

The converse is not true!
Example: $Z[\sqrt{-5}]$ has irreducibles that are not prime, and does not have unique factorization to irreducibles.

Proof: We claim that 2 is irreducible but not prime.

We first show that 2 is irreducible.
Suppose $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ where *a,b,c,d* integers, then since this ring is a subring of the field of complex numbers, recalling that for complex numbers $x + iy$ we have: $\|x+iy\|^2 = x^2 + y^2$, and that the complex norm is multiplicative, we get: $4 = (a^2 + 5b^2)(c^2 + 5d^2)$.This yields either: $(a^2 + 5b^2) = 2 = (c^2 + 5d^2)$ which is impossible, or one of the factors equals 1 and the other 4. Wlog if $(a^2 + 5b^2) = 1$ then $a = \pm 1, \quad b = 0$ and then $a + b\sqrt{-5}$ is invertible in the ring.

We now show that 2 is not prime.
In the ring we have: $6 = 3 \cdot 2 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ so that $2 | (1 + \sqrt{-5})(1 - \sqrt{-5})$.
However it is easy to see that 2 does not divide $1 \pm \sqrt{-5}$ in the ring, and so is not prime.

Generalizing the special properties of Z:

Principal ideal domains – definition.
Examples: *Z* but $Z[x]$ is not a PID.
Claim: The ring of polynomials over field is a PID – proof in assignment 2.

We say 2 elements are <u>associates</u> if they are equal up to multiplication by a unit (= an invertible element)
e.g. 2 and (-2) are associates in *Z.*

Unique factorization domains
<u>Definition</u>: A commutative domain is a <u>unique factorization domain</u> (= UFD)if every nonzero, noninvertible element can be decomposed as a product of primes, and this decomposition is unique up to order of the factors and associates.

Examples:
Z, *Z*[*x*], *F*[*x*] but not $Z\left(\sqrt{-5}\right)$.

Definition of a greatest common divisor in a ring.

Claim: In a PID every two nonzero elements have a gcd.
Proof:
Let *a*, *b* be nonzero elements of *R* . Look at: *I =Ra + Rb*
It is an ideal and so principal. So there is some element *d* such that *Rd =Ra + Rb*.
We claim that it is a *d*=(*a*,*b*).
Since $a \in Rd$ so $d|a$. Similarly we get $d|b$.
It remains to show the maximality of *d.*
Suppose we have *d'* such that $d'|a, b$ then $Ra, Rb \subseteq Rd'$ and so also $Rd = Ra + Rb \subseteq Rd'$ which implies that $d'|d$

As a corollary we obtain:
<u>Bezout's Theorem</u>
In a PID, if *a*,*b* nonzero non-units such that *d*=(*a*,*b*) then there exist *u*, *v* in the rin g such that *au + bv = d.*

As a corollary from Bezout's theorem we also have that *Z/pZ* is a field for prime *p.*
(From Assignment 3, question 2 we get a different proof of this fact!)

Claim: In a PID an element is prime element if and only if it is irreducible.
Proof: omitted.

Claim: Every PID is a UFD.
Proof: omitted.
Note that this implies that $Z\left(\sqrt{-5}\right)$ is not a PID.

Converse is not true: Example: $Z[x]$ is a UFD but not a PID.

Claim: In a UFD every two nonzero elements have a gcd.
Proof by calculation of the gcd (and lcm) in a UFD using the factorizations:
If $a = \prod p_i^{r_i}$, $b = \prod p_i^{s_i}$ we can calculate directly:
$(a,b) = \prod p_i^{\min\{r_i,s_i\}}$, $[a,b] = \prod p_i^{\max\{r_i,s_i\}}$

Note:
In Z we have 3 different ways of finding the $(a,b)=d$
1. Using the fact that $Za + Zb = Zd$.
2. Using prime factorizations as above.
3. Using the Euclidean algorithm.

4. Chinese Remainder Theorem and RSA.

Chinese Remainder Theorem:

Historical introduction

Chinese Remainder Theorem

The following problem was posed by Sunzi [Sun Tsu](4th century AD) in the book Sunzi Suanjing:

There are certain things whose number is unknown.

Repeatedly divided by 3, the remainder is 2;
by 5 the remainder is 3;
and by 7 the remainder is 2.

What will be the number?

The answer is hidden in the following song:

孫子歌 Sunzi Ge

三人同行七十里
五樹梅花廿一枝
七子團圓正月半
一百零五轉回起

Solution:

Recall: $a \equiv b(\mathrm{mod}\, n) \Leftrightarrow n \mid a-b \Leftrightarrow a+nZ = b+nZ$

x must be 2(mod3), 3(mod5) and 2(mod7).

We can take x = 23 for example.

Statement of the CRT for *Z*.

Let $n_1, \cdots n_k$ be mutually prime positive integers. Then given any integers $r_1, \cdots r_k$ there exists an integer *x* such that: $x \equiv r_i \pmod{n_i}$ for all *i*.

Examples and counterexamples.

If: $n_1 = 3, n_2 = 5, n_3 = 14$
$r_1 = 4, r_2 = 0, r_3 = -3,$

Then we want *x* to satisfy: $x \equiv 4 \pmod 3$
$x \equiv 0 \pmod 5$
$x \equiv -3 \equiv 11 \pmod{14}$

So that *x* = 25 is a solution.
Note that the solution is not unique.
In fact $x = 25 + 3 \cdot 5 \cdot 14k$ is a solution for any integer *k*.

How do we solve?
It is best to look at the congruence for the largest of the n_i (in our case $x \equiv 11 \pmod{14}$ and construct a sequence of solutions:
11, 25, 39, …
And check which satisfy the other congruences. First find one which satisfies the second congruence $x \equiv 0 \pmod 5$, and then continue as necessary in the arithmetic sequence with difference $n_2 n_3 = 70$ and so on.

Example: There is no solution to the congruences: $x \equiv 4 \pmod 9$
$x \equiv 0 \pmod 3$

Oystein Ore mentions a puzzle with a dramatic element from *Brahma-Sphuta-Siddhanta* (Brahma's Correct System) by Brahmagupta (born 598 AD):

An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

We have to solve:

$$x \equiv 1(\text{mod } 2)$$
$$x \equiv 1(\text{mod } 3)$$
$$x \equiv 1(\text{mod } 4)$$
$$x \equiv 1(\text{mod } 5)$$
$$x \equiv 1(\text{mod } 6)$$
$$x \equiv 0(\text{mod } 7)$$

The smallest solution here is 301!

Statement of the CRT for an arbitrary commutative ring *R*.

Let $I_1,\cdots I_k$ be mutually prime ideals, that is: $I_j + I_k = R$ for $i \neq j$.
Then given arbitrary elements $a_1,\cdots a_k \in R$ there exists an $x \in R$ such that for all *j*: $x + I_j = a_j + I_j$ (or in other words: $x \equiv a_j (\text{mod } I_j)$ for all *j*).

We first show how the CRT for *Z* follows from the general theorem:

Proof:
Define $I_j = n_j Z$ then as we have $n_1,\cdots n_k$ be mutually prime we get $I_i + I_j = Z, \quad i \neq j$. Therefore the ideals satisfy the requirements of the Theorem and the conclusion holds: $x + n_j Z = a_j + n_j Z$, in other words: $x \equiv a_j (\text{mod } n_j)$ for all *j*.

We prove the theorem only for 2 ideals in an arbitrary commutative ring:

Since $I_1 + I_2 = R$ we have $b_j \in I_j$ such that $b_1 + b_2 = 1$.
Let $x = a_2 b_1 + a_1 b_2$. Then we have:
$x + I_1 = a_2 b_1 + a_1 b_2 + I_1 = a_1 b_2 + I_1$ as $a_2 b_1 \in I_1$.
$x + I_1 = a_1 b_2 + I_1 = a_1(1 - b_1) + I_1 = a_1 - a_1 b_1 + I_1 = a_1 + I_1$
as $a_2 b_1 \in I_1$.
Simlarly we get: $x + I_2 = a_2 + I_2$.

The proof in the general case, which we shall skip, is actually proved directly using the case for *n* = 2.

Example:

Calculation of an element satisfying simultaneous congruencies in Z:
Let us find an integer x such that:

$$x \equiv 2(\mathrm{mod}\,3)$$
$$x \equiv 3(\mathrm{mod}\,5)$$
$$x \equiv 2(\mathrm{mod}\,7)$$

We start with, say 2(mod7), and construct a sequence of elements satisfying it:
2, 9, 16, 23, 30, 37, 44, 51, 58, 65, 72, 72, 79, 86, 93, 100, 107, 114, 121, 128, …

The red elements satisfy that they equal also 2(mod3)
From these we choose the elements (underlined) satisfying also that they equal 3(mod5).
Here we have 23 and 128 that satisfy all 3 congruences.

Corollary from the CRT:

Let $m = \prod_{i=1}^{k} p_i^{r_i}$ where p_i are distinct prime numbers. Then

$$Z/nZ \cong \prod_{i=1}^{k}\left(Z/p_i^{r_i} Z \right)$$

Proof:

We define $f : Z \to \prod_{i=1}^{k}\left(Z/p_i^{r_i} Z \right)$ as follows: $f(a) = \left(a + p_1^{r_1} Z, \cdots, a + p_k^{r_k} Z\right)$.

Then f is a homomorphism of rings as:

$$a + b + p_i^{r_i} Z = a + p_i^{r_i} Z + b + p_i^{r_i} Z$$
$$ab + p_i^{r_i} Z = \left(a + p_i^{r_i} Z\right)\left(b + p_i^{r_i} Z\right)$$
$$f(1) = \left(1 + p_1^{r_1} Z, \cdots, 1 + p_k^{r_k} Z\right)$$

What is the kernel of f?

$f(a) = \left(0 + p_1^{r_1} Z, \cdots, 0 + p_k^{r_k} Z\right) \Leftrightarrow a \equiv 0(\mathrm{mod}\, p_i^{r_i})$ for all i.

This holds if and only if $a \equiv 0(\mathrm{mod}\, n)$.

Hence $\ker f = nZ$.

Our theorem will then follow from the homomorphism theorem if we show that the map f is onto $\prod_{i=1}^{k}\left(Z/p_i^{r_i} Z \right)$.

Let $b_1, \cdots b_k$ be arbitrary integers. We need to find some x such that for all i.

$f(x) = \left(b_1 + p_1^{r_1} Z, \cdots, b_k + p_k^{r_k} Z\right)$ but this means that $x \equiv 0(\mathrm{mod}\, p_i^{r_i})$ for all i.

Such an element is guaranteed by the CRT.

Hence: $Z/nZ \cong \prod_{i=1}^{k}\left(Z/p_i^{r_i} Z \right)$.

Note: The CRT is actually equivalent to this isomorphism.

Corollary: For $(k,l)=1$ we have $Z/klZ \cong Z/kZ \times Z/lZ$.

As an application of the CRT we look at:

RSA public key cryptography:

Introduction.
In 1976, Rivest, Shamir and Adelman published the following method of public key cryptography.
The basic idea:
The encryption method is known to the public.
The decoding method is secret.

Description of the encoding and decoding.

We start with 2 "very large" primes (at least 1000 digits long): p_1, p_2
We note here that the largest prime known so far has 12.9 million digits!
Define: $d = p_1 p_2$.
The factorization of *d* is considered impossible in practical terms without knowing the primes.
Example: In 2005 it took 5 months to factor on huge computers a number with 193 digits.
We define: $e=(p_1-1)(p_2-1)$ and choose a "large" integer *r* prime to *e*.
There exists an integer *s* such that $sr \equiv 1 (\mathrm{mod}\, e)$ (for instance, by Bezout).

We publish *d* and *r*.
(the other numbers remain secret.)

Encryption: We take message *a* which is a sequence, say of binary digits.
We limit our messages to be smaller than *d*.
Encrypt this as $b \equiv a^r (\mathrm{mod}\, d)$.
Decoding:
We calculate $b^s (\mathrm{mod}\, d)$ and claim that it equals *a*!

Proof that it works using previous corollary.
$Z/dZ \cong Z/p_1Z \times Z/p_2Z$ and under the isomorphism we constructed:
$b+ \leftrightarrow (b+p_1Z, b+p_2Z)$ so that $b^s \leftrightarrow (b^s+p_1Z, b^s+p_2Z) = (a^{rs}+p_1Z, a^{rs}+p_2Z)$
By Bezout we have integers *t, r:* $te+rs=1$.

Case 1: *a* is prime to *d*.

By Fermat's Little Theorem (that we shall prove later):

$a^{(p_1-1)} \equiv 1 (\text{mod } p_1), \quad a^{(p_2-1)} \equiv 1 (\text{mod } p_2)$, so $a^e = a^{(p_1-1)(p_2-1)} \equiv 1 (\text{mod } p_i)$

Then we shall have: $a = a^{te+rs} = a^{te} \cdot a^{rs} \equiv 1 \cdot a^{rs} \equiv b^s (\text{mod } p_i)$ giving

$a \equiv b^s (\text{mod } d)$ using our isomorphism.

Case 2: *a* is not prime to *d*.

In this case, one of the primes divides *a*, and the other does not.

We omit the details but assuming wlog that $a \equiv 0 (\text{mod } p_1)$ we obtain in a similar manner to Case 1 that

$b^s + dZ \leftrightarrow (0 + p_1 Z, a + p_2 Z) \leftrightarrow a + dZ$ and as this correspondence is an isomorphism we have again $a \equiv b^s (\text{mod } d)$.

5. Group theory: Introduction, subgroups, quotient groups

Read Mario Livio pp 45 – 50.
We shall assume from now that operation in our group is multiplication.

Cosets in groups: If *H* is a subgroup of a group *G*, *a* an element of *G*, then the set *Ha* is a right coset of *H* in *G*.

As in rings, cosets of groups are disjoint or equal.

Example: We examine S_n in some detail.

- Cycle notation:

We take for example *n* = 7.

Let $\sigma = \begin{pmatrix} 1234567 \\ 3156472 \end{pmatrix}$

We note that we have: $1 \to 3 \to 5 \to 4 \to 6 \to 7 \to 2 \to 1$.
This is a cycle and we write it as (1354672).
Any permutation can be decomposed as a product of disjoint cycles.

For example: $\tau = \begin{pmatrix} 1234567 \\ 3512476 \end{pmatrix} = (13)(254)(67)$

Note that the order of the disjoint cycles will not matter as they commute!

This notation makes multiplying easier and is more convenient in general.

We denote the action of a permutation on an index as follows: $\sigma(i) = i^{\sigma}$.
This fits in with our reading the multiplication from the left was we then have: $i^{\sigma\tau} = \left(i^{\sigma}\right)^{\tau}$ i.e. the left-most permutation acts first.

For example:

(135)(214) = (13542)
(13)(123) = (1)(23) = (23)

Cosets in S_3:

We can now write $S_3 = \{1, (12), (13), (23), (123), (132)\}$ and take the subgroup $H = \{1, (12)\}$.
The right cosets will be:

$H = \{1, (12)\}$
$H(13) = \{(13), (12)(13)\} = \{(13), (123)\}$
$H(23) = \{(23), (12)(23)\} = \{(23), (132)\}$

Odd and even permutations and their properties:

Definition: A permutation is **odd** if the number of pairs of indices whose order is switched is odd.

A permutation is **even** if the number of pairs of indices whose order is switched is even.

Example: $\sigma = \begin{pmatrix} 1234567 \\ 3156472 \end{pmatrix}$ By connecting equal indices in both rows, we can count the number of switched orders. For instance, this is an even permutation.

An easier way of checking is by using the cycle decomposition as we have that:

Cycles of odd length are even, cycles of even length are odd.

Example: Look at (1345). Connecting the equal indices in the 2-row representation and see it is odd. $(1345) = \begin{pmatrix} 12345 \\ 32451 \end{pmatrix}$

Moreover:

- the product of 2 even permutations is even.
- the product of 2 odd permutations is odd.
- the product of an even permutation with an odd one is odd.

Hence we also have that set of all even permutations, A_n, is a subgroup of S_n.

Definition:

A subgroup N of a group G is normal if for any $a \in G : Na = aN.$

We denote this : $N \lhd G$.

We note that $Na = aN \Leftrightarrow a^{-1}Na = N.$

Note that this is an equality of sets – and does not imply that elements of N commute with all the elements in G.

Examples:

In an abelian group every subgroup is normal.

The subgroup H above is not normal, however A_n is a normal subgroup of S_n.

More examples from Mario Livio's book:

Taking a pair of reversible, symmetric pants, we look at the group of symmetries of the pants.

That is, defining σ to be the operation reversing left and right (flipping the pants over), and τ to be the operation that turns the pants inside-out, we have a group of 4 operations: $G = \{1, \sigma, \tau, \sigma\tau = \tau\sigma\}$.

S. Loyd's 14-15 puzzle:

S. Loyd (1841 – 1911) offered a prize to anyone who could find a series of moves that could reverse 15 and 14 only in the puzzle:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Where one can slide squares into the empty slot up, down or sideways.
For instance, the following sequence of moves into the empty slot:
15, 14, 13, 9, 5, 6, 7, 8, 12, 15
will give us the following :

1	2	3	4
6	7	8	12
5	10	11	15
9	13	14	

Corresponding to the permutation: (5 6 7 8 12 15 14 13 9)
1, 2, 3, 4, 10 and 11 and the empty space remain as they were. This is an even permutation.
The group defined by the puzzle is the group of all possible permutations of
1,2,….15, and an empty space that we can get.

We can prove that every possible permutation we obtain in this way is even.
Hence the permutation that switches only 14 and 15 cannot be obtained as it is odd!

Rubik's cube (1974)

The group of the cube is the group of all possible rotations of the cube.
For example for $i = 1,3$ we can denote by R_i a rotation of layer i (x-y plane, around
the z-axis) through 90 degrees clockwise.
Its inverse will be the rotation of layer i anticlockwise.
Similarly for $i = 1,3$ we denote by S_i a rotation of column i (y-z plane, around the

x-axis) through 90 degrees clockwise, and for *i* = 1,3 we denote by T_i a rotation of
column *i* (*x*-*z* plane, around the *y*-axis) through 90 degrees clockwise.

These 6 elements generate all the elements of the group.

For example note that: R_1S_1 does not equal to S_1R_1 so the group is not abelian.

It turns out that the order of the group is 43,252,003,274,489,856,000.

Index of a subgroup:

Definition: The **index of a subgroup** H in a group G is the cardinality of the set of cosets.
Note that the cardinality is the same for right and left cosets.
We denote the index $|G:H|$

Lagrange's Theorem
If H is a subgroup of a finite group G, then its order divides the order of the group.

The proof follows from the fact that every coset contains the same number of elements which is the number of elements in H, hence:
$|G| = |H| \cdot |G:H|$.
Note that this implies that the index divides the order of the group as well!

Corollary: If a is an element of a finite group then its order divides the order of the group.

Quotient groups.
For a normal subgroup N of a group G we define a product on the set of cosets G/N as follows: $Na \cdot Nb = Nab$.
This is well-defined, as if $Na = Na'$, $Nb = Nb'$ then we have $Nab = Na'b'$
(Check! - here we have to use the normality of N)and gives us a group (the quotient group).

6. Homomorphisms of groups, simple groups, cyclic groups, finite groups: The Sylow's theorems.

Homomorphisms of groups.

Definition: $\varphi: G \to H$ is a group homomorphism if
for $a,b \in G: \varphi(ab) = \varphi(a)\varphi(b)$.
Note: This implies also that $\varphi(1) = 1$.
As with rings we define the kernel and image of a homomorphism.

Claim:
The kernel and image of a group homomorphisms are both subgroups.
The kernel is a normal subgroup.

The homomorphism theorem for groups.
Let $\varphi: G \to H$ is a group homomorphism onto *H*. Then $G/\ker\varphi \cong H$.

Examples:

1. *GL(n,F)*, the group of matrices over *F* of nonzero determinant.

   We map each matrix to its determinant.
   This maps the group onto *F**.
   The kernel is *SL(n,F)*.

2. S_n.

   We map each even permutation to 1, and each odd permutation to -1.
   The kernel of the homomorphism is A_n.

A group is called **simple** if it has no nontrivial normal subgroups.

Claim:
A nontrivial finite abelian group is simple if and only if it is of prime order.

Proof: Use Lagrange's theorem.

Example: A_n is simple for all *n* greater or equal to 5.

Cyclic groups

Definition: The cyclic group $< a >$ generated by a group element *a* is the smallest subgroup containing that element.
In fact: $< a >= \{a^k \mid k \in Z\}$.
Examples:

Note that in *Z* as an additive group, 1 is a generator.

Claim: Every subgroup of a cyclic group is cyclic.
Proof: in the assignment.

Note: Also quotients of cyclic groups will be cyclic.

Claim:
Suppose *G* is cyclic of order *n* and *m* divides *n*, the there exists a unique subgroup of order *m*.

Proof:
We write $n = md$.
Suppose $G =< a >$. Then it is easy to see that $< a^d >$ is cyclic of order *d*.
Now suppose that $H =< b >$ is a subgroup of order *m*.
There exists some integer *k* such that $a^k = b$. Wlog we assume *k* is positive.
$a^{km} = b^m = 1$ Hence $md = n \mid km$ and so $d \mid k$. That means that *b* is a power of a^d
And so $H \subseteq < a^d >$ but as both sets are of order *m*, they must then be equal.

Conjugacy classes.

Definition: *x* and *y* are conjugate in a group *G* if $\exists a \in G: \quad y = a^{-1}xa$.

Note that conjugacy is an equivalence relation.
The classes are called conjugacy classes.

Examples:

1. *GL*(2,*C*)
In a group of square matrices, conjgate matrices are "similar".
We know for instance that over the complex numbers, every matrix is similar to a matrix in Jordan form, so that in the group *GL*(2,*C*) the possible Jordan forms are:

$\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$, $\alpha,\beta\neq 0$ **or** $\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}$, $\alpha\neq 0$

This means that the conjugacy classes with a representative which is a diagonal matrix of the first type or a non-diagonalisable matrix of the second type.

2. S_n

It turns out that 2 permutations in S_n are conjugate if and only they have the same cycle structure when decomposed as a product of disjoint cycles.
For example we can check that:

$[(124)(37)(695)]^{\sigma}=(123)(48)(375)$ where $\sigma=\begin{pmatrix}123456789\\ 124653897\end{pmatrix}$

Definition: The centre of a group G is the set $Z(G)=\{z\in G \mid zg=gz\ \forall g\in G\}$
It is easy to check that it is a normal (abelian) subgroup.

For a specific element g in a group we define its centralizer:
Definition: The centralizer of a g is the set $C(g)=\{a\in G \mid ag=ga\}$
It is easy to check that it is a subgroup.

It turns out that if G is finite then the number of elements in the conjugacy class $Cl(g)$of an element g is given by $|Cl(g)|=\frac{|G|}{|C(g)|}$

Corollary: $|Cl(g)|$ divides the order of the group.

Definition: For a prime p, a p-group is a group in which all the elements are orders which are powers of p.

Claim: The centre of a nontrivial finite p-group G is nontrivial.

We write the elements of the group as a disjoint union of its conjugacy classes:

$$G=C_1\cup\cdots\cup C_n$$

We then get that:

$$|G|=|C_1|+\cdots|C_n|=\sum_{|C_i|=1}|C_i|+\sum_{|C_i|>1}|C_i|$$

Since we already know that $|C_i|$ divides $|G|$ then we must have $|C_i| \equiv 0 (\text{mod } p)$ if $|C_i| > 1$.

Hence we conclude that:

$$0 \equiv |G| \equiv \sum_{|C_i|=1} |C_i| (\text{mod } p)$$

Note also that $|C_i| = 1$ only for classes whose representative is in the centre of the group. Hence we conclude that the number of such classes is $|Z(G)|$.

In other words: $|Z(G)| \equiv 0 (\text{mod } p)$ meaning that the centre is nontrivial.

The Sylow theorems.

We have seen that in the case of a finite cyclic group, for every number dividing the order of the group we have a unique subgroup of that order. In general this is not true.

For example in S_4 there are 2 non-isomorphic subgroups of order 4:

- the cyclic group generated by (1234)
- the subgroup $\{1, (12)(34), (13)(24), (14)(23)\}$
- and there are cases when there does not exist a subgroup of certain orders which divide the group order.
-

For finite groups and prime divisors of the group order, however, we can guarantee the existence of subgroups of prime power orders. This turns out to be very useful.

The Sylow theorems

Let G be a finite group of order $p^k m$ where p is a prime and $(p, m) = 1$.

Then:

1. G has subgroups of order p^r for every $r \le k$.
   In particular it has a maximal p-subgroup of order p^k called a Sylow p-subgroup.
2. All Sylow p-subgroups are conjugate, and so isomorphic.
3. The number of Sylow p-subgroups $n_p \equiv 1 (\text{mod } p)$.
4. Every p-subgroup is contained in a Sylow p-subgroup.
5. $n_p | m$.

Note: The theorems actually give more information about n_p, but we shall omit it.

Classification of all groups of order 15.

We shall apply the Sylow theorems to classify all groups of order 15. Suppose *G* is of order 15.

By Sylow we have:
$n_3 \mid 5, \quad n_3 \equiv 1 (\mathrm{mod}\, 3)$, hence $n_3 = 1.$
Similarly: $n_5 \mid 3, \quad n_5 \equiv 1 (\mathrm{mod}\, 5)$, hence $n_5 = 1.$
This means that the two Sylow subgroups are unique.
Since any conjugate of a Sylow subgroup is also a Sylow subgroup, this also implies that they are both normal.

Both will be cyclic as 3 and 5 are primes.

If *x* generates the group of order 3 and *y* generates the group of order 5, then as <*y*> is normal we must have $x^{-1}yx = y^t$ for some *t*.

Now we have $x^3 = 1$ so $x^{-3}yx^3 = y$ but
$x^{-3}yx^3 = x^{-2}x^{-1}yx \cdot x^2 = x^{-2}y^t x^2 = x^{-1}\left(x^{-1}y^t x\right)x = x^{-1}\left(x^{-1}yx\right)^t x = x^{-1}y^{t^2}x = y^{t^3}$
We then have $y^{t^3} = y$ which means $t^3 \equiv 1 (\mathrm{mod}\, 5).$
Checking possibilities we find that only *t* = 1 satisfies this!
This means that *x* and *y* commute, so their product is an element of order 15 and our group is cyclic.

7. Solvable groups and finite simple groups. The Feit -Thompson Theorem, The Classification of finite simple groups,

Solvable groups

Example:

We have the following "normal series" in S_4:

$$1 \lhd H = \{1, (12)(34)\} \lhd V_4 \lhd A_4 \lhd S_4$$

We examine the quotients:

- H is cyclic of order 2
- V_4/H is cyclic of order 3
- A_4/V_4 is cyclic of order 3
- S_4/A_4 is cyclic of order 2

Definition:
G is **solvable** if there exists a normal series:
$1 = G_1 \lhd G_2 \lhd \cdots \lhd G_n$ such that $G_i \lhd G_{i+1}$ and G_{i+1}/G_i for all i.

Note:
If we have such a series we can always find a normal series in which the quotients are cyclic.

Examples:
- S_4
- any abelian group is solvable.
- any nonabelian simple group is not solvable, e.g. A_5 is not solvable.
- S_5 is not solvable!

This uses the fact that A_5 is not solvable.

If we had a normal series as above for S_5:

$1 = G_1 \lhd G_2 \lhd \cdots \lhd G_n = S_5$ such that $G_i \lhd G_{i+1}$ and G_{i+1}/G_i for all i.

then intersecting each G_i with A_5 we would get a normal series for A_5, and it is easy to show that the quotients would all be abelian – giving a contradiction.

Claim: Finite p-groups are solvable.
Proof:
If our group G is abelian then it is solvable. Assume not.
We showed already that the centre of a p-group is nontrivial.
We take $G_2 = Z(G)$. If the quotient $G/Z(G)$ is abelian, we are done.

If not, as it is also a *p*-group, its centre $Z(G/Z(G))$ is nontrivial. By the homomorphism theorem, this group is of the form $G_3/Z(G)$ where $G_3 \lhd G$.
Hence we have now: $1 = G_1 \lhd Z(G) = G_2 \lhd G_3$.
If G/G_3 is abelian, we are done – if not we continue by taking its (nontrivial) centre.
We reach *G* in a finite number of steps.
The notion of a solvable group goes back to Galois, and turns out to be of great importance in his proof that the general polynomial equation of degree *n* is not solvable by radicals.

For modern group theory the most important theorem regarding solvable groups was proved in 1962:

The Feit-Thompson Theorem(1962)

Finite groups of odd order are solvable

Example:
Any group of order 3974821 is solvable!

Conclusion:

Every finite nonabelian simple group has **even** order.

The theorem was a first in many respects:

Apart from its mathematical importance, it had the longest proof of any theorem up to that time!

The proof used results of Brauer in modular representations and characters of finite groups developed in the 1950s, as well as including other new methods and results.

It turned out to have long-range important implications.

The proof was 252 pages long, the whole of Volume 13, no.3 of the Pacific Journal of Mathematics

Chapter I, from Solvability of groups of odd order, Pacific J. Math, vol. 13, no. 3 (1963)

Walter Feit and John G. Thompson; 775-787

View PDF View Abstract

Chapter II, from Solvability of groups of odd order, Pacific J. Math., vol. 13, no. 3 (1963)

Walter Feit and John G. Thompson; 789-802

View PDF View Abstract

ChapterIII, from Solvability of groups of odd order, Pacific J. Math., vol. 13, no. 3 (1963)

Walter Feit and John G. Thompson; 803-843

View PDF View Abstract

Chapter IV, from Solvability of groups of odd order, Pacific J. Math., vol. 13, no. 3 (1963)

Walter Feit and John G. Thompson; 845-942

View PDF View Abstract

Chapter V, from Solvability of groups of odd order, Pacific J. Math., vol. 13, no. 3 (1963)

Walter Feit and John G. Thompson; 943-1010

View PDF View Abstract

Chapter VI, from Solvability of groups of odd order, Pacific J. Math., vol. 13, no. 3 (1963)

Walter Feit and John G. Thompson; 1011-1027

View PDF View Abstract

Bibliography, from Solvability of groups of odd order, Pacific J. Math., vol. 13, no. 3 (1963)

The Classification of finite simple groups (1983, 2004) (Gorenstein, Lyons, Solomon, Aschbacher,…and about 100 others!)

Historical background:

Question: What are all the finite simple groups (up to isomorphism)?

Motivation:
The classification of finite simple Lie groups, and the Feit-Thompson theorem, which suggested ways of characterizing the structure of a finite simple group.

Clearly there are an infinite number of isomorphism types – for instance:
- Z/pZ for any prime p.
- $A_n, \quad n \geq 5$

There are also many infinite families of matrix groups, for instance, if F is a field of order q:
- $PSL(n,q) = SL(n,q)/Z(SL(n,q))$ are simple unless $n = 2$, and $q = 2$ or 3.

(We shall see later that there are infinitely many such q.

Better Question:
Is it possible to list all the finite simple groups (up to isomorphism)?

It turns out that in addition to the infinite families of the types listed above, there are also examples of special simple groups:

In 1860 Mathieu discovered a simple group not of the above types, and then later found another 4 such groups: $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$

Additional "sporadic" finite simple groups were discovered between 1965 (the Janko groups) and 1974 in an attempt to classify all finite simple groups (these were discovered by chance, by trying to build counter-examples!).

In 1972, Gorenstein suggested that it would be possible to give a complete list of finite simple groups involving the known infinite families plus a finite list of sporadic groups.

In 1976, it was in the final stages of proof.
Finally announced in 1980.

Statement of the theorem:

If G is a finite simple group then it is one of the following:

- Z/pZ for a prime p.
- $A_n, \quad n \geq 5$
- a simple matrix group over a finite field. (these are called groups of Lie type, there is a list of a finite number of types: classical families, exceptional families and twisted families)
- one of 26 sporadic groups.

Significance and implications:

The proof was a huge step forward, it was not even believed possible in the early 70s!
It now means that many general theorems can be proved using the classification, by checking cases.
There is also the task of understanding the structure of the known groups, especially the stranger of the sporadic groups.

The proof consists of hundreds of papers – the first being the Feit-Thompson theorem.

In the 1990s Gorenstein, Lyons, and Solomon gradually published a simplified and revised version of the proof (in 6 volumes) but still containing some significant gaps,

In 2004 Aschbacher and Smith published a two-volume supplement (almost 1300 pages!) that removed the last gaps in the proof (the case of quasi-thin groups).

The sporadic groups, the Fisscher Griess Monster (1982)

The Fischer –Griess Monster

In 1973, Fischer and Griess hypothesized the existence of a new and gigantic simple group with very special properties.
Griess constructed it (thus proving its existence) in 1980.

John Thompson showed that the uniqueness would follow from a claim that was proved in 1990 by Griess, Meierfrankenfeld and Yoav Segev.

The order of the group M is:

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

$$= 808017424794512875886459904961710757005754368000000000$$

$$\approx 8 \cdot 10^{53}.$$

- **M has 194 conjugacy classes.**
- **"Moonshine" properties:**
  Connections between conjugacy classes of M and a special class of modular elliptic functions.
  1998 – Richard Borcherds received the Fields medal for proving these connections.

The first 3 irreducible character degrees are: 1, 196883, 21296876
Corresponds to the elliptic modular function

$$j(z) = \frac{1}{q} + 196884\,q + 21493760\,q^{2} + \cdots \quad , \quad q = e^{2\pi i z}$$

And:

1 +196883 = 196884
1 + 196883 + 21296876 = 21493760

Bibliography

- J. H. Conway and S. P. Norton, *Monstrous Moonshine*, Bull. London Math. Soc. 11 (1979), no. 3, 308—339.
- R. L. Griess, Jr, *The Friendly Giant*, Inventiones Mathematicae 69 (1982), 1-102
- Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; and Wilson, R. A.: *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups.* Oxford, England 1985.
- S. P. Norton, *The uniqueness of the Fischer-Griess Monster*, Finite groups---coming of age (Montreal, Que., 1982), 271—285, Contemp. Math., 45, Amer. Math. Soc., Providence, RI, 1985.
- Griess, Robert L., Jr.; Meierfrankenfeld, Ulrich; Segev, Yoav *A uniqueness proof for the Monster.* Ann. of Math. (2) 130 (1989), no. 3, 567-602.
- Koichiro Harada, *Monster*, Iwanami Pub. (1999) ISBN 4-000-06055-4, (written in Japanese)
- P. E. Holmes and R. A. Wilson, *A computer construction of the Monster using 2-local subgroups*, J. London Math. Soc. 67 (2003), 346—364.
- Ivanov, A. A., *The Monster Group and Majorana Involutions*, Cambridge tracts in mathematics, **176**, Cambridge University Press, ISBN 978-0521889940
- S. A. Linton, R. A. Parker, P. G. Walsh and R. A. Wilson, *Computer construction of the Monster*, J. Group Theory 1 (1998), 307-337.
- M. Ronan, *Symmetry and the Monster*, Oxford University Press, 2006, ISBN 0192807226 (concise introduction for the lay reader).
- M. du Sautoy, *Finding Moonshine*, Fourth Estate, 2008, ISBN 978-0-00-721461-7 (another introduction for the lay reader; published in the US by HarperCollins as *Symmetry*, ISBN 978-0060789404).
- Thompson, John G. (1984), "Some finite groups which appear as Gal *L*/*K*, where $K \subseteq \mathbb{Q}(\mu_n)$", *Journal of Algebra* **89** (2): 437–499,doi:10.1016/0021-8693(84)90228-X, MR751155.

8. Field theory: Introduction. Extensions of fields.

Algebraic extensions of fields

Definition:
If $F \subseteq K$ are fields, $\alpha \in K$ is algebraic over F if it is a root of a polynomial in $F[x]$.

If $\alpha \in K$ is algebraic over F, the monic polynomial of minimal degree over F of which α is a root is called its minimal polynomial.

Claim: Minimal polynomials are irreducible.
Proof: Assignment 7

Claim: If $p(x)$ is the minimal polynomial of α, and $f(\alpha)=0$ then $p(x)|f(x)$.
Proof: Assignment 7

Definition:
If $F \subseteq K$ are fields, and every element of K is algebraic over F, then it is called an algebraic extension.

Definition:
If $F \subseteq K$ are fields, $\alpha \in K$ is transcendental over F if it is not algebraic over F.

Examples:

- All elements of F are algebraic over F.
- i, $\sqrt{2}$ are algebraic over Q.
- $\sqrt{7+\sqrt{5}+1}$ is algebraic over Q.
- e, π are transcendental over Q.

If $F \subseteq K$ are fields, $\alpha \in K$ denote by $F(\alpha)$ the smallest subfield of K containing F and α, and by $F[\alpha]$ the smallest subring of K containing F and α.

If $F \subseteq K$ are fields, we denote by $|K:F|$ the dimension of K as a vector space over F.

Note that as π is transcendental over Q, the powers of π are linearly independent over Q. Hence we have: $|R:Q|=\infty$.

In fact we have:

Claim: If $F \subseteq K$ are fields: $\alpha \in K$ is algebraic over $F \Leftrightarrow$ $|F(\alpha):F|$ is finite $\Leftrightarrow$ $F(\alpha)=F[\alpha]$.

In fact in the above situation we have that $|F(\alpha):F|=\deg f$ where f is the minimal polynomial of α over F.

Proof of the claim:

The first "iff" is clear: the existence of a polynomial of which α is a root shows that its powers are linearly dependent.
We now look at the second part of the claim:
Clearly $F(\alpha) \supseteq F[\alpha]$, so it suffices to show that $F[\alpha]$ is in fact a field.

We need to show that every nonzero element has an inverse.

Let $0 \neq f(\alpha) \in F[\alpha]$ and let $p(x)$ be the minimal polynomial of α.
We write:

$$f(x)=q(x)p(x)+r(x) \text{ where } r(x) \equiv 0 \text{ or } \deg r(x) < \deg p(x).$$

By our previous claims, $p(x)$ is irreducible, and as $0 \neq f(\alpha)=r(\alpha)$ we must have that $r(x) \neq 0$ and that $p(x)$ and $r(x)$ are relatively prime.
We there fore have g and h such that $p(x)g(x)+r(x)h(x)=1$ and then get: $1=p(\alpha)g(\alpha)+r(\alpha)h(\alpha)=r(\alpha)h(\alpha)=f(\alpha)h(\alpha)$. This means that $h(\alpha)=f(\alpha)^{-1}$ in $F[\alpha]$.

Fundamental extension theorem:
Let $p(x) \in F[x]$ be irreducible, then there exists and extension field K of F in which $p(x)$ has a root, and if K is minimal with respect to this property, then K is unique up to isomorphism, in fact $K \cong F[x] \big/ p(x)F[x]$.

Proof:
If $\deg p(x)=1$ we can take $F = K$.
We now assume $\deg p(x)>1$.
We take a new indeterminate u.
$p(u)F[u]$ is a maximal ideal in $F[u]$.

Hence $K = F[u]/p(u)F[u]$ is a field.
We shall show this also directly:

Any nonzero element $\beta \in K$ is of the form $\beta = g(u) + p(u)F[u], \quad g \notin pF[u]$.
Since *p* is irreducible this means that *p* and *g* are relatively prime. Hence by Bezout we have *r, s*: $p(u)r(u) + g(u)s(u) = 1$ and so:
$g(u)s(u) \in 1 + p(u)F[u]$.
So $\beta^{-1} = s(u) + p(u)F[u]$ in *K*.

We now show that $p(x)$ has a root in *K*. Writing $p(x) = \sum a_i x^i$ and denoting $\alpha = u + p(u)F[u]$ in *K* we get that:
$p(\alpha) = \sum a_i (u + p(u)F[u])^i = \sum a_i u^i + p(u)F[u] = 0$ in *K*.
Regarding *F* as embedded in *K* via the map: $a \mapsto a + p(u)F[u]$, we regard *K* as an extension of *F*.
We shall skip the proof of the uniqueness of *K*.

Example:

$Q(\sqrt{2}) \cong Q[x]/(x^2 - 2)$.
All the elements are of the form: $a + b\sqrt{2}$.
In fact the isomorphism is: $\varphi : a + b\sqrt{2} \mapsto a + bx + (x^2 - 2)$.
For instance we can check directly that it is multiplicative.
We note that over this field $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ factorization to linear factors.

9. Splitting fields, Galois groups.

Definition: If $F \subseteq K$ are fields, $f(x) \in F[x]$, K is called a **splitting field** for f over F if f factors completely over K and K is minimal with respect to this property.

Examples:

- $Q(\sqrt{2})$ is a splitting field for x^2-2 over Q.
- $Q(\sqrt[3]{2}) \cong Q[x]/(x^3-2)$ is not a splitting field for x^3-2 over Q as over $Q(\sqrt[3]{2})$ we have: $x^3-2=\left(x-\sqrt[3]{2}\right)\left(x^2+\sqrt[3]{2}x+\left(\sqrt[3]{2}\right)^2\right)$ and both factors are irreducible over $Q(\sqrt[3]{2})$ as the roots of the quadratic polynomial are : $\frac{-\sqrt[3]{2}\pm\sqrt{\left(\sqrt[3]{2}\right)^2-4\left(\sqrt[3]{2}\right)^2}}{2}=\left(\sqrt[3]{2}\right)\frac{-1\pm i\sqrt{3}}{2}$ which are non-real whereas $Q(\sqrt[3]{2})$ is a subfield of the reals.

In fact the field $Q\left(\sqrt[3]{2},i\sqrt{3}\right)$ is a splitting field for x^3-2 over Q.

Corollary from the Extension Theorem:

Let $f(x) \in F[x]$. Then there exists a splitting field for f over F and it is unique up to isomorphism.

Proof:

We extend F if necessary to a field K_1 containing a root of f: α_1.

We recall that:

Claim: a is a root of $f(x)$ in a field F if and only if $x-a \mid f(x)$ over F.

Hence we have $f(x)=(x-\alpha_1)f_1(x)$ over K_1, and the degree of $f_1(x)$ is smaller than the degree of $f(x)$.

We continue to extend K_1 to a field K_2 containing a root α_2 of $f_1(x)$.

We then have some $f_2(x)$ of smaller degree than $f_1(x)$ such that $f(x)=(x-\alpha_1)(x-\alpha_2)f_2(x)$ over K_2 and so on.

The process ends as the degree of f is finite. The uniqueness follows from the uniqueness at each stage when we extend to get another root.

Characteristic of a field:

Definition: If there exists some positive integer n such that 1 added to itself n times equals zero, the smallest such n is called the **characteristic** of the field: char$F$ = n

If no such n exists we say char$F$ = 0.

Examples:

- char $Q = 0$
- $charZ/2Z = 2$
- $charZ/pZ = p$

Note: (Assignment 7**)** The characteristic of a field is either 0 or prime.

Note also: Any field is a vector space over any subfield (Assignment 7).

In particular:

Claim: If $p(x)$ is the minimal polynomial of an element *a* over a field *F*, then the dimension of $K \cong {F[x]}/{p(x)F[x]}$ over *F* as a vector space equals the degree of $p(x)$.

Notation:
If F and *K* are fields, We denote by K/F the fact that $F \subseteq K$.
This is not ambiguous as fields do not have nontrivial ideals, hence no quotient structures!

Detailed Example:

We calculate the splitting field of the polynomial $x^4 - 5$ over *Q:*
Extending to $Q(\sqrt{5})$ we can begin to factor the polynomial:
$x^4 - 5 = \left(x^2 - \sqrt{5}\right)\left(x^2 + \sqrt{5}\right)$
Extending again to $Q(\sqrt[4]{5})$ we get:
$x^4 - 5 = \left(x - \sqrt[4]{5}\right)\left(x + \sqrt[4]{5}\right)\left(x^2 + \sqrt{5}\right)$
In order to factor the irreducible quadratic we need to adjoin *i* to get $K = Q(i, \sqrt[4]{5})$:
This is the splitting field of the polynomial $x^4 - 5$ over *Q* as we have:
$x^4 - 5 = \left(x - \sqrt[4]{5}\right)\left(x + \sqrt[4]{5}\right)\left(x - i\sqrt[4]{5}\right)\left(x + i\sqrt[4]{5}\right)$

We define a function $\varphi : K \to K$ by $\varphi(a) = \bar{a}$.
Note that this is an automorphism of *K* (= isomorphism from *K* onto itself).
It fixes all real elements of *K*.
For example: $\varphi\left(2 + i\left(\sqrt[4]{5}\right)^3 - 7\sqrt[4]{5}\right) = 2 - i\left(\sqrt[4]{5}\right)^3 - 7\sqrt[4]{5}$
This means that the subfield $Q(\sqrt[4]{5})$ is fixed point-wise by φ.

In general:

If φ,ψ are 2 automorphisms of a field K then so are their product (composition), so is the identity map, and so is their inverse (check that the inverse is indeed a field homomorphism!) – so that the set of automorphisms form a group denoted: Aut$K$.

Given a field extension K/F we denote by $Aut\,K/F$ those automorphisms of K that fix every element of F.
In the example above, $\varphi \in K/Q(\sqrt[4]{5})$.

Galois groups:

Definition: The Galois group of a field extension K/F is the set of automorphisms of K that fix F element-wise. It is denoted by $Gal(K/F)$.

Definition: The Galois group of a polynomial over F is the Galois group of its splitting field over F.

Examples: We note that GalK/K = 1 and that if Q is a subfield of K we have that Gal(K/Q) = Aut K.

Galois Theory gives a one-to-one correspondence between normal subgroups of $Gal(K/F)$ and certain subfields (called normal extensions) of K containing F.

Separable polynomials.

A polynomial is called separable if its irreducible factors have distinct roots.

We note that this is always true for any polynomial when the field characteristic is 0.
However, there are cases when the field characteristic is prime, where the polynomial is not separable.

Theorem (Galois):

If E/F is the splitting field of a separable polynomial in $F[x]$ then
$\left|Gal\left(E/F\right)\right| = \dim_F E = |E:F|$

Recall that:

Claim: If $F \subseteq K \subseteq E$ are fields then $|E:F| = |E:K| \cdot |K:F|$

Proof: Assignment 8

We return to our example above: $K = Q(i, \sqrt[4]{5})$.

$$\left|Q(i,\sqrt[4]{5}) : Q\right| = \left|Q(i,\sqrt[4]{5}) : Q(\sqrt[4]{5})\right| \cdot \left|Q(\sqrt[4]{5}) : Q(\sqrt{5})\right| \cdot \left|Q(\sqrt{5}) : Q\right| = 2 \cdot 2 \cdot 2 = 8$$

Hence we have that $Gal\left(Q(i,\sqrt[4]{5})/Q\right)$ is a group of order 8.
We shall look at this group in detail later.

10. Galois groups of polynomials as permutation groups on their roots.

Important observation of Galois:
Claim: If $f(x) \in F[x]$ then $Gal\left(K/F\right)$ permutes the roots of $f(x)$ that are contained in *K*.

This then means that the Galois group can be considered to be a subgroup of S_n where *n* is the number of roots of *f*.

Proof of claim:
Suppose α is a root of *f* in *K*, and φ is an automorphism in $Gal\left(K/F\right)$.
We have $f(x) = \sum a_n x^n, \quad a_n \in F$.
Hence we have: $0 = \varphi(0) = \varphi\left(f(\alpha)\right) = \sum a_n \varphi(\alpha)^n$ as $a_n \in F$.
This means that $\varphi(\alpha)$ is also a root of *f*.

Examples of Galois groups:

1. What is the Galois group of x^2+1 over *Q*?
The splitting field is *Q(i)* which has degree 2 over *Q*. so we know $Gal\left(Q(i)/Q\right)$ has 2 elements and so is cyclic of order 2.
Here the only nontrivial automorphism is complex conjugation which indeed is of order 2 and switches *i* and –*i* the 2 roots of x^2+1.

- The Galois group of the polynomial $x^4 - 5x^2 + 6$ and determining them up to isomorphism.

2. What is the Galois group *G* of $x^4 - 5x^2 + 6$ over *Q*?

We note that $x^4 - 5x^2 + 6 = \left(x^2 - 3\right)\left(x^2 - 2\right)$ so that the splitting field is $Q\left(\sqrt{3}, \sqrt{2}\right)$.
If $\varphi \in G$ then $\varphi\left(\sqrt{3}\right)^2 = \varphi(3) = 3$ Hence $\varphi\left(\sqrt{3}\right) = \pm\sqrt{3}$.
Similarly $\varphi\left(\sqrt{2}\right) = \pm\sqrt{2}$.
This gives 4 options $1, \varphi, \psi, \varphi\psi$:
$\varphi\left(\sqrt{3}\right) = -\sqrt{3}, \quad \varphi\left(\sqrt{2}\right) = \sqrt{2}$,
$\psi\left(\sqrt{3}\right) = \sqrt{3}, \quad \psi\left(\sqrt{2}\right) = -\sqrt{2}$,
$\varphi\psi\left(\sqrt{3}\right) = -\sqrt{3}, \quad \varphi\psi\left(\sqrt{2}\right) = -\sqrt{2}$.
We therefore have $G \cong C_2 \times C_2$

We also note that: $Gal\left(Q\left(\sqrt{3},\sqrt{2}\right)/Q\left(\sqrt{2}\right)\right)=\{1,\varphi\}$ and $Gal\left(Q\left(\sqrt{3},\sqrt{2}\right)/Q\left(\sqrt{3}\right)\right)=\{1,\psi\}$.

3. Class Activity:

דף פעילות

מיצאו את חבורת Galois של הפולינום x^3+2x+1 מעל שדה המספרים הרציונליים לפי הצעדים הבאים:

א. הראו שהפולינום אי-פריק מעל הרציונליים. (אפשר להשתמש בלמה של גאוס.)

ב. השתמשו באנליזה כדי להראות שיש לו שורש ממשי יחיד שנסמן ב- α.

ג. הראו ששני השורשים האחרים שלו הם זוג של מספרים מרוכבים צמודים זה לזה, שנסמן ב- $\beta,\overline{\beta}$.

ד. מיצאו את המימד של שדה הפיצול $Q(\alpha,\beta,\overline{\beta})$ של הפולינום מעל הרציונליים.

ה. לפי משפט של Galois, המימד שווה למספר האברים בחבורה. היעזרו בכך כדי לקבוע את מבנה החבורה.

Solution – in separate file.

Example 4:

Determining the Galois group $Gal\left(Q(i,\sqrt[4]{5})/Q\right)$ of the polynomial x^4-5 over *Q:*

As in our previous examples we know that it can be considered a subgroup of S_4 as it is a permutation group on the 4 roots: $\pm\sqrt[4]{5},\pm i\sqrt[4]{5}$ of x^4-5.

Calculating dimensions again we see that the Galois group has order 8.

Fact: There are only 5 groups of order 8 up to isomorphism:

$$C_8,\quad C_4\times C_2,\quad C_2\times C_2\times C_2,\quad D_8,\quad Q_8$$

Our group cannot be cyclic as S_4 has no cyclic subgroup of order 8.
Similarly, one can rule out all the other groups on the list except for D_8.
However we can show that the group is isomorphic to D_8 directly:

Clearly complex conjugation (which is an automorphism of *C* restricts to an automorphism of the splitting field of order 2. This corresponds to a reflection in D_8.
Also the map which sends *i* to itself and sends $\sqrt[4]{5}$ to $i\sqrt[4]{5}$ will in fact be of order 4 and rotates the roots $\pm\sqrt[4]{5}, \pm i\sqrt[4]{5}$ cyclically – corresponding to a rotation in D_8 through 90 degrees.
All other elements in the group will be generated by these 2 maps, and gives the isomorphism between the two groups.

11. Cyclotomic fields: $Q(\sqrt[n]{1})$

Definitions:

A cyclotomic field is an extension of the rationals by a root of unity.

An *n*th root of unity is primitive if it is of order n.

We denote $\xi = e^{\frac{2\pi i}{n}} = \sqrt[n]{1}$.

Note that all roots of unity lie on the unit circle in the complex plane.

Examples:

- i is a primitive 4^{th} root of unity.
- We find all primitive 9^{th} roots of unity:

  $e^{\frac{2\pi i}{9}} = \xi,\quad \xi^2,\quad \xi^4,\quad \xi^5,\quad \xi^7,\quad \xi^8$

Clearly over $Q(\sqrt[n]{1})$ we have: $x^n - 1 = \prod_{k=0}^{n-1}\left(x - \xi^k\right)$.

Definition:

The minimal polynomial of a primitive nth root of unity over the rationals
is called the *n*th cyclotomic polynomial and denoted $\lambda_n(x)$.

The factorization of $x^n - 1$, over the rational numbers:

Note that $\lambda_n(x) \mid x^n - 1$ over the rationals.

We determine the cyclotomic polynomials for some values of *n*:

- $\lambda_1(x) = x - 1$
- $\lambda_2(x) = x + 1$
- $\lambda_3(x) = x^2 + x + 1$
- $\lambda_4(x) = x^2 + 1$
- $\lambda_6(x) = x^2 - x + 1$
- $\lambda_p(x) = x^{p-1} + \cdots + x^2 + x + 1$, for a prime *p*.
  (We get that these are irreducible as a corollary of Eisenstein's Criterion.)

Detailed examples:

Example 1: We shall factor $x^6 - 1$ over *Q*.

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

We shall find the roots of each factor:

$(x-1)$	$(x+1)$	(x^2+x+1)	(x^2-x+1)
1	-1	$\omega, \overline{\omega}$	$\rho, \overline{\rho}$

where ω is a primitive cubed root of unity and ρ is a primitive 6th root of
unity. We conclude therefore that $\lambda_6(x) = x^2 - x + 1$.

Note that using the quadratic formula we can calculate these directly.

In fact: $\omega = \frac{-1 + i\sqrt{3}}{2}$, $\rho = \frac{1 - i\sqrt{3}}{2}$ so we see that in fact $-\omega = \rho$.
(The choice of *i* or *–i* is arbitrary.)
This actually tells us that $Q(\sqrt[6]{1}) = Q(\sqrt[3]{1})$.

Comparison of different cyclotomic fields of dimension 2 over the rationals:

We note that as vector spaces over the rationals, the fields $Q(\sqrt[3]{1})$ and $Q(i)$ are both of dimension 2 and therefore isomorphic. However they are not isomorphic as fields – which we can see by checking the multiplication, or by noting that, for instance $Q(i)$ does not contain a root of $\lambda_3(x) = x^2 + x + 1$.

Example 2: **We shall factor $x^9 - 1$ over *Q*.**

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1) = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

We omit the check that in fact $x^6 + x^3 + 1$ is irreducible, giving us that:

$$\lambda_9(x) = x^6 + x^3 + 1.$$

Definition of Euler's φ-function:

$\varphi(n)$ = the number of positive integers smaller than *n* and prime to *n*.

Theorem: $\left|Q(\sqrt[n]{1}) : Q\right| = \deg \lambda_n(x) = \varphi(n)$

- without proof.

Theorem: $x^n - 1 = \prod_{d|n} \lambda_d(x)$.

Number theoretic corollary: $n = \sum_{d|n} \varphi(d)$

Example:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x-1)(x+1)(x^2 + x + 1)(x^2 - x + 1) = \lambda_1(x)\lambda_2(x)\lambda_3(x)\lambda_6(x)$$

We note also that indeed $\deg \lambda_6(x) = \varphi(6) = 2$.

Proof:

First it is clear that if $d|n$ then $\lambda_d(x)|x^n-1$, as $\sqrt[d]{1}$ is also a root of x^n-1 in this case, so its minimal polynomial must divide x^n-1.
We now assume that $p(x)|x^n-1$ and $p(x)$ is irreducible.
If α is a root of p then it is a root of x^n-1, and so $\alpha^n=1$. Hence if d is minimal such that $\alpha^d=1$ we have that α is a root of $\lambda_d(x)$ which is irreducible. Hence we have $\lambda_d(x)=p(x)$.
We note that since all the complex roots of x^n-1 are distinct, each factor appears exactly once, and we have proved the theorem.

More examples to illustrate both theorems:

2. ***n = 9***

$$x^9-1=(x^3-1)(x^6+x^3+1)=(x-1)(x^2+x+1)(x^6+x^3+1)=\lambda_1(x)\lambda_3(x)\lambda_9(x)$$

and $\deg\lambda_9(x)=\varphi(9)=6$.

3. ***n = 12.***

By the theorem:

$$x^{12}-1=\lambda_1(x)\lambda_2(x)\lambda_3(x)\lambda_4(x)\lambda_6(x)\lambda_{12}(x)$$

And we have:

$$x^{12}-1=(x^6-1)(x^6+1)=(x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^6+1)$$
$$=(x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^4+x^2-1)$$

By dividing x^6+1 by x^2+1.
Hence we conclude that $\lambda_{12}(x)=(x^4+x^2-1)$, and indeed $\varphi(12)=4$.

Note:

We note that in all the examples we have seen so far, all the coefficients
in the factorizations over the integers have been 0, 1 or -1.
It is interesting to speculate if this is always the case.

In fact: it is not! The first counterexample is $n = 105$!
Note that 105 is the first integer to be divisible by 3 distinct odd primes.

Migotti's Theorem (1883):
If $n = pq$, for p and q distinct primes, then the coefficients of the nth cyclotomic polynomial are only 0, 1 or -1.

12. The general polynomial equation of degree *n* and solvability by radicals.

Prime fields in characteristic 0.

Let F be a field of characteristic 0.
The smallest subfield of F is called its prime field.

We claim that this field is isomorphic to Q.

We first note that it necessarily contains 0 and 1.

For any positive integer n denote by $\bar{n}$ the element in F obtained by adding 1 to itself n times.
Note that in F, $n \neq m$ implies $\bar{n} \neq \bar{m}$ as the characteristic is 0.
Identifying $-n$ with $-\bar{n}$ we see that the prime field of F contains a copy of the integers.

In a natural way we can then see, that identifying $\frac{1}{n}$ with $\bar{n}^{-1}$ for nonzero integers n and extending the map multiplicatively, we have constructed an isomorphism between the prime field and Q.

Statement of Theorem (Galois):
If char$F$ = 0, and F contains a primitive nth root of unity then:
The Galois group $Gal\left(K/F\right)$ is cyclic if and only if $K = F(\alpha)$ where is a root of a polynomial of the form $x^n - a, \quad a \in F$.

For instance if $F = Q(\sqrt[n]{1})$ the condition holds.
Note that the condition on F guarantees that K will be a splitting field for $x^n - a, \quad a \in F$.

Example: $F = Q(\omega), \quad K = F\left(\sqrt[3]{2}\right)$

Corollary:
If $f(x) \in Q[x]$ and K is its splitting field over Q then:

$Gal\left(K/Q\right)$ is a solvable group if and only there is a sequence of fields:
$Q = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_s = K$ such that the Galois groups $Gal\left(K_{i+1}/K_i\right)$ are cyclic for all *i*.

Solvability by radicals:
Note that in this case *K* is generated over *Q* by *n*th roots of various elements of *Q* for some *n*, or of extension fields of *Q* by adjoining *n*th roots.
In such a situation, the roots of $f(x) \in Q[x]$ will therefore be expressible in terms of the 4 arithmetic operations and extraction of *n*th roots.

We say in a situation like this that $f(x) = 0$ is <u>solvable by radicals</u>.

Example: $Gal\left(Q(i,\sqrt[4]{5})/Q\right) \cong D_8$ is a solvable group.
We have the sequence:
$Q = K_1 \subseteq Q(i) = K_2 \subseteq Q\left(\sqrt{5}, i\right) = K_3 \subseteq Q\left(\sqrt[4]{5}, i\right) = K_4$

All the Galois groups of the quotients are cyclic of order 2.

Indeed the roots of the polynomial $x^4 - 5$ are expressible in terms of radicals of elements of $Q(i)$, including of course the roots of unity $\pm i$ over *Q*.

Example: The quadratic equation $ax^2 + bx + c = 0$ is solvable by radicals over *Q* as the roots are: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ which are elements in the field $Q(a,b,c,\sqrt{b^2 - 4ac})$ which is an extension of dimension 2 of $Q(a,b,c)$.

Theorem (Galois):
The polynomial equation $f(x) = 0$ over *Q* is solvable by radicals **if and only if** its Galois group over *Q* is solvable.

We now look at the general polynomial equation of degree n over Q:

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = 0$$

and the question of solvability by radicals for this equation.

Recall that the question Galois wanted to answer was whether formulas exist for the roots in terms of the coefficients of the equations.

We therefore need to consider the field $Q(a_0, a_1, \cdots, a_{n-1})$, where $a_0, a_1, \cdots, a_{n-1}$ are **transcendental** over Q, in other words, considered as formal variables, and then if the roots belong to an extension of this field obtained by taking roots, then they will be expressible in a formula of the type we see in the quadratic formula.

Statement of main theorem:

If K is the splitting field for the equation:
$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = 0$ over $Q(a_0, a_1, \cdots, a_{n-1})$, where $a_0, a_1, \cdots, a_{n-1}$ are transcendental over Q, then:

$$Gal\left(K \big/ Q(a_0, a_1, \cdots, a_{n-1})\right) \cong S_n .$$

Corollary:

Since S_n is not solvable for $n \geq 5$, the general polynomial equation of degree n over Q, for $n \geq 5$ is not solvable by radicals over Q.

Example of a rational polynomial which is not solvable by radicals (Emil Artin):

$f(x) = x^5 - x - 1$ is a rational polynomial whose Galois group over Q is the full symmetric group S_5, which is not solvable. Therefore this polynomial is not solvable by radicals!

13. Finite fields: detailed examples and properties

Prime fields in characteristic p:

Claim: If p is prime and char$F = p$ then $F_p = Z/pZ \subseteq F$.

Proof: We look at the set:

$$0,\quad 1,\quad 1+1,\quad 1+1+1,\quad \cdots\quad ,\underbrace{1+1+\cdots+1}_{p\text{-}1 \text{ times}}.$$

Clearly, this set is isomorphic to Z/pZ as an additive group.

Moreover, as a consequence of the distributive law, looking at products, we get that it is also isomorphic to Z/pZ as a field.

Consequences:

1. Every field of finite characteristic is an extension of Z/pZ.
2. In particular, every finite field is an algebraic extension of Z/pZ.
3. Z/pZ is the only field of order p (up to isomorphism).

Note:
There exist infinite fields of characteristic p as well.

We shall prove the following theorem in stages:

Main Theorem:
For every prime p and natural number $k \geq 1$ there exists a **unique** field of order p^k, and every finite field is of prime power order. (We denote this field $GF(p^k)$.)

Notes and comments:

The theory of finite fields developed throughout the 19th century beginning with unpublished work of Gauss and Galois.

The theorem above was the result of the work of a number of people and not all details are known.

Dedekind constructed in 1857 fields of order p^k as quotient rings of polynomial rings modulo ideals generated by irreducible polynomials.
Dickson's book published in 1901 contained the entire theorem and most of the results presented here.

We first show the last statement in the theorem:

Every finite field is of prime power order.
(proved by Eliakim H. Moore in 1893)

Proof:
Suppose F is a field of order n.
As we showed, $Z/pZ \subseteq F$, where p is prime and char$F = p$.
Therefore F is a vector space of finite dimension, say k over Z/pZ, as it is finite. A vector space of dimension k over a field of order p has p^k elements, as each element can be represented uniquely as a linear combination of k basis elements where each coefficient can be chosen in p ways. so $n = p^k$.

Comments:
1. Regarding the uniqueness in the theorem - note that the situation in characteristic zero is very different.
   For example the fields: $Q(i)$, $Q(\sqrt{2})$, $Q(\omega)$ are all of dimension 2 over Q but are nonisomorphic.
2. Note that the theorem tells us that there are no fields of order 6, 10 etc!

Examples:
- **The finite field of order 4 as the quotient $F_2[x]/F_2[x](x^2+x+1)$:**

Note that the polynomial x^2+x+1 is irreducible over F_2. Indeed it is the only irreducible quadratic over this field!
We can represent its elements wlog as the representatives of the cosets to be: $0,\ 1,\ x,\ x+1$.

Constructing multiplication and addition tables $\bmod(x^2+x+1)$ we can show that we get a field isomorphic to that constructed in the exercises.
We have now proved the existence of such a field. We saw then that there was only one way to construct the tables. This shows that $GF(4)$ is unique.

- **The finite field of order 16,** $K = F_2[x] \big/ F_2[x](x^4+x^3+1)$ **:**

Checking we can verify that x^4+x^3+1 is irreducible over F_2, and use it to construct $F_2[x] \big/ F_2[x](x^4+x^3+1)$ which will then be of order 16.
We regard the elements as polynomials in *x* of degree less or equal to 3.

We give examples to illustrate addition and multiplication in this field:

$$(x^2+1)+(x^3+x^2+1)=(x^3+x+1)$$

- this is simply addition (mod2).

$$(x^2+1)\cdot(x^3+x^2+1)=x^5+2x^4+x^3+x+x\equiv x^5+x^3+x+x \pmod 2$$
$$=(x+1)\cdot(x^4+x^3+1)+(x^2+1)\equiv(x^2+1) \qquad \bmod(x^4+x^3+1)$$

Note also for instance that in this field:

$$(x+1)\cdot x^3 = x^4+x^3 \equiv 1$$

So that x^3 is the inverse of $x+1$ in the field.

As we saw in the proof of the basic extension theorem, the element $\alpha = x + F_2[x](x^4+x^3+1)$ is a root of x^4+x^3+1 in our field.
The elements: $1,\ \alpha,\ \alpha^2,\ \alpha^3$ form a basis for the field as a vector space over F_2.

The multiplicative group of the field K^* is of order 15.
Hence the order of α in this group must divide 15.

We note that $\alpha \neq 1, \quad \alpha^3 \neq 1$.
Moreover we have:

$$\alpha^4 = \alpha^3 + 1, \quad \alpha^5 = (\alpha^3 + 1)\alpha = \alpha^4 + \alpha = \alpha^3 + \alpha + 1 \neq 1.$$

So α must be of order 15 and so the multiplicative group of the field is cyclic.
Indeed, one can write all the elements of *K* as powers of α together with the zero element.

We can use the following table to do arithmetic in GF(16), using the first column for multiplication, and the second or third for addition.

3 representations of the elements of GF(16)

Let α be a root of the polynomial $f(x) = x^4 + x^3 + 1$ over GF(2).

I	II	III
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha^3 + 1$	1001
α^5	$\alpha^3 + \alpha + 1$	1011
α^6	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^7	$\alpha^2 + \alpha + 1$	0111
α^8	$\alpha^3 + \alpha^2 + \alpha$	1110
α^9	$\alpha^2 + 1$	0101
α^{10}	$\alpha^3 + \alpha$	1010
α^{11}	$\alpha^3 + \alpha^2 + 1$	1101
α^{12}	$\alpha + 1$	0011
α^{13}	$\alpha^2 + \alpha$	0110
α^{14}	$\alpha^3 + \alpha^2$	1100

Theorem (without proof):
The multiplicative group of a finite field is cyclic.

Note: Q^* is not cyclic!

Theorem:
If F is a finite field of order q, then it is the splitting field of the polynomial $x^q - x$ over GF(p), where p is prime and char$F = p$.

Proof:
Note that every element of F is a root of $x^q - x$ as F^* is of order q-1 so $a^{q-1} = a, \quad \forall a \in F^*$, and therefore these are roots of $x^q - x$, and clearly 0 is also a root of $x^q - x$.

Note:
Over a field, using the fact that over a field, a is a root of $f(x)$ in a field F if and only if $x - a \mid f(x)$ over F, we can show by induction on n that a polynomial of degree n has at most n roots. (This is not true over rings!)

Since $x^q - x$ is of degree q, it has at most q roots in any extension field of F. Hence these are <u>all</u> the roots of $x^q - x$ and over F we have:
$x^q - x = \prod_{a \in F} (x - a)$ which means that F is the splitting field of $x^q - x$.

Consequences of the theorem:
1. If F is a field of order q, then the minimal polynomial of any element of F divides $x^q - x$.
2. The theorem implies the uniqueness of any field of a given order, as splitting fields are unique up to isomorphism.

<u>Construction of a field of order</u> p^k <u>:</u>

We take the field F_p and the polynomial $x^{p^k} - x$.

Let E be its splitting field over F_p.

We claim that E has p^k elements.

We note first that in E, the roots of $x^{p^k} - x$ are distinct.
To show this we apply the derivative test. The derivative can be defined formally for any polynomial.

Derivative test for multiple roots:
If a is a root of $f(x)$ then:
a is a multiple root for $f(x) \Leftrightarrow a$ is a root of $f'(x)$

Proof: Since a is a root of $f(x)$ we have $g(x)$ such that:

$$f(x) = (x-a)g(x)$$

So that a is a multiple root for $f(x) \Leftrightarrow g(a) = 0$
We have $f'(x) = g(x) + (x-a)g'(x)$, so that a is a multiple root for $f(x) \Leftrightarrow f'(a) = 0$.

We now check the derivative of $x^{p^k} - x$:

$$\left(x^{p^k} - x\right)' = p^k x^{p^k - 1} - 1 \equiv -1 (\text{mod } p)$$

In particular the derivative is never zero, and so has no multiple roots.

Therefore E contains all the p^k distinct roots of $x^{p^k} - x$ and so has at least p^k elements. It remains to show it has at most p^k elements.

To show this we shall show the set of roots is in fact a subfield, so by minimality of the splitting field it equals E.

Clearly 0 and 1 are roots of $x^{p^k} - x$ so they are contained in the set of roots.

If a and b are roots then we have $a^{p^k} = a, \quad b^{p^k} = b$

It is easy to see that $(ab)^{p^k} = a^{p^k} b^{p^k} = ab$.

Now $(a+b)^p = a^p + b^p$ over any field of characteristic p.

Similarly: $(a+b)^{p^2} = \left(a^p + b^p\right)^p = a^{p^2} + b^{p^2}$

Inductively we then get: $(a+b)^{p^k} = a^{p^k} + b^{p^k} = a+b$
Hence ab and a + b are in the set of roots.

If a is a root then $-a$ will also be a root as:

- if the characteristic of the field is 2, then simply $a = -a$
- if the characteristic is greater than 2 then p^k is odd, in which case:

$(-a)^{p^k} = -a^{p^k}$ so that $(-a)^{p^k} - (-a) = -a^{p^k} + a = 0$.

If a is a root then a^{-1} will also be a root as since $(a)^{p^k} = a$, we get that $a^{-1} = a^{-p^k} = \left(a^{-1}\right)^{p^k}$

Hence the set of roots is a field and so equals E.

As we noted before, the uniqueness of the field follows from the uniqueness of splitting fields in general. However we shall show it directly by constructing an isomorphism:

Claim:
Suppose $q = p^k$ and E is the splitting field of $x^{p^k} - x$ that we just constructed, and that E' is also a field of order q. Then $E \cong E'$.

Proof:
Since E' is finite, its prime field must be cyclic of prime order, and since its order is a power of p. the prime field will be F_p.
Every element in $(E')^*$ is a root of $x^{q-1} - 1$ hence all elements of E' are roots of $x^q - x$, and the polynomial factors completely over E'.

We now use the fact that E^* is cyclic: we take a generator α of E^*, and let $m(x)$ be its minimal polynomial over F_p. We must have $m(x) \mid x^q - x$.
Since E' contains all the roots of $x^q - x$, it must contain a root β of $m(x)$.

We construct our isomorphism φ from E to E' by mapping 0 to 0, and α^i
to β^i.

<u>We first show it is onto E':</u>
It is sufficient to show that β generates $(E')^*$.
Suppose negatively that β has order $r < q-1$. Then it is a root of the polynomial $x^r - 1$. Since $m(x)$ is the minimal polynomial of β, we then get that $m(x) \mid x^r - 1$. However from this it follows that also α is a root of $x^r - 1$. However, we chose α as a generator of E^* and so its order is $q - 1$ – contradiction!

Since φ maps a finite set to a finite set of the same order, it follows also that the map is therefore 1-1.

<u>We now show that φ is multiplicative and additive:</u>
By definition it is multiplicative as $\alpha^i \alpha^j = \alpha^{i+j}$ will be mapped to $\beta^i \beta^j = \beta^{i+j}$, and if one of the factors is 0, it will be mapped to 0.
We now show it is additive.
Clearly for any a in E: $\varphi(a+0) = \varphi(a) = \varphi(a) + \varphi(0)$.
Now we assume we have two nonzero elements in E: α^i, α^j.
We need to check two cases –

$$\alpha^i + \alpha^j = 0$$
$$\alpha^i + \alpha^j \neq 0.$$

If $\alpha^i + \alpha^j = 0$ then α is a root of $x^i + x^j$ and so $m(x) \mid x^i + x^j$.
That implies that β is also a root of $x^i + x^j$, and so $\beta^i + \beta^j = 0$, giving:
$\varphi(\alpha^i) + \varphi(\alpha^j) = \beta^i + \beta^j = 0 = \varphi(0) = \varphi(\alpha^i + \alpha^j)$.

If $\alpha^i + \alpha^j \neq 0$ the we have k such that $\alpha^i + \alpha^j = \alpha^k$ in which case α is a root of $x^i + x^j - x^k$. As before this means that

$m(x) \mid x^i + x^j - x^k$ which implies that β is also a root of $x^i + x^j - x^k$, and so $\beta^i + \beta^j = \beta^k$ as required.

This completes the proof of the existence and uniqueness theorem.

Detailed example: GF(9), and factorization of $x^9 - x$ over GF(3).

GF(9) is the splitting field of $x^9 - x$ over GF(3) and every element is a root of this polynomial.
We now factor it over GF(3):
$x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) = x(x^2 - 1)(x^2 + 1)(x^4 + 1)$
By trial and error we can factor $x^4 + 1$ to a product of quadratics over GF(3): $x^4 + 1 = (x^2 + x + 2)(x^2 + 2x + 2)$
These are both irreducible over GF(3) as they have no roots in the field.
Similarly, $x^2 + 1$ is irreducible.
We have $x^2 - 1 = (x+1)(x+2)$ over GF(3) so finally:

$$x^9 - x = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

We know that GF(9)* is cyclic, so if α is a generator, which of the irreducible quadratics above is its minimal polynomial?
We know that α will be of order 8.

Clearly any root β of $x^2 + 1$ satisfies $\beta^4 = 1$ so it cannot be a generator.
The roots of $x^2 + 1$ will be α^2, α^4 .
The other powers of α will all have order 8: $\alpha, \alpha^3, \alpha^5, \alpha^7$ and so any of these can be generators of GF(9)*. They must therefore be the roots of the polynomials $x^2 + 2x + 2$ and $x^2 + x + 2$.
Wlog if α is a root of $x^2 + 2x + 2$ then we can check to show that its other root is α^3. The roots of $x^2 + x + 2$ will then be α^5, α^7.

It is important to remember that we can generate the field of order 9 also by taking x^2+1. In other words, we have:

$$F_3[x]/F_3[x](x^2+1) \cong F_3[x]/F_3[x](x^2+x+2)$$

- even though the roots of x^2+1 do not generate the cyclic group of the field. However, the element 1, together with any root of either quadratic polynomial will be a *basis* for GF(9) over GF(3), as they are linearly independent over the prime field.

Corollaries from the theorem:

1. For every natural $n > 0$ there exists an irreducible polynomial of degree n over GF(p).

Proof:

Look at the field $GF(p^n)$ and take a generator a of $GF(p^n)^*$. Let $m(x)$ be its minimal polynomial over GF(p). Then we have:

$$GF(p^n) \cong F_p[x]/F_p[x]m(x)$$

From which it follows that the degree of $m(x)$ must be n, and it is irreducible as it is a minimal polynomial.

Note that a similar argument will give us that there is an irreducible polynomial of degree n over GF(q) for any prime power q.

2. Any two extensions of degree n over a finite field are isomorphic.

   In particular, for any two irreducible polynomials f, g of degree n over GF(p) we have:

$$F_p[x]/F_p[x]f(x) \cong F_p[x]/F_p[x]g(x)$$

We saw this an example of this in GF(9), taking two different polynomials to generate the field.

Factorization of x^n-1 over GF(p).

We assume we have an irreducible factor f of x^n-1.

Case 1: $n=p^k$

In this case we have $f(x)\mid x^n-1=x^{p^k}-1=(x-1)^{p^k}$

So that $f(x)=x-1$ and the factorization is simply $x^n-1=(x-1)^{p^k}$.

Case 2: $n=p^k m,\quad (p,m)=1$

In this case we have $f(x)\mid x^n-1=x^{mp^k}-1=\left(x^m-1\right)^{p^k}$

So that $f(x)\mid x^m-1$ and we need to determine the factorization of x^m-1 where $(p,m)=1$.

We shall therefore concentrate on **Case 3:** $(p,n)=1$.

We claim first that in this case there exists some k such that $n\mid p^k-1$:

By Bezout we have u, v such that $pu+nv=1$ so $nv\equiv 1(\text{mod } p)$.

This means that p is invertible in the ring Z/nZ.

The set of invertible elements $\left(Z/nZ\right)^*$ is a finite group, hence every element is of finite order, and so we have some k such that $p^k\equiv 1(\text{mod } n)$ which means that $n\mid p^k-1$.

We assumed $f(x)\mid x^n-1$ so if a is a root of f we have $a^n=1$.

Since $n\mid q-1$ we then have that $a^{q-1}=1$ so a is an element of F_q.

Therefore F_q contains all the roots of all the irreducible factors of x^n-1.

Hence any irreducible factor of x^n-1 over GF(p) is also an irreducible factor of x^q-x.

So in fact we need to investigate:

The factorization of $x^{p^k} - x$ over GF(*p*).

Example: Factorization of $x^{16} - x$ over *GF*(2).

We know that *GF*(16) is the splitting field of $x^{16} - x$, and that every element of the field is a root of the polynomial. Hence every element is a root of some irreducible factor of $x^{16} - x$ over *GF*(2).

Let α be a root of $x^4 + x^3 + 1$ in *GF*(16).
We have $(x^4 + x^3 + 1)^2 = x^8 + x^6 + 1$ over *GF*(2).
Hence α^2 is also a root.
Similarly $(x^4 + x^3 + 1)^4 = x^{16} + x^{12} + 1$ so that α^4 is also a root, and finally α^8 is a root as well.

We can therefore begin to factor:

$$x^{16} - x = x(x+1)(x^4 + x^3 + 1)h(x)$$

$$roots: \quad 0 \quad 1 \quad \alpha, \alpha^2, \alpha^4, \alpha^8$$

- so all other elements of *GF*(16) will be roots of *h(x)*.

We note that α^3 is of order 5 and so is a root of $x^4 + x^3 + x^2 + x + 1$. We have already checked that this polynomial is irreducible over *GF*(2).
Its roots are $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ and this polynomial must therefore also divide $x^{16} - x$, and so divides *h(x)*.
We now have:

$$x^{16} - x = x(x+1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)k(x)$$

We continue to factor *k(x)* which is of degree 6.

We note that α^5 is of order 3 and so is a root of $x^2 + x + 1$. We have already checked that this polynomial is irreducible over *GF*(2). Hence this polynomial divides *k(x)* and its roots are: α^5, α^{10}.

We are left with the remaining factor of *k(x)* which is of degree 4.

The roots of this factor are those elements of the field that remain:
$\alpha^{14},\alpha^{13},\alpha^{11},\alpha^{7}$ which can also be written as $\alpha^{-1},\alpha^{-2},\alpha^{-4},\alpha^{-8}$.

Observe that since $\alpha^4+\alpha^3+1=0$, we have:

$$0=(\alpha^4+\alpha^3+1)\alpha^{-4}=1+\alpha^{-1}+\alpha^{-4}.$$

This means that α^{-1} is a root of the polynomial x^4+x+1, which turns out to be irreducible and the remaining 3 elements of the field are indeed the other roots.

We now have the full factorization over *GF*(2):

$$x^{16}-x=x(x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$$

In fact we have the following theorem:

Theorem:

$x^{p^k}-x$ factors over GF(p) as the product of all the irreducible polynomials of degree m for $m\mid k$ over GF(p), and each factor appears exactly once.

The above example illustrates our theorem.

We now summarize the method for factoring x^n-1 over GF(p) using the following example:

$x^{35}-1$ over GF(5)

$x^{35}-1=(x^7-1)^5 \pmod 5$ so we need to factor x^7-1.

$x^{5^6-1}-1$, so that all its irreducible factors are factors of x^7-1, moreover they are distinct so we have that $x^7-1 \mid x^{5^6-1}-1$.
We therefore have to lookk at its factorisation over GF(5).
By the theorem we know it is the product of all irreducible polynomials of degrees dividing 6 over GF(5).

Since we have $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$, this tells us that the factors of the polynomial of degree 6 can be either of degrees 1,2,3 or 6. There can be no irreducible factor of degree 4 or 5.
We leave the remainder as an exercise.

14. Applications of Galois theory, constructibility by straight-edge and compass, squaring the circle, doubling the cube, trisecting an angle.

בניות סרגל ומחוגה:

Constructions with straight-edge and compass:

1. רקע היסטורי וחוקי המשחק

מהן הבניות גיאומטריות האפשריות במישור בעזרת סרגל ומחוגה?

זוהי שאלה גיאומטרית עם תשובה אלגברית!

The rules of the game:

"חוקי המשחק" הם:

מותר להשתמש בכלים הבאים בלבד:

- סרגל (straight-edge) ללא מידות מסומנות – רק לאפשר שרטוט קטעים ישרים.
- מחוגה.
- קטע באורך יחידה אחת.

Basic constructions.

למעשה זה מתאים ל-3 מתוך הפוסטולאטים של אוקלידס שמתייחסות לבניות בסיסיות:

1. **ניתן לשרטט קטע מנקודה לנקודה כלשהי.**
2. **ניתן להמשיך קטע לישר.**
3. **בהינתן נקודה, ניתן לשרטט מעגל סביבו בעל רדיוס כלשהו.**

בניות סרגל ומחוגה הן למעשה סדרה סופית של בניות כאלה.

Intersections of straight lines and circles.

הנחה בסיסית:

- נקודה נקבעת על-ידי חיתוך של ישרים, ישר ומעגל או שני מעגלים.
- קטע "נתון" על-ידי שתי נקודות.

דוגמאות פשוטות:

- בהינתן קטע באורך a וקטע באורך b ניתן לבנות קטעים באורכים הבאים:

$$a \pm b$$

$$a \cdot b$$

$$\frac{a}{b}$$

$$\sqrt{a}$$

- ניתן לחצות קטע.
- ניתן לחצות זוית.
- ניתן לבנות זוית ישרה.
- ניתן לבנות זוית בת 60 מעלות...
- ניתן לעביר ישר המקביל לישר נתון דרך נקודה כלשהי.

ראו למשל את האתר:

http://commons.wikimedia.org/wiki/Category:Animations_of_ruler_and_compass_constructions

The Classical questions:

1. Squaring the circle.
2. Doubling the cube.
3. Trisecting an angle.

השאלות הקלאסיות:

האם ניתן:

1. לרבע את המעגל?
2. להכפיל את הקוביה?
3. לחלק זוית לשלוש זויות שוות?

כעת, אלגברה

Reduction to the construction of points in the complex plane.

הערה חשובה:

בכל צעד בבניה בעזרת סרגל ומחוגה מתקבלת נקודה במישור.

למשל - בחיבור או כפל קטעים, הוצאת שורשים ריבועיים וכו' – אנו בונים נקודות.

כדי לעשות אלגבראיזציה של הבעיות, נניח שמדובר במישור המרוכב.
כל נקודה בו מזוהה עם מספר מרוכב.

ברור שכל נקודה במישור שרכיביה רציונליות ניתנת לבניה על-ידי סרגל ומחוגה.

השאלות הקלאסיות שקולות לשאלות הבאות:

1. לרבע את המעגל – שקול לבניית קטע שאורכו $\sqrt{\pi}$.
2. הכפלת הקוביה – שקולה לבניית קטע שאורכו $\sqrt[3]{2}$.
3. חלוקת זוית לשלוש זויות שוות –
שקולה לבעיה הבאה: אם נתונה הנקודה $z=\cos\alpha+i\sin\alpha$, האם נוכל לבנות את הנקודה: $\sqrt[3]{z}=\cos\frac{\alpha}{3}+i\sin\frac{\alpha}{3}$.

התשובות לשלוש השאלות הקלאסיות כולן שליליות!

ההוכחות הסתמכו על העבודות של Galois , Abel ואחרים בנוגע למציאת נוסחאות לפתרון.

כזכור, Galois גילה ש**אין** אפשרות לבטא באופן "דומה" את שורשיהם של המשוואה הפולינומיאלית הכללית מסדר n:

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = 0$$

- עבור $n \geq 5$.

הקשר לבניות סרל ומחוגה:

אם נתונים המספרים המרוכבים במישור a, b, c אז ניתן לבנות בעזרת סרגל ומחוגה גם את המספרים $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

לכן למעשה Galois גילה שאין אפשרות לבנות בעזרת סרגל ומחוגה את השורשים של הפולינום הנ"ל אם נתונים כל המקדמים.

הוא גם הוכיח משפט הנותן תנאי הכרחי ומספיק לכך שמספר מרוכב יהיה ניתן לבניה בעזרת סרגל ומחוגה.

Statement of Galois' Theorem and explanation:

Let $z_1, \cdots, z_n \in C$, $F = Q\left(z_1, \cdots, z_n, \overline{z_1}, \cdots, \overline{z_n}\right)$. Then z is constructible using straight-edge and compass if and only if $z \in F(u_1, \cdots, u_r)$ where $u_1^{\,2} \in F$, and each $u_i^{\,2} \in F(u_1, \cdots, u_{i-1})$.
A field of this type is called a **root tower** over F.

Examples of root towers over Q:

$$Q\left(\sqrt{2}\right) \subseteq Q\left(\sqrt{2}, \sqrt{\sqrt{2}-5}\right) \subseteq Q\left(\sqrt{2}, \sqrt{\sqrt{2}-5}, \sqrt{3}\right)$$

$$Q \subseteq Q(i) \subseteq Q\left(\sqrt{i}\right).$$

Answers to the classical questions:

Pierre Laurent Wantzel (June 5, 1814 in Paris – May 21, 1848 in Paris) proved in 1837 that constructions 2 and 3 in the list of classical questions above were impossible to solve using only compass and straightedge:

Clearly $\sqrt[3]{2}$ does not belong to a root tower since the dimension of a root tower over the rationals will be a power of 2, whereas $\left|Q\left(\sqrt[3]{2}\right) : Q\right| = 3$.

Similarly, given a complex z, such that $x^3 - z$ is irreducible over $Q(z)$ we also have $\left|Q\left(\sqrt[3]{z}\right) : Q\right| = 3$ hence we cannot construct $\sqrt[3]{z}$.

התשובה השלילית גם לשאלה הראשונה – ניתנה בעקבות ההוכחה ב- 1882 של Lindemann שהמספרים e, π אינם אלגבריים, כלומר אינם שורשים של פולינומים עם מקדמים רציונליים ולכן גם $\sqrt{\pi}$ אינו אלגברי, ואינו ניתן לבניה.

We note also that Galois' theorem shows that the ruler and straightedge constructions we listed above are essentially the only ones possible.

משפט Gauss-Wantzel:

Theorem (Gauss): A regular *n*-gon is constructible using straight-edge and compass if and only if $n = 2^e p_2 \times \cdots \times p_s$, $p_2, \ldots, p_s$ distinct Fermat primes.

גאוס הוכיח שניתן לבנות פוליגון משוכלל בעל n קדקדים (בעזרת סרגל ומחוגה) אם n הוא מכפלה של חזקה של 2 כלשהי יחד עם מספר כלשהו של ראשוניים של Fermat. כלומר:

$n = 2^e p_2 \times \cdots \times p_s$, כאשר $p_2, \ldots, p_s$ ראשוניים שונים של Fermat.

Wantzel הוכיח לאחר מכן שתנאי זה הוא גם הכרחי.

Fermat primes – definition and examples.

תזכורת:

מספר ראשוני של Fermat הוא מספר ראשוני מהצורה: $2^{2^n}+1$.

תחילה דוגמא קלה: $n = 3 = 2+1$.

וכידוע משולש משוכלל ניתן לבניה.

הפולינום המינימלי של הנקודה $\omega = e^{\frac{2\pi i}{3}} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ במישור המורכב הוא $x^2 + x + 1$.

ניתן לרשום את שורשיו: $\frac{-1 \pm i\sqrt{3}}{2}$ ואלה הנקודות שאנו בונים כאשר נבנה משולש שווה צלעות החסום במעגל ברדיוס 1.

This following example utilizes much of the material learned in the course and so is an appropriate conclusion:

Detailed construction of a regular pentagon:

בניה של הפנטגון

דוגמא מאתגרת יותר: $n = 5 = 2^2 + 1$.

לכן פנטגון משוכלל ניתן לבניה!

נתאר בניה של פנטגון כזה שחסום במעגל יחידה סביב ראשית הצירים במישור המורכב.

Algebraic construction of root tower: $Q \subseteq Q(\alpha) \subseteq Q(\rho)$

where $\alpha = \rho + \rho^4, \quad \rho = \sqrt[5]{1}$, calculating minimal polynomials of α over Q and of ρ over $Q(\alpha)$:

עלינו למעשה לבנות את הנקודה: $\rho = e^{\frac{2\pi i}{5}} = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$.

We show how solving the quadratic equations gives solution by radicals of $x^4 + x^3 + x^2 + x + 1 = 0$ and so explicit formulas for ρ using radicals, and so also of length of side of regular pentagon, inscribed in unit circle:

ρ הוא שורש של הפולינום: $x^4 + x^3 + x^2 + x + 1$.

נגדיר $\alpha = \rho + \bar{\rho} = \rho + \rho^4$.

אז α הוא מספר ממשי ונשים לב כי:

$$\alpha^2 = (\rho + \bar{\rho})^2 = \rho^2 + \rho^8 + 2\rho\bar{\rho} = \rho^2 + \rho^3 + 2$$
$$\alpha + \alpha^2 = \rho + \bar{\rho} + \rho^2 + \rho^3 + 2 = 1$$

לכן α הוא שורש של הפולינו הריבועי: $x^2 + x - 1$ ששורשיו הם: $\frac{-1 \pm \sqrt{1+4}}{2}$.

נבחר: $\alpha = \frac{-1+\sqrt{5}}{2}$ (הוא הפתרון שמתאים לשורש הפרימטיבי של 5 ברביע הראשון).

נשים לב כי השורש השני $\frac{-1-\sqrt{5}}{2}$ הוא הנגדי של יחס הזהב!

כעת נשים לב כי: $(x-\rho)(x-\bar{\rho}) = x^2 - (\rho + \bar{\rho})x + 1 = x^2 - \alpha x + 1$

לכן ρ הוא שורש של הפולינום: $x^2 - \alpha x + 1$ מעל $Q(\alpha)$ ששורשיו הם: $\frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2}$.

We now have the root tower: $Q \subseteq Q(\alpha) \subseteq Q(\rho)$.

נבחר שוב סימן + כדי לקבל שורש ברביע הראשון:

$$\rho = \frac{\alpha + \sqrt{\alpha^2 - 4}}{2} =$$

$$= \frac{\left(\frac{-1+\sqrt{5}}{2}\right) + \sqrt{\left(\frac{-1+\sqrt{5}}{2}\right)^2 - 4}}{2} = \frac{-1+\sqrt{5}}{4} + i\frac{\sqrt{10+2\sqrt{5}}}{4}$$

We have shown $Q(\rho) = Q\left(\sqrt{5}, i\sqrt{10+2\sqrt{5}}\right)$

אורך הצלע של הפנטגון יהיה איפוא המרחק בין הנקודה (1,0) לבין הנקודה:

$$\left(\frac{-1+\sqrt{5}}{4}, \frac{\sqrt{10+2\sqrt{5}}}{4}\right)$$

שהוא: $\sqrt{\left(\frac{-1+\sqrt{5}}{4} - 1\right)^2 + \frac{10+2\sqrt{5}}{16}} = \sqrt{\frac{5-\sqrt{5}}{2}}$

- וזה אכן אורך שניתן לבנות על-ידי סרגל ומחוגה!

Geometric construction using the algebraic information.

הבניה הגיאומטרית:

נסמן $A = (0,1)$.

נשים לב שהיתר במשולש ישר-הזוית שניצביו הם 1 וחצי יהיה: $\frac{\sqrt{5}}{2}$.

בעזרתו ניתן לבנות את הנקודה B ששיעוריה הן: $\left(-\frac{1}{2}+\frac{\sqrt{5}}{2}, 0\right)$.

המרחק ממנו ל-A יהיה אורך צלע הפנטגון כי:

$$AB = \sqrt{1+\left(-\frac{1}{2}+\frac{\sqrt{5}}{2}\right)^2} = \sqrt{\frac{5-\sqrt{5}}{2}}$$

נקצה אותו על המעגל מהנקודה A ונקבל קדקד שני בפנטגון – ומשם ניתן להשלים את שאר הקדקדים.

כעת נראה אנימציה של הבניה:

http://www.mathsisfun.com/geometry/construct-pentagon.html

קשר ליחס הזהב

ראינו כי בחישובים שלנו, קיבלנו בדרך את יחס הזהב.
למעשה הוא מופיע בפנטגון.

http://cage.ugent.be/~hs/polyhedra/dodeca.html

כשנצייר את האלכסונים, נקבל את הפנטגרם.

הוא בנוי ממשולשי זהב: אלה משולשים שווי-שוקיים שהיחס בין השוק לבסיס הוא יחס הזהב.

זויותיהן (במעלות) הן: 36, 72, 72.

נסיים בשתי פעילויות של גזירה וקיפולי נייר:

יחס הכסף וקיפולי נייר

כזכור, יחס הזהב הוא היחס x המקיים: $\frac{x}{1}=\frac{1}{x-1}$ וערכו הוא $\frac{1+\sqrt{5}}{2}$.
תכונתו של מלבן זהב הוא שכשמורידים ממנו ריבוע – נותר מלבן זהב קטן יותר.
יחס הכסף מוגדר באופן הבא:
הוא היחס x שגדול מ-1 והמקיים: $\frac{x}{1}=\frac{2x+1}{x}$.
נחשב אותו. עלינו לפתור: $x^2-2x-1=0$
נרצה את השורש שגדול מ-1 והוא $1+\sqrt{2}$.

מלבן כסף הוא מלבן שהיחס בין צלעותיו הוא יחס הכסף.

- יש לקחת דף A4.

היחס בין הצלע הארוכה לקצרה יותר היא בערך $\sqrt{2}$. תבדקו!
בהמשך נניח שהיחס הוא בדיוק $\sqrt{2}$!

- הורידו בעזרת קיפול וגזירה מתאימה, ריבוע שצלעו הצלע הקצרה של הדף.

מה שנשאר הוא מלבן שהיחס בין צלעותיו הוא $\sqrt{2}-1:1$.
נשים לב: $\frac{1}{\sqrt{2}-1}=\sqrt{2}+1$

כלומר - מה שנשאר הוא מלבן כסף.

- ממלבן זה נוריד שוב ריבוע.

היחס בין הצלעות במלבן השני שקיבלתם הוא שוב $\sqrt{2}:1$ כמו הדף ממנו יצאנו.
כשנוריד ממנו ריבוע – נקבל שוב מלבן כסף – וכן הלאה.

בניית הפנטגון בקיפולי נייר

http://www.jimloy.com/geometry/pentagon.htm

- קחו רצועת נייר באורך דף A4 ורוחב 6 ס״מ.
- תעשו קשר פשוט ברצועה.
- יש לדאוג להדק את הקשר ולהשטיח אותו.

נסו להסביר מדוע קיבלתם פנטגון משוכלל!