

Basic Abstract Algebra Factbook

©Robert Muth
muth@cs.arizona.edu

December 11, 1997

Contents

1 Homomorphisms	2
2 Groups	3
2.1 Basics	3
2.2 Homomorphisms	5
2.3 Direct and Semidirect Product	6
2.4 Normal Subgroups	7
2.5 Finitely Generated Abelian Groups	9
2.6 Exact Sequences	10
2.7 Sylow Subgroups	11
2.8 Simple Groups	12
2.9 Solvable Groups	13
2.10 Concrete Groups	14
3 (Commutative) Rings (with Unity)	15
3.1 Basics	15
3.2 Ideals	17
3.3 Chinese Remainder Theorem	19
3.4 Localization	20
4 Polynomial Rings	21
4.1 Polynomial Rings in One Variable	21
4.2 Polynomial Rings in Several Variables	23
4.3 Factorization and Irreducibility	27
4.4 Symmetric Polynomials	28
4.5 Concrete Polynomial Rings	29
4.6 Affine Varieties	30
4.7 Elimination Theory	32
4.8 Concrete Varieties	33
5 Fields	34
5.1 Basics	34
5.2 Field Extensions	35
5.3 Algebraic Closure	36

1 Homomorphisms

Definition 1.1 (Homomorphisms of A and B)

Definition 1.2 (Isomorphisms of A and B) $\text{Iso}[A, B] := \{f \in \text{Hom}[A, B] \mid f \text{ bijective}\}$

Definition 1.3 (Isomorphic) A, B isomorphic $\Leftrightarrow A \simeq B \Leftrightarrow \text{Iso}[A, B] \neq \emptyset$

Definition 1.4 (Epimorphisms of A and B) $\text{Epi}[A, B] := \{f \in \text{Hom}[A, B] \mid f \text{ surjective}\}$

Definition 1.5 (Monomorphisms of A and B) $\text{Mon}[A, B] := \{f \in \text{Hom}[A, B] \mid f \text{ injective}\}$

Definition 1.6 (Endomorphisms of A) $\text{End}[A] := \text{Hom}[A, A]$

Definition 1.7 (Automorphisms of a Group A) $\text{Aut}[A] := \text{Iso}[A, A]$

2 Groups

2.1 Basics

Definition 2.1 (Group)

Remark 2.2 G finite semigroup and $(\forall a, b, c \in G : ab = ac \Rightarrow b = c) \Rightarrow G$ group.

Definition 2.3 (Order of a Group G) $\text{Order}[G] := \text{Card}[G]$

Definition 2.4 (Order (Period) of an Element x of a Group G)

$\text{Order}[x] := \text{Card}[\{x^n \mid x \in G \text{ and } n \in \mathbb{N}\}]$

Fact 2.5 $\forall x \in G : \text{Order}[x] \mid \text{Order}[G]$

Fact 2.6 $\forall x \in G : x^{\text{Order}[x]} = e$

Definition 2.7 (Exponent of a Group G) $\text{Exponent}[G] = \text{lcm}_{x \in G} \text{Order}[x]$

Definition 2.8 (Subgroup H of a Group G) $H \subseteq G : \Leftrightarrow$

Fact 2.9 $\text{Exponent}[G] \mid \text{Order}[G]$

Fact 2.10 $\forall x \in G : x^{\text{Exponent}[G]} = e$

Fact 2.11 G abelian $\Rightarrow \exists x \in G : \text{Order}[x] = \text{Exponent}[G]$

Example 2.12 $\text{Exponent}[S_3] = 6, \{\text{Order}[x] \mid x \in S_3\} = \{1, 2, 3\}$

Corollary 2.13 $H \subseteq G \Rightarrow \text{Order}[H] \mid \text{Order}[G]$

Fact 2.14 $H_1, H_2 \subseteq G \Rightarrow H_1 \cap H_2 \subseteq G$

Definition 2.15 (Cyclic Group) *A group generated by a single element.*

Fact 2.16 *A cyclic group is abelian.*

Fact 2.17 $\forall a, b \in G : (ab)^2 = a^2b^2 \Rightarrow G$ abelian

Fact 2.18 *A group of prime order is cyclic.*

Fact 2.19 *A subgroups of a cyclic group is cyclic.*

Fact 2.20 *A group with no subgroups is cyclic and of prime order.*

Fact 2.21 *A subgroups of an abelian group is abelian.*

Theorem 2.22 G abelian and $\forall n \in \mathbb{N} : \text{Card}[\{x \in G \mid x^n = e\}] \leq n \Rightarrow G$ cyclic

Fact 2.23 $G = \langle a \rangle$ and $\text{Order}[G] = n \Rightarrow$ the generators of G are $\{a^m \mid \text{Gcd}(n, m) = 1\}$

Fact 2.24 *An automorphism of a cyclic group maps a generator to a generator.*

Corollary 2.25 G cyclic and $\text{Order}[g] = n \Rightarrow \text{Aut}[G] \simeq \mathbb{Z}_{\phi(n)}$

Corollary 2.26 G cyclic and $\text{Order}[g] = p^n$ prime $\Rightarrow \text{Aut}[G] \simeq \mathbb{Z}_{(p-1)p^{n-1}}$

Corollary 2.27 G infinite cyclic $\Rightarrow \text{Aut}[G] \simeq \mathbb{Z}_2$

Definition 2.28 (Left (Right) Translation of an Element y by an Element x) $T_x(y) := x \cdot y$

Definition 2.29 (Left (Right) Translation of a Subset by an Element x)

Remark 2.30 Translation by any x is a bijective mapping.

Definition 2.31 (Left (Right) Coset of a Subgroup H)

Remark 2.32 The translation of a subgroup is not necessarily a subgroup.

Theorem 2.33 For a given subgroup H of G all coset are either disjoint or equal, have the same cardinality, and cover G completely.

Definition 2.34 (Index of a subgroup H) $\text{Index}[G, H] := \text{Card}[\{x \cdot H \mid x \in G\}]$

Fact 2.35 $H \subseteq G \Rightarrow \text{Index}[G, H] = \text{Card}[G]/\text{Card}[H]$.

Corollary 2.36 $H \subseteq G \Rightarrow \text{Card}[G] = \text{Card}[H] \cdot \text{Index}[G, H]$

Remark 2.37 The traditional notation for the $\text{Index}[G, H]$ is $(G : H)$.

Fact 2.38 $G_1 \subseteq G_2 \subseteq G_3 \Rightarrow \text{Index}[G_3, G_1] = \text{Index}[G_3, G_2] \cdot \text{Index}[G_2, G_1]$

2.2 Homomorphisms

Theorem 2.39 $f \in \text{Hom}[A, B] \Rightarrow (f \text{ injective} \Leftrightarrow \text{Kernel}[f] = \{e\})$

Fact 2.40 $f \in \text{Hom}[A, B]$ and $H \subseteq A \Rightarrow f(H) \subseteq B$

Fact 2.41 $f \in \text{Hom}[A, B]$ and $H \subseteq B \Rightarrow f^{-1}(H) \subseteq A$

Fact 2.42 $f \in \text{Hom}[A, B]$ and $N \trianglelefteq B \Rightarrow f^{-1}(N) \trianglelefteq A$

Theorem 2.43 (First Isomorphism Theorem)

$f \in \text{Hom}[G, H] \Rightarrow G/\text{Kernel}[f] \simeq \text{Image}[f]$

Fact 2.44 For each normal subgroup N there is a canonical endomorphism with kernel N .

Theorem 2.45 (Second Isomorphism Theorem)

$N \subseteq \text{Normalizer}[G, H] \Rightarrow H/(H \cap N) \simeq (H \cdot N)/N$

Corollary 2.46 $N \trianglelefteq G \Rightarrow H/(H \cap N) \simeq (H \cdot N)/N$

Fact 2.47 $N_1, N_2 \trianglelefteq G$ and $N_1 \subseteq N_2 \Rightarrow N_1 \trianglelefteq N_2$

Fact 2.48 $N_1, N_2 \trianglelefteq G$ and $N_1 \subseteq N_2 \Rightarrow N_2/N_1 \trianglelefteq G/N_1$

Theorem 2.49 (Third Isomorphism Theorem)

$N_1, N_2 \trianglelefteq G$ and $N_1 \subseteq N_2 \Rightarrow (G/N_1)/(N_2/N_1) \simeq G/N_2$

Theorem 2.50

$f \in \text{Hom}[A, B]$ and $N_B \trianglelefteq B$ and $N_A = f^{-1}(N_B) \Rightarrow A/N_A \simeq B/N_B$

Fact 2.51 The homomorphic image of cyclic group is a cyclic group.

Fact 2.52 The homomorphic image of abelian group is an abelian group.

Fact 2.53 The homomorphic image of a group is a group.

2.3 Direct and Semidirect Product

Definition 2.54 ((External) Direct Product of Two Groups A, B)

$A \times B :=$

Theorem 2.55 $G = A \times B \Rightarrow A \times \{e_B\} \trianglelefteq G$

Fact 2.56 *The direct product of two groups is a group.*

Definition 2.57 (Product of Two Subgroups H_1, H_2) $H_1 \cdot H_2 := \{h_1 h_2 \mid h_1 \in H_1 \text{ and } h_2 \in H_2\}$

Theorem 2.58 $A, B \trianglelefteq G$ and $A \cdot B = B \cdot A = G \Rightarrow G/A$ isomorphic $B/(A \cap B)$

Remark 2.59 $H_1 \cdot H_2$ is not necessarily a subgroup

Fact 2.60 $H_1 \cdot H_2 \subseteq G \Leftrightarrow H_1 \cdot H_2 = H_2 \cdot H_1$

Fact 2.61 $H_1 \subseteq \text{Normalizer}[G, H_2] \Rightarrow H_1 \cdot H_2 = H_2 \cdot H_1$

Corollary 2.62 $H_1 \trianglelefteq G \Rightarrow H_1 \cdot H_2 = H_2 \cdot H_1$

Fact 2.63 $H_1, H_2 \trianglelefteq G$ and $H_1 \cdot H_2 = G \Rightarrow G/H_1 \simeq H_2/(H_1 \cap H_2)$

Fact 2.64 $H_1, H_2 \trianglelefteq G$ and $H_1 \cdot H_2 = G \Rightarrow G/(H_1 \cap H_2) \simeq H_1/(H_1 \cap H_2) \times H_2/(H_1 \cap H_2)$

Definition 2.65 (Semidirect (Internal Direct) Product) of a Normal Subgroup N and a Subgroup H

$N \rtimes H \Leftrightarrow H \cdot N = G$ and $H \cap N = \{e\}$

Remark 2.66 *Each element of $g \in G$ has a unique representation as $h \cdot n$ where $h \in H, n \in N$.*

2.4 Normal Subgroups

Definition 2.67 (Conjugation of an Element y by an Element x) $\gamma_x(y) := xyx^{-1}$

Definition 2.68 (Inner Automorphism) *An automorphism described by conjugation.*

Definition 2.69 (Conjugation of a Set S by an Element x)

Fact 2.70 $\forall x \in G : H \subseteq G \Rightarrow \gamma_x(H) \subseteq G$

Definition 2.71 (Normal Subgroup N of a Group G) $H \trianglelefteq G \Leftrightarrow \forall x \in G : xH = Hx$

Remark 2.72 *A right coset of a normal subgroup is also a left coset.*

Fact 2.73 $N \trianglelefteq G \Rightarrow \gamma_x(N) = N$

Corollary 2.74 $N \trianglelefteq G$ and $n \in N \Rightarrow \forall x \in G : \gamma_x(n) \in N$

Fact 2.75 (Intersection of Normal subgroups) $H_1, H_2 \trianglelefteq G \Rightarrow H_1 \cap H_2 \trianglelefteq G$

Fact 2.76 (Normality is not Transitive) $G_1 \trianglelefteq G_2 \trianglelefteq G_3 \not\Rightarrow G_1 \trianglelefteq G_3$

Remark 2.77 *Normal subgroups are left invariant by inner automorphisms.*

Remark 2.78 *All subgroups of an abelian group are normal.*

Fact 2.79 *The kernel of a homomorphism is a normal subgroup.*

Definition 2.80 (Factor Group of G and one of its normal subgroups N) $G/N :=$

Theorem 2.81 (Factor Group)

$H \trianglelefteq G \Rightarrow G/H := \{xH \mid x \in G\}$ is a group with group law $xH \cdot yH = xyH$

Fact 2.82 *A factor group of a cyclic group is cyclic.*

Fact 2.83 *A factor group of a abelian group is abelian.*

Definition 2.84 (Normalizer of a Subset S of G) $\text{Normalizer}[G, S] := \{g \in G \mid g \cdot S = S \cdot g\}$

Theorem 2.85 $N \subseteq \text{Normalizer}[G, H] \Rightarrow H/(H \cap N) \simeq (H \cdot N)/N$

Fact 2.86 $\forall S \subseteq G : \text{Normalizer}[G, S] \subseteq G$

Fact 2.87 $\text{Normalizer}[G, G] = G$

Fact 2.88 $\text{Normalizer}[G, \{e\}] = G$

Fact 2.89 $H \subseteq G \Rightarrow H \trianglelefteq \text{Normalizer}[G, H]$

Remark 2.90 *The normalizer of H is the biggest subgroup that H is normal in.*

Fact 2.91 $N_1, N_2 \trianglelefteq H$ and $N_1 \subseteq N_2 \Rightarrow N_1 \trianglelefteq N_2$

Corollary 2.92 $H \trianglelefteq N \subseteq G \Rightarrow K \subseteq \text{Normalizer}[G, H]$

Fact 2.93 $K \subseteq \text{Normalizer}[G, H] \Rightarrow K \cap H \trianglelefteq H$

Fact 2.94 $K \subseteq \text{Normalizer}[G, H] \Rightarrow K \cdot H = H \cdot K \subseteq G$

Definition 2.95 (Centralizer of a subset S of G) $\text{Centralizer}[G, S] := \{x \in G \mid \forall s \in S : xs = sx\}$

Fact 2.96 $\forall S \subseteq G : e \in \text{Centralizer}$

Fact 2.97 $\text{Centralizer}[G, S] \trianglelefteq \text{Normalizer}[G, S]$

Definition 2.98 (Center of a Group G) $\text{Center}[G] := \text{Centralizer}[G, G]$

Remark 2.99 *The elements of the center of a group commute with every other element of the group.*

Theorem 2.100 $x \in \text{Center}[G] \Leftrightarrow \text{Normalizer}[\{x\}] = G$

Fact 2.101 $\text{Centralizer}[G, H] \trianglelefteq \text{Normalizer}[G, H]$

Fact 2.102 $\text{Normalizer}[\{x\}] = \text{Centralizer}[\{x\}]$

Definition 2.103 (Orbit of an element x of a Group G) $\text{Orbit}[G, x] := \{yxy^{-1} \mid y \in G\}$

Fact 2.104 $\text{Card}[\text{Orbit}[G, x]] = \text{Index}[G, \text{Normalizer}[G, \{x\}]]$

Corollary 2.105 $\text{Card}[\text{Orbit}[G, x]] \mid \text{Card}[G]$

Theorem 2.106 (Class Equation)

Fact 2.107 $\text{Normalizer}[\text{Center}[G]] = G$

Fact 2.108 $H \subseteq G$ and $\text{Index}[G, H] = p$ and p smallest prime dividing $\text{Order}[G] \Rightarrow H \trianglelefteq G$

Definition 2.109 (Maximal Normal Subgroup)

2.5 Finitely Generated Abelian Groups

Definition 2.110 (Finitely Generated Group)

Definition 2.111 (Torsion Element of a Group) *An element of finite order*

Definition 2.112 (Torsion Group) *All elements are torsion elements*

Fact 2.113 (A finite groups is always a torsion group)

Definition 2.114 (Torsion Free Group) *No element other than e is a torsion element*

Remark 2.115 G abelian $\Rightarrow x \mapsto x^n \in \text{Aut}[G]$

Theorem 2.116 *A finitely generated abelian group is the semidirect product of its torsion subgroup and a torsion free subgroup*

Theorem 2.117 *A finitely generated torsion free abelian group G is isomorphic to $Z \times \dots \times Z = Z^b$ for some some unique b , the betti number of G .*

2.6 Exact Sequences

Definition 2.118 (Exact sequence)

Fact 2.119

$$0 \mapsto A \mapsto 0 \text{ exact} \Rightarrow A = 0$$

Fact 2.120

$$0 \mapsto A \xrightarrow{f} B \text{ exact} \Rightarrow f \text{ injective}$$

Fact 2.121

$$A \xrightarrow{f} B \mapsto 0 \text{ exact} \Rightarrow f \text{ surjective}$$

Fact 2.122

$$0 \mapsto A \xrightarrow{f} B \mapsto 0 \text{ exact} \Rightarrow f \text{ bijective}$$

Fact 2.123

$$0 \mapsto A \xrightarrow{f} B \xrightarrow{g} C \mapsto 0 \text{ exact} \Rightarrow C \simeq B/f(A)$$

2.7 Syslow Subgroups

Definition 2.124 (p-Group) G p -Group $\Leftrightarrow \text{Order}[G] = p^n$ and p prime

Definition 2.125 (p-Subgroup) $H \subseteq G$ p -Subgroup $\Leftrightarrow \text{Order}[H] = p^n$ and p prime

Definition 2.126 (p-Syslow Subgroup) $H \subseteq G$ p -Syslow Subgroup $\Leftrightarrow p^{n+1} \nmid |G|$ and $|H| = p^n$ and p prime

Theorem 2.127 (Cauchy) p prime and $p \mid \text{Order}[G] \Rightarrow \exists a \in G : \text{Order}[a] = p$

Corollary 2.128 p prime and $p \mid \text{Order}[G] \Rightarrow \mathbb{Z}_p \subseteq G$

Theorem 2.129 (Syslow) p prime and $p^n \mid |G| \Rightarrow \exists H \subseteq G : \text{Order}[H] = p^n$

Theorem 2.130 Every p -subgroup is contained in some p -Syslow subgroup.

Theorem 2.131 All p -Syslow subgroups are conjugate.

Corollary 2.132 The number of different p -Syslow subgroups divides the order of the group

Theorem 2.133 The number of different p -Syslow subgroups is $1 + kp$.

Theorem 2.134 A p -Group has a nontrivial center.

Fact 2.135 $\text{Order}[G] = p^k$ and G abelian $\Rightarrow p^2 \nmid \text{Card}[G / \text{Commutator}[G]]$

Corollary 2.136 $\text{Order}[G] = p^2$ and p prime $\Rightarrow G$ abelian

2.8 Simple Groups

Definition 2.137 (Simple Group) *A group with no nontrivial normal subgroups.*

Corollary 2.138 (Alternative Definition of Simple Group) *A group whose only homomorphisms to other groups are the identity map and the map that is 1 everywhere.*

Definition 2.139 (Composite Group) *A group which is not simple.*

Fact 2.140 *Cyclic groups of prime order are simple.*

Fact 2.141

$$\{i, j\} = \{r, s\} \Rightarrow (ij)(rs) = (ijr)(jrs)$$

$$i = r \Rightarrow (ij)(rs) = (ij)(is) = (isj)$$

$$\{i, j\} \cap \{r, s\} = \emptyset \Rightarrow (ij)(rs) = (ijr)(jrs)$$

Remark 2.142 $3 \leq n \Rightarrow A_n$ is generated by all the three cycles.

Fact 2.143 $5 \leq n \Rightarrow$ all three cycles are conjugate.

Fact 2.144 $5 \leq n \Rightarrow$ a proper subgroup of A_n contains a three cycle.

Fact 2.145 $5 \leq n \Rightarrow A_n$ is simple

Fact 2.146 *All simple groups belong to one of the following four classes:*

- *cyclic groups of prime order*
- *alternating groups*
- *groups of Lie type*
- *26 sporadic groups the largest of which is the Monster group of order $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$*

2.9 Solvable Groups

Fact 2.147 $ab = (aba^{-1}b^{-1})ba$

Theorem 2.148 $\text{Commutator}[G] = \{xyx^{-1}y^{-1} \mid x, y \in G\}$

Fact 2.149 $\text{Commutator}[G] \trianglelefteq G$

Fact 2.150 $G \text{ abelian} \Rightarrow \text{Commutator}[G] = \{e\}$

Theorem 2.151 $f \in \text{Hom}[A, B] \text{ and Babelian} \Rightarrow \text{Commutator}[A] \subseteq \text{Kernel}[f]$

Corollary 2.152 $G/\text{Commutator}(G) \text{ is abelian.}$

Corollary 2.153 $H \subseteq G \Rightarrow G/H \text{ abelian} \Leftrightarrow \text{Commutator}[G] \subseteq H$

Definition 2.154 (Tower (Chain) of Subgroups)

$$G_n \subseteq \dots \subseteq G_0$$

Definition 2.155 (Normal Tower (Chain) of Subgroups)

$$G_n \subseteq \dots \subseteq G_0 \text{ normal} :\Leftrightarrow G_n \trianglelefteq \dots \trianglelefteq G_0$$

Definition 2.156 (Abelian Tower of Subgroups)

$$G_n \trianglelefteq \dots \trianglelefteq G_0 \text{ abelian} :\Leftrightarrow \forall 1 \leq i \leq n : G_i/G_{i-1} \text{ abelian}$$

Definition 2.157 (Cyclic Tower of Subgroups)

$$G_n \trianglelefteq \dots \trianglelefteq G_0 \text{ cyclic} :\Leftrightarrow \forall 1 \leq i \leq n : G_i/G_{i-1} \text{ cyclic}$$

Fact 2.158 $f \in \text{Hom}[A, B] \text{ and } B_n \subseteq \dots \subseteq B_0 = B \text{ normal} \Rightarrow f^{-1}(B_n) \subseteq \dots \subseteq f^{-1}(B_0) \text{ normal}$

Fact 2.159 $H \subseteq G \text{ and } G_n \subseteq \dots \subseteq G_0 = B \text{ normal} \Rightarrow G_n \cap H \subseteq \dots \subseteq B_0 \cap H \text{ normal}$

Fact 2.160 $f \in \text{Hom}[A, B] \text{ and } B_n \subseteq \dots \subseteq B_0 = B \text{ abelian} \Rightarrow f^{-1}(B_n) \subseteq \dots \subseteq f^{-1}(B_0) \text{ abelian}$

Fact 2.161 $f \in \text{Hom}[A, B] \text{ and } B_n \subseteq \dots \subseteq B_0 = B \text{ cyclic} \Rightarrow f^{-1}(B_n) \subseteq \dots \subseteq f^{-1}(B_0) \text{ cyclic}$

Definition 2.162 (Reduced Tower) *inclusion is strict*

Definition 2.163 (Refinement of a Tower of Subgroups)

Theorem 2.164 (Two normal towers of subgroups have isomorphic refinements)

Definition 2.165 (Solvable Group)

$$G \text{ solvable} :\Leftrightarrow \exists \{G_i\}_{0 \leq i \leq n} : G_n \trianglelefteq \dots \trianglelefteq G_0 \text{ abelian and } G_0 = G \text{ and } G_n = \{e\}$$

Fact 2.166 *An abelian group is solvable.*

Fact 2.167 $H \subseteq G \text{ and } G \text{ solvable} \Rightarrow H \text{ solvable}$

Theorem 2.168 $H \trianglelefteq G : G \text{ solvable} \Leftrightarrow G/N \text{ solvable}$

Corollary 2.169 *Factor groups of solvable groups are solvable.*

Theorem 2.170 (A p-Group is solvable)

Fact 2.171 *A noncyclic simple group is not solvable.*

Fact 2.172 $G \text{ simple solvable} \Rightarrow G \simeq \mathbb{Z}_p$

Fact 2.173 $5 \leq n \Rightarrow S_n \text{ is not solvable}$

Fact 2.174 $p, q \text{ prime and } p \neq q \text{ and } \text{Order}[G] = pq \Rightarrow G \simeq \mathbb{Z}_{qp}$

Corollary 2.175 $p, q \text{ prime and } p \neq q \text{ and } \text{Order}[G] = pq \Rightarrow G \text{ solvable}$

Theorem 2.176 (Feit-Thompson) $\text{Order}[G] \text{ odd} \Rightarrow G \text{ solvable}$

2.10 Concrete Groups

Definition 2.177 (General Linear Group ($GL_n(F)$), Invertible Matrices)

$$GL_n(F) = \{M \in M_n(F) \mid \det(M) \neq 0\}$$

Definition 2.178 (Special Linear Group ($SL_n(F)$))

$$SL_n(F) = \{M \in M_n(F) \mid \det(M) = 1\}$$

Definition 2.179 (Orthogonal Group ($O_n(F)$))

$$O_n(F) = \{M \in M_n(F) \mid M^t M = E\}$$

Fact 2.180 ($O_n(R)$ represents the length preserving linear mappings)

Fact 2.181 (A length preserving mapping also preserves angles)

Definition 2.182 (Special Orthogonal Group ($SO_n(F)$), Rotations)

$$SO_n(F) = \{M \in O_n(F) \mid \det(M) = 1\}$$

Remark 2.183 (Matrices over rings)

It is possible to define determinants of matrices over arbitrary rings. An invertible matrix is a matrix whose determinant is a unit.

Fact 2.184 (There are only two nonisomorphic groups of order 4)

$$Z_4 \text{ and } Z_2 \times Z_2$$

Fact 2.185 (A group of order p^2 is abelian)

$$|G| = p^2 \text{ and } p \text{ prime} \Rightarrow G \text{ abelian}$$

Fact 2.186 (A group of even order has an element of order 2)

Fact 2.187 (A group of order less than 60 is solvable)

Example 2.188 (Dihedral Group)

Fact 2.189 (A group of order less than 6 is abelian)

Fact 2.190 ($\langle \sigma \rangle$ is normal in S_n)

$$\sigma = (1234 \dots n) \in S_n \Rightarrow \langle \sigma \rangle \trianglelefteq S_n$$

3 (Commutative) Rings (with Unity)

3.1 Basics

Definition 3.1 ((Commutative) Ring (with Unity))

Example 3.2 (The Ring \mathbb{Z})

Example 3.3 (The Rings \mathbb{Z}_n)

Definition 3.4 (Subring A of a Ring B) $A \subseteq B \Leftrightarrow$

Definition 3.5 (Units of a Ring R) $\text{Units}[R] := \{r \in R \mid \exists s \in R : rs = 1\}$

Fact 3.6 $\text{Card}[\text{Units}[\mathbb{Z}_n]] = \phi(n)$

Remark 3.7 *Do not confuse a unit with the unity.*

Definition 3.8 (Characteristic of a Ring R) $\text{Char}[R] := \min\{n \in \mathbb{N} \mid \underbrace{1 + \dots + 1}_{n \text{ times}} = 0\}$

Remark 3.9 *If the characteristic is undefined we set it to zero.*

Fact 3.10 $\text{Char}[R] = n \Rightarrow \mathbb{Z}_n \subseteq R$

Fact 3.11 $\text{Char}[R] = 0 \Rightarrow \mathbb{Z} \subseteq R$

Fact 3.12 $R \text{ finite} \Rightarrow \text{Char}[R] > 0$

Definition 3.13 (Entire Ring, Integral Domain (ID))

A ring with no zero-divisors.

Fact 3.14 *The characteristic of an entire ring is prime or zero.*

Theorem 3.15 *The cancellation laws hold in a ring \Leftrightarrow the ring is entire.*

Fact 3.16 $R \text{ finite entire} \Rightarrow R \text{ field}$

Definition 3.17 (Irreducible Element f of an Entire Ring)

$f \text{ irreducible} \Leftrightarrow f \notin \text{Units}[R] \text{ and } f = ab \Rightarrow a \in \text{Units}[R] \text{ or } b \in \text{Units}[R]$

Definition 3.18 (Factorial Ring, Unique Factorization Domain (UFD))

An entire ring so that every nonzero element has a unique factorization into irreducible elements.

Remark 3.19 *In a factorial ring we have a notion of gcd and lcm.*

Example 3.20 (Non-factorial Ring) $\mathbb{Z}[\sqrt{-5}]$ is not factorial since $(9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}))$

Definition 3.21 (Principal Ring, Principal Ideal Domain (PID))

An entire ring such that every ideal is principal.

Definition 3.22 (Euclidean Ring)

An entire ring with a function $g : R \mapsto \mathbb{N}$ so that

Definition 3.23 (Division Ring, Skew-Field)

Ring where every nonzero element is a unit.

Example 3.24 (Skew Field) $GL_n(R)$ **Example 3.25 (Skew Field) Quaternion (Skew) Field****Theorem 3.26 (Wedderburn) R finite division ring $\Rightarrow R$ field****Definition 3.27 (Field)**

An entire ring where every nonzero element is a unit.

Fact 3.28 R field $\Rightarrow R$ euclidean

Fact 3.29 R finite entire $\Rightarrow R$ field

Fact 3.30 The number of elements in a finite field is a prime power.

Fact 3.31 Two finite fields with the same number of elements are isomorphic.

Fact 3.32 k^* is a multiplicative cyclic group.

Definition 3.33 (Noetherian Ring) A ring where each ideal is finitely generated.

Fact 3.34 R field $\Rightarrow R$ euclidean

Example 3.35 (Euclidean Ring Which is not a Field) $\mathbb{C}[x]$

Fact 3.36 R euclidean $\Rightarrow R$ principal

Example 3.37 (Principal Ring Which is not a Euclidean Ring)

Fact 3.38 R principal $\Rightarrow R$ noetherian

Example 3.39 (Noetherian Ring Which is not a Principal Ring) $\mathbb{C}[x, y]$

Fact 3.40 R principal $\Rightarrow R$ factorial

Example 3.41 (Factorial Ring Which is not a Principal Ring)**Definition 3.42 (Quotient Field of an Entire Ring)**

3.2 Ideals

Definition 3.43 ((Two-sided) Ideal I of a Ring R) $I \subseteq R \trianglelefteq \Leftrightarrow \forall r \in R, i \in I : ri \in I$

Theorem 3.44 $f \in \text{Hom}[A, B] \Rightarrow f \text{ injective} \Leftrightarrow \text{Kernel}[f] = \{0\}$

Theorem 3.45 $f \in \text{Hom}[A, B] \Rightarrow \text{Kernel}[f] \trianglelefteq A$

Fact 3.46 $f \in \text{Hom}[A, B]$ and $H \subseteq A \Rightarrow f(H) \subseteq B$

Fact 3.47 $f \in \text{Hom}[A, B]$ and $I_B \trianglelefteq B$ and $I_A := f^{-1}(I_B) \Rightarrow I_A \trianglelefteq A$

Definition 3.48 (Factor Ring) R/I

Fact 3.49 $I \trianglelefteq R$ and $I \cap \text{Units}[R] \neq \emptyset \Rightarrow I = R$

Definition 3.50 (Ideal Generated by a Set S)

$\langle S \rangle := \{r \in R \mid \exists a_1, \dots, a_n \in R, s_1, \dots, s_n \in S : \sum_{1 \leq i \leq n} a_i \cdot s_i = r\}$

Definition 3.51 (Basis of an Ideal) *The elements of a generator of a ideal are also called a basis.*

Definition 3.52 (Product of Two Ideals I, J) $I \cdot J := \{\sum_k i_k j_k \mid i_k \in I \text{ and } j_k \in J\}$

Fact 3.53 $I, J \trianglelefteq R \Rightarrow I \cdot J \trianglelefteq R$

Fact 3.54 $I \cdot J = \langle \{i \cdot j \mid i \in I \text{ and } j \in J\} \rangle$

Definition 3.55 (Sum of Two Ideals I, J) $I + J := \{i + j \mid i \in I \text{ and } j \in J\}$

Fact 3.56 $I, J \trianglelefteq R \Rightarrow I + J \trianglelefteq R$

Remark 3.57 $I + J$ is the smallest ideal containing I and J .

Fact 3.58 $\langle a_1, \dots, a_k \rangle = \langle a_1 \rangle + \dots + \langle a_k \rangle$

Definition 3.59 (Intersection of Ideals) $I \cap J \trianglelefteq R \Rightarrow I \cap J \trianglelefteq R$

Fact 3.60 $I, J \trianglelefteq R \Rightarrow I \cdot J \subseteq I \cap J$

Example 3.61 $\langle x, y \rangle \cdot \langle x, y \rangle = \langle x^2, xy, y^2 \rangle \neq \langle x, y \rangle$

Fact 3.62 $A, B \trianglelefteq R$ and $A + B = R \Rightarrow A \cdot B = A \cap B$

Definition 3.63 (Quotient (Colon) Ideal of Two Ideal I, J) $I : J := \{r \in R \mid \forall j \in J : r \cdot j \in I\}$

Fact 3.64 $I : J \trianglelefteq R$

Fact 3.65 $I \subseteq I : J$

Fact 3.66 $I \cdot J \subseteq K \Leftrightarrow I \subseteq K : J$

Fact 3.67 $I : J = R \Leftrightarrow J \subseteq I$

Fact 3.68 $I : R = I$

Fact 3.69 $I : (J : K) = I : (J \cdot K)$

Fact 3.70 $(I_1 \cap I_2) : J = (I_1 : J) \cap (I_2 : J)$

Fact 3.71 $I : (J_1 + J_2) = (I : J_1) \cap (I : J_2)$

Fact 3.72 $\langle f_1, \dots, f_k \rangle = I \cap \langle g \rangle \Rightarrow \langle f_1/g, \dots, f_k/g \rangle = I$

Definition 3.73 (Unit Ideal) *The ideal consisting of all the units of the ring.*

Fact 3.74 $\text{Units}[R]$ forms a field.

Definition 3.75 (Proper Ideal) I proper $:\Leftrightarrow I \neq R$ and $I \neq \emptyset$

Fact 3.76 R field $\Leftrightarrow (I \trianglelefteq R \Rightarrow \neg I \text{ proper})$

Definition 3.77 (Finitely Generated Ideal) *Ideal generated by a finite set.*

Definition 3.78 (Principal Ideal) *Ideal generated by a singleton set.*

Fact 3.79 R entire $\Rightarrow \langle a \rangle = \langle b \rangle \Leftrightarrow \exists c \in \text{Units}[R] : ac = b$

Theorem 3.80 R factorial and $\langle a \rangle, \langle b \rangle \trianglelefteq R \Rightarrow \langle a \rangle \cap \langle b \rangle = \langle \text{lcm}[a, b] \rangle$

Remark 3.81 *The intersection of principal ideals in a factorial ring is a principal ideal.*

Definition 3.82 (Radical Ideal) I radical $:\Leftrightarrow i^n \in I \Rightarrow i \in I$

Definition 3.83 (Prime Ideal) $I \trianglelefteq R$ prime $:\Leftrightarrow (a \cdot b \in I \Rightarrow a \in I \text{ or } b \in I)$

Theorem 3.84 $I \trianglelefteq R$ prime $\Rightarrow R/I$ entire

Fact 3.85 $\{0\} \trianglelefteq R$ prime $\Leftrightarrow R$ entire

Fact 3.86 $I = \langle r \rangle \trianglelefteq R$ and $\langle r \rangle$ prime $\Rightarrow r$ irreducible

Remark 3.87 $\langle 3 \rangle \trianglelefteq \mathbb{Z}[\sqrt{-5}]$ and $9 \in \langle 3 \rangle$ but $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$

Theorem 3.88 R factorial $\Rightarrow (\langle r \rangle \text{ prime} \Leftrightarrow r \text{ irreducible})$

Remark 3.89 *A irreducible element in a factorial ring is often called a prime.*

Fact 3.90 $f \in \text{Hom}[A, B]$ and $I_B \trianglelefteq B$ prime and $I_A := f^{-1}(I_B) \Rightarrow I_A \trianglelefteq A$ prime

Definition 3.91 (Primary Ideal) $I \trianglelefteq R$ primary $:\Leftrightarrow (a \cdot b \in I \Rightarrow a \in I \text{ or } \exists 1 \leq n : b^n \in I)$

Definition 3.92 (Maximal Ideal) $I \trianglelefteq R$ maximal $:\Leftrightarrow I \neq R$ and $(I \trianglelefteq U \trianglelefteq R \Rightarrow U = I \text{ or } U = R)$

Theorem 3.93 $I \trianglelefteq R$ maximal $\Rightarrow I$ prime

Remark 3.94 $\langle xy \rangle \trianglelefteq \mathbb{C}[x, y]$ prime but $\langle xy \rangle \subset \langle x \rangle$

Theorem 3.95 R principal $\Rightarrow (I \trianglelefteq R \text{ maximal} \Leftrightarrow I \text{ prime})$

Corollary 3.96 R principal and $p \in R$ irreducible $\Rightarrow \langle r \rangle$ maximal

Remark 3.97 *Every ideal is contained in some maximal ideal.*

Theorem 3.98 $I \trianglelefteq R$ maximal $\Leftrightarrow R/I$ field

Fact 3.99 $f \in \text{Hom}[A, B]$ and f injective and $I_B \trianglelefteq B$ maximal and $I_A := f^{-1}(I_B) \Rightarrow I_A \trianglelefteq A$ maximal

Fact 3.100 F field and $\text{Char}[F] = p \Rightarrow \mathbb{Z}_p \subseteq F$

Fact 3.101 F field and $\text{Char}[F] = 0 \Rightarrow \mathbb{Q} \subseteq F$

3.3 Chinese Remainder Theorem

Theorem 3.102 (Chinese Remainder Theorem)

$$I_1, \dots, I_n \trianglelefteq R \text{ and } \forall i \neq j : I_i + I_j = R \Rightarrow \forall x_1, \dots, x_m \in R : \exists x \in R : \forall i : x \equiv_{I_i} x_i$$

Corollary 3.103

$$a_i \in N \text{ and for all } i, j : \gcd(a_i, a_j) = 1 \Rightarrow Z_{a_1} \times \dots \times Z_{a_n} = Z_{a_1 \dots a_n}$$

3.4 Localization

Definition 3.104 (Multiplicative Subset M of a Ring R) $M \subseteq R \Leftrightarrow$

Definition 3.105 (Quotient Ring)

Definition 3.106 (Localization) $\frac{R}{M} :=$

Remark 3.107 $S = R^* \Rightarrow S^{-1}R = R$

Definition 3.108 (Quotient Field of an ID (Field of Fractions))

$$R \text{ entire and } S = R \setminus 0 \Rightarrow S^{-1}R \text{ field}$$

Theorem 3.109 (Every entire ring can be imbedded in a field)

Remark 3.110 (Quotient Field of a Polynomial Ring)

$$S = R^* \Rightarrow S^{-1}R = R$$

Definition 3.111 (Local Ring)

Commutative ring with a unique maximal ideal.

Theorem 3.112 (Local Ring at a Prime Ideal) I prime and $S = (R \setminus I) \Rightarrow S^{-1}R$ local ring

Fact 3.113 $I \trianglelefteq R$ and $S \subseteq R \Rightarrow S^{-1}I \trianglelefteq S^{-1}R$

Fact 3.114

$$\begin{aligned} I_1, I_2 \trianglelefteq R \text{ and } S \subseteq R \Rightarrow \quad & S^{-1}(I_1 + I_2) = S^{-1}I_1 + S^{-1}I_2 \text{ and} \\ & S^{-1}(I_1 \cap I_2) = S^{-1}I_1 \cap S^{-1}I_2 \text{ and} \\ & S^{-1}(I_1 I_2) = S^{-1}I_1 S^{-1}I_2 \end{aligned}$$

Theorem 3.115 R principal and $S \subseteq R \Rightarrow S^{-1}R$ principal

Theorem 3.116 R factorial and $S \subseteq R \Rightarrow S^{-1}R$ factorial

Theorem 3.117 R factorial and $I \trianglelefteq R$ prime $\Rightarrow R_I$ factorial

4 Polynomial Rings

4.1 Polynomial Rings in One Variable

Definition 4.1 (Polynomial Ring in One Variable) *A ring of the form $R[x]$ where x is variable and R is a ring.*

Theorem 4.2 R entire $\Rightarrow R[x]$ entire

Corollary 4.3 R field $\Rightarrow R[x]$ factorial

Corollary 4.4 R factorial $\Rightarrow R[x]$ factorial

Corollary 4.5 R noetherian $\Rightarrow R[x]$ noetherian

Remark 4.6 *If we assume that R is a field, we shall write $k[x]$.*

Definition 4.7 (Coefficient of a Monomial m of a Polynomial p) $\text{Coeff}[p, m] :=$

Definition 4.8 (Degree of a Polynomial p) $\text{Deg}[p] := \text{Max}\{\{x^n \mid \text{Coeff}[p, x^n] \neq 0\}\}$

Definition 4.9 (Leading Monomial of a Polynomial p) $\text{LeadM}[p] := x^{\text{Deg}[p]}$

Definition 4.10 (Leading Coefficient of a Polynomial p) $\text{LeadC}[p] := \text{Coeff}[p, \text{LeadM}[p]]$

Definition 4.11 (Leading Term of a Polynomial p) $\text{LeadT}[p] := \text{LeadC}[p] \cdot \text{LeadM}[p]$

Definition 4.12 (Monic Polynomial) p monic $:\Leftrightarrow \text{LeadC}[p] = 1$

Definition 4.13 (Rational Function) *Quotient of two polynomials.*

Definition 4.14 (Field of Rational Functions, $k(x)$)

Fact 4.15 $p \in k[x] : (p)$ maximal $\trianglelefteq \Leftrightarrow p$ prime

Remark 4.16 $f \in k[x]$ can be regarded as a function $f : k \mapsto k$.

Definition 4.17 (Evaluation Homomorphism) $\text{Eval}[f, x] :=$

Remark 4.18 $f = 0 \Rightarrow \forall x \in k : \text{Eval}[f, x] = 0$

Remark 4.19 $f = x^2 - x \in \mathbb{Z}_2[x] \Rightarrow \forall x \in \mathbb{Z}_2 : \text{Eval}[f, x] = 0$

Remark 4.20 $\forall x \in k : \text{Eval}[f, x] = 0 \not\Rightarrow f = 0$

Theorem 4.21 k infinite field and $\forall x \in k : \text{Eval}[f, x] = 0 \Rightarrow f = 0$

Corollary 4.22 k infinite field and $\forall x \in k : \text{Eval}[f, x] = \text{Eval}[g, x] \Rightarrow f = g$

Algorithm 4.23 (Division Algorithm for $k[x]$)

```

Divide[f, g] ≡
  q := 0
  r := f
  WHILE r ≠ 0 AND LeadT[g] \ LeadT[r] DO
    q := q + LeadT[r] / LeadT[g]
    r := r - LeadT[r] / LeadT[g] · g
  END
  RETURN (q, r)

```

Definition 4.24 $(\text{Div}[f, g], \text{Rem}[f, g]) := \text{Divide}[f, g]$

Corollary 4.25 *Let $g \in k[x]$ be a nonzero polynomial then every $f \in k[x]$ can be written as $f = q \cdot g + r$ where $\text{Deg}[r] < \text{Deg}[g]$. Furthermore q and r are unique up to multiplication by units.*

Corollary 4.26 $I \trianglelefteq k[x] \Rightarrow I = \langle f \rangle$ where f is a minimal degree polynomial in I .

Corollary 4.27 R field $\Rightarrow R[x]$ principal

Definition 4.28 (Greatest Common Divisor of Two Polynomials, GCD) *A polynomial g so that $g \mid f_1, f_2$ and $\forall p \mid f_1, f_2 : p \mid g$*

Fact 4.29 *The GCD is unique up to multiplication with units.*

Remark 4.30 *In order to make the GCD unique we usually pick the monic gcd.*

Algorithm 4.31 (Euclidean Algorithm for $k[x]$)

```

EuclidGcd[a, b] ≡
  WHILE b ≠ 0 DO
    t := Rem[a, b]
    a := b
    b := t
  END
  RETURN a

```

Fact 4.32 *In $k[x]$ we have $\langle f, g \rangle = \langle \text{Gcd}[f, g] \rangle$*

Fact 4.33 $\text{Gcd}[f, g, h] = \text{Gcd}[f, \text{Gcd}[g, h]]$

Fact 4.34 *In $k[x]$ we have $\langle f, g, h \rangle = \langle \text{Gcd}[f, g, h] \rangle$*

Fact 4.35 $\exists h_1, h_2 \in k[x] : f_1 \cdot h_1 + f_2 \cdot h_2 = \text{Gcd}[f_1, f_2]$

4.2 Polynomial Rings in Several Variables

Definition 4.36 (Polynomial Ring in Several Variables) A ring of the form $R[x_1, \dots, x_n]$ where x_i are variables and R is a ring.

Definition 4.37 (Monomial) Product of the form $x_1^{a_1} \cdot \dots \cdot x_n^{a_n} = \vec{x}^{\vec{a}}$

Definition 4.38 (Set of Monomials of a Polynomial Ring) $\text{Monomials}[R[x_1, \dots, x_n]] :=$

Definition 4.39 (Coefficient of a Monomial m of a Polynomial p) $\text{Coeff}[p, m] :=$

Definition 4.40 (Multi Degree of a Monomial) $\text{DegMulti}[\vec{x}^{\vec{a}}] := \vec{a}$

Definition 4.41 (Total Degree of a Monomial) $\text{DegTotal}[\vec{x}^{\vec{a}}] := \sum_{1 \leq i \leq n} a_i$

Remark 4.42 For a polynomial ring in a single variable $\text{DegMulti} = \text{DegTotal} = \text{Deg}$.

Definition 4.43 (Multi Degree of a Term)

Definition 4.44 (Total Degree of a Term)

Definition 4.45 (Monomial Ordering, \prec) An ordering defined on the set of monomials with the following properties:

- \prec is a total (linear) ordering.
- $a \prec b \Rightarrow a + c \prec b + c$
- \prec is a well ordering, ie. every nonempty and possibly infinite set of monomials has a smallest element.

Theorem 4.46 A monomial ordering is a well ordering \Leftrightarrow every strictly decreasing sequence of monomials eventually terminates.

Theorem 4.47 A monomial ordering is a well ordering \Leftrightarrow for all monomials m we have $1 \preceq m$.

Definition 4.48 (Lexicographic Ordering, $\text{lex}(x_1, \dots, x_n)$)

$$\vec{x}^{\vec{a}} \prec \vec{x}^{\vec{b}} \Leftrightarrow \exists i \in [1 : n] : a_i < b_i \text{ and } \forall 1 \leq j \leq i - 1 : a_j = b_j$$

Fact 4.49 The lexicographic ordering is a monomial ordering.

Definition 4.50 (Graded Lexicographic Ordering, $\text{gplex}(x_1, \dots, x_n)$)

$$\vec{x}^{\vec{a}} \prec \vec{x}^{\vec{b}} \Leftrightarrow \text{totdeg}(\vec{x}^{\vec{a}}) < \text{totdeg}(\vec{x}^{\vec{b}}) \text{ or } \exists i \in [1 : n] : a_i < b_i \text{ and } \forall 1 \leq j \leq i - 1 : a_j = b_j$$

Fact 4.51 The graded lexicographic ordering is a monomial ordering.

Definition 4.52 (Graded Reverse Lexicographic Ordering, $\text{grevlex}(x_1, \dots, x_n)$)

$$\vec{x}^{\vec{a}} \prec \vec{x}^{\vec{b}} \Leftrightarrow \text{totdeg}(\vec{x}^{\vec{a}}) < \text{totdeg}(\vec{x}^{\vec{b}}) \text{ or } \exists i \in [1 : n] : a_i > b_i \text{ and } \forall i + 1 \leq j \leq n - 1 : a_j = b_j$$

Fact 4.53 The graded reverse lexicographic ordering is a monomial ordering.

Fact 4.54 *If there are only two variables graded reverse lexicographic ordering and graded lexicographic ordering are identical.*

Remark 4.55 *We assume a monomial order has been fixed when we compare monomials.*

Definition 4.56 (Multi Degree of a Polynomial)

Definition 4.57 (Total Degree of a Polynomial)

Definition 4.58 (Leading Coefficient of a Polynomial p) $\text{LeadC}[p] :=$

Definition 4.59 (Leading Monomial of a Polynomial p) $\text{LeadM}[p] :=$

Definition 4.60 (Leading Term of a Polynomial p) $\text{LeadT}[p] := \text{LeadC}[p] \cdot \text{LeadM}[p]$

Definition 4.61 (Field of Rational Functions, $k(x_1, \dots, x_n)$)

Definition 4.62 (Monomial Ideal) I monomial $:\Leftrightarrow p \in I \Leftrightarrow$ every term of f lies in I .

Definition 4.63 (Alternative Definition of Monomial Ideal)

$I \trianglelefteq k[x_1, \dots, x_n]$ monomial $:\Leftrightarrow \exists S \subseteq \text{Monomials}[k[x_1, \dots, x_n]] : I = \langle S \rangle$

Theorem 4.64 *Two monomial Ideals are the same \Leftrightarrow they contain the same monomials.*

Theorem 4.65 (Dickson's Lemma) *A monomial Ideal has a finite generating set.*

Algorithm 4.66 (Division Algorithm for $k[\vec{x}]$)

```

DivideMulti[ $f, g_1, \dots, g_k$ ]  $\equiv$ 
   $q_1 := 0; \dots; q_k := 0; r := 0$ 
  WHILE  $f \neq 0$  DO
    FOR  $i = 1$  TO  $k$  DO
      division_occured := false
      IF  $\text{LeadT}[g_i] \setminus f$  THEN
         $q_i = q_i + \text{LeadT}[f] / \text{LeadT}[g_i]$ 
         $f := f - \text{LeadT}[f] / \text{LeadT}[g_i] \cdot g_i$ 
        division_occured := true
      BREAK
    IF  $\neg$  division_occured THEN
       $r := r + \text{LeadT}[f]$ 
       $f := f - \text{LeadT}[f]$ 
  RETURN  $((q_1, \dots, q_k), r)$ 

```

Definition 4.67 $(\text{DivMulti}[f, (g_1, \dots, g_k)], \text{RemMulti}[f, (g_1, \dots, g_k)]) := \text{DivideMulti}[f, (g_1, \dots, g_k)]$

Corollary 4.68 *Let $g_i \in k[\vec{x}]$ be nonzero polynomials then every $f \in k[x]$ can be written as $f = \sum q_i \cdot g_i + r$ where none of the terms in r is divisible by the leading terms of the g_i and $\forall 1 \leq i \leq k : \text{DegMulti}[q_i g_i] \preceq \text{DegMulti}[f]$.*

Fact 4.69 $\preceq = \text{lex}(x, y) f = x^2 y + x y^2 + y^2, g_1 = y^2 - 1, g_2 = x y - 1 \Rightarrow$

$\text{DivideMulti}[f, g_1, g_2] = ((x + 1, x), 2x + 1)$

$\text{DivideMulti}[f, g_2, g_1] = ((x + y, 1), x + y + 1)$

Remark 4.70 *The remainder depends on the order of the g_i*

Definition 4.71 (Leading Terms of a Set of Polynomials S) $\text{LeadT}[S] := \bigcup_{s \in S} \{\text{LeadT}[s]\}$

Fact 4.72 $I = \langle p_1, \dots, p_n \rangle \subseteq k[\vec{x}] \Rightarrow \langle \text{LeadT}[p_1], \dots, \text{LeadT}[p_n] \rangle \subseteq \langle \text{LeadT}[I] \rangle$

Theorem 4.73 $I \subseteq k[\vec{x}] \Rightarrow \exists X \subseteq I$ finite : $\langle \bigcup_{x \in X} \{\text{LeadT}[x]\} \rangle = \langle \text{LeadT}[I] \rangle$

Corollary 4.74 (Hilbert's Basis Theorem) *For any X determined as above we have $\langle X \rangle = I$, ie. every ideal has a finite basis.*

Fact 4.75 $\forall 1 \leq i : I_i \subseteq k[\vec{x}]$ and $I_i \subseteq I_{i+1} \Rightarrow \bigcup_{1 \leq i} I_i \subseteq k[\vec{x}]$

Corollary 4.76 (Ascending Chain Condition (ACC)) *Every ascending chain of ideal eventually stabilizes.*

Definition 4.77 (Groebner Basis of an Ideal I) $S \subseteq I$ Groebner basis : $\Leftrightarrow \langle S \rangle = I$ and $\langle \text{LeadT}[S] \rangle = \langle \text{LeadT}[I] \rangle$

Definition 4.78 (S-Polynomial of two polynomials f, g) $S[f, g] := \frac{\text{lcm}(\text{LeadM}[f, g])}{\text{LeadT}[f]} f - \frac{\text{lcm}(\text{LeadM}[f, g])}{\text{LeadT}[g]} g$

Definition 4.79 (Groebner Basis Criterion) $G = \{g_i \mid i \in [1 : n]\}$ Groebner basis $\Leftrightarrow \forall i, j \in [1 : n] : \text{RemMulti}[S[g_i, g_j], G] = 0$

Remark 4.80 $G = \{g_i \mid i \in [1 : n]\}$ Groebner basis $\Rightarrow x \in I \Leftrightarrow \text{RemMulti}[x, G] = 0$

Remark 4.81 $I = \langle p \rangle \Rightarrow \{p\}$ Groebner basis

Algorithm 4.82 (Groebner Basis) $\text{GroebnerBasis}[f_1, \dots, f_n] \equiv$

```

 $G := \{f_1, \dots, f_n\}$ 
UNTIL  $H = G$ 
   $H := G$ 
  FORALL  $i, j \in G$ 
    IF  $\text{RemMulti}[S[i, j], H] \neq 0$ 
       $G := G \cup \{S[i, j]\}$ 
RETURN  $G$ 

```

Fact 4.83 $G = \{f, g_1, \dots, g_n\}$ Groebner basis and $\text{LeadT}[f] \in \langle \text{LeadT}[\{g_1, \dots, g_n\}] \rangle \Rightarrow \{g_1, \dots, g_n\}$ Groebner basis

Definition 4.84 (Minimal Groebner Basis) $G = \{g_1, \dots, g_n\}$ minimal Groebner basis : $\Leftrightarrow \forall i \in [1 : n] : \text{LeadC}[g_i] = 1$ and $G - g_i$ is not a Groebner Basis.

Definition 4.85 (Reduced Groebner Basis) $G = \{g_1, \dots, g_n\}$ reduced Groebner basis : $\Leftrightarrow \forall i \in [1 : n] : \text{LeadC}[g_i] = 1$ and no monomial of g_i lies in $G - g_i$

Remark 4.86 *The reduced Groebner Basis is unique.*

Fact 4.87 (Ideal Membership Testing) $x \in \langle f_1, \dots, f_n \rangle \Leftrightarrow \text{RemMulti}[x, \text{GroebnerBasis}[f_1, \dots, f_n]] = 0$ identical.

Fact 4.88 (Ideal Equality Testing) *Two ideals are identical \Leftrightarrow their reduced Groebner basis are identical.*

Fact 4.89 $tf + (1 - t)f = f$

Theorem 4.90 $I, J \trianglelefteq k[\vec{x}] \Rightarrow I \cap J = (\langle t \rangle I + \langle 1 - t \rangle J) \cap k[\vec{x}]$

Fact 4.91 $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle \Rightarrow I$ maximal

Fact 4.92 $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle \trianglelefteq k[x_1, \dots, x_n] \Rightarrow I$ maximal

Fact 4.93 $I \trianglelefteq k[x_1, \dots, x_n]$ and I maximal $\Rightarrow I$ prime

Theorem 4.94 $I = \trianglelefteq k[x_1, \dots, x_n]$ and I maximal and k algebraically closed $\Rightarrow I = \langle x_1 - a_1, \dots, x_n - a_n \rangle$

Example 4.95 $\langle x^2 + 1 \rangle \trianglelefteq \mathbb{R}[x]$ maximal

Remark 4.96 $f = 0 \Rightarrow \forall \vec{x} \in k^n : f(\vec{x}) = 0$

Remark 4.97 $f = x^2 - x \in \mathbb{Z}_2[x] \Rightarrow \forall x \in \mathbb{Z}_2 : f(x) = 0$

Remark 4.98 $\forall \vec{x} \in k^n : f(\vec{x}) = 0 \not\Rightarrow f = 0$

Theorem 4.99 k infinite field and $\forall \vec{x} \in k^n : f(\vec{x}) = 0 \Rightarrow f = 0$

Corollary 4.100 k infinite field and $\forall \vec{x} \in k^n : f(\vec{x}) = g(\vec{x}) \Rightarrow f = g$

Definition 4.101 (Linear Polynomial) *A polynomial where the total degree of each term is 1.*

4.3 Factorization and Irreducibility

Definition 4.102 (Irreducible Polynomial) *A nonconstant polynomial that can not be factored into two nonconstant polynomials.*

Fact 4.103 $f(x) \in \mathbb{Z}[x]$ irreducible $\Leftrightarrow f(x+1)$ irreducible

Fact 4.104 $f(x) \in \mathbb{Z}[x]$ reducible $\wedge n \nmid \text{LeadC}[f(x)] \Rightarrow f_{\text{mod } n}(x) \in \mathbb{Z}_n[x]$ reducible

Definition 4.105 (Reducible Polynomial)

Fact 4.106 (Unique Factorization in $k[\vec{x}]$) *Every nonconstant polynomial can be written as a product of irreducible polynomials. The factors are unique up to multiplication of units.*

Fact 4.107 $a, b, c \in k[x_1, \dots, x_n]$ and c irreducible and $c \mid ab \Rightarrow c \mid a$ or $c \mid b$

Theorem 4.108 $a, b \in k[x_1, \dots, x_n] \Rightarrow a, b$ have a common factor in $k[x_1, \dots, x_n]$ of positive degree in $x_1 \Leftrightarrow a, b$ have a common factor in $k(x_2, \dots, x_n)[x_1]$ of positive degree in x_1

Corollary 4.109 $a, b \in \mathbb{Z}[x] \Rightarrow a, b$ have a common factor in $\mathbb{Z}[x]$ of positive degree in $x \Leftrightarrow a, b$ have a common factor in $\mathbb{Q}[x]$ of positive degree in x_1

Definition 4.110 (Root (Zero) of a Polynomial p) $r \in k$ root $:\Leftrightarrow p(r) = 0$

Fact 4.111 $f \in k[x]$ and $a \in k$ and $f(a) = 0 \Rightarrow (x - a) \mid f$

Definition 4.112 (Simple Root of a Polynomial p) $r \in k$ simple root $:\Leftrightarrow r$ root and $(x - r)^2 \nmid p$

Definition 4.113 (Multiple Root of a Polynomial p)

Fact 4.114 $f \in k[x]$ and $\text{Deg}[f] = n \Rightarrow f$ has at most n distinct roots.

Definition 4.115 (Primitive Polynomial) $p = a_n \cdot x^n + \dots + a_1 \cdot x^1 + a_0 \cdot x^0 \in \mathbb{Z}[x]$ primitive $:\Leftrightarrow \text{Gcd}[a_n, \dots, a_1, a_0] = 1$

Theorem 4.116 p_1, p_2 primitive $\Rightarrow p_1 \cdot p_2$ primitive

Theorem 4.117 (Eisenstein's Irreducibility Criterion)

R factorial and $p = \sum_{0 \leq i \leq n} a_i x^i \in R[x]$ and $\exists p \in R$ prime : $p \nmid a_n$ and $p \mid a_0, \dots, a_{n-1}$ and $p^2 \nmid a_0 \Rightarrow p \in \frac{R}{R^*}[x]$ irreducible.

Corollary 4.118 $p = \sum_{0 \leq i \leq n} a_i x^i \in \mathbb{Z}[x]$ and $\exists p$ prime : $p \nmid a_n$ and $p \mid a_0, \dots, a_{n-1}$ and $p^2 \nmid a_0 \Rightarrow p \in \mathbb{Q}[x]$ irreducible

Fact 4.119 $p(x) \in \mathbb{Z}[x]$ irreducible $\Leftrightarrow p(x+c)$ irreducible

Fact 4.120 $p(x) \in \mathbb{Z}_p[x]$ irreducible $\Rightarrow p(x) \in \mathbb{Z}$ irreducible

Theorem 4.121 (Integral Root Test)

R factorial and $p = \sum_{0 \leq i \leq n} a_i x^i \in R[x]$ and $\frac{a}{b} \in \frac{R}{R^*}$ and $\text{Gcd}[a, b] = 1$ and $p(\frac{a}{b}) = 0 \Rightarrow a \mid a_0$ and $b \mid a_n$

Corollary 4.122 $p = \sum_{0 \leq i \leq n} a_i x^i \in \mathbb{Z}[x]$ and $\frac{a}{b} \in \mathbb{Q}$ and $\text{Gcd}[a, b] = 1$ and $p(\frac{a}{b}) = 0 \Rightarrow a \mid a_0$ and $b \mid a_n$

Algorithm 4.123 (Berlekamp's Factoring Algorithm for \mathbb{Z}_p)

4.4 Symmetric Polynomials

Remark 4.124 $f(t) = (t - a_1) \cdot \dots \cdot (t - a_n) = c_0 + c_1 t + \dots + c_n t^n$

$$\begin{aligned}c_0 &= (-1)a_1 \cdot \dots \cdot a_n \\&\dots \\c_{n-2} &= a_1 a_2 + a_1 a_3 + \dots + a_{n-1} a_n \\c_{n-1} &= -(a_1 + a_2 + \dots + a_n) \\c_n &= k\end{aligned}$$

Definition 4.125 (Elementar Symmetric Polynomials)

$$\text{Sym}_k[x_1, \dots, x_n] := \sum_{S \in \text{PowerSet}_{n-k}[\{x_1, \dots, x_n\}]} \prod_{v \in S} v$$

Fact 4.126 *A symmetric polynomial can be expressed as a polynomial of smaller or equal degree in the elementary symmetric polynomials.*

4.5 Concrete Polynomial Rings

Theorem 4.127 (Fundamental Theorem of Algebra) *Every nonconstant polynomial $f \in \mathbb{C}[x]$ has a root in \mathbb{C} .*

Example 4.128 (Twisted Cubic) $\langle y - x^2, z - x^3 \rangle \subseteq \mathbb{R}^3$

Example 4.129 (Parameterization of Twisted Cubic) $\{(t, t^2, t^3) \mid t \in \mathbb{R}\}$

Example 4.130 $G = \{y - x^2, z - x^3\}$ is a Groebner basis for $\text{lex}(x \prec z \prec y)$.

Example 4.131 $G = \{y - x^2, z - x^3\}$ is not a Groebner basis for $\text{lex}(z \prec y \prec x)$.

4.6 Affine Varieties

Definition 4.132 (Variety of a Set of Polynomials S) $\text{Variety}[S] = \{v \in k^n \mid \forall f \in S : f(v) = 0\}$

Fact 4.133 (Inclusion Reversion) $S_1 \subseteq S_2 \Rightarrow \text{Variety}[S_2] \subseteq \text{Variety}[S_1]$

Definition 4.134 (Affine Variety) $V \subseteq k^n$ affine variety $:\Leftrightarrow \exists S \subseteq k[x_1, \dots, x_n] : \text{Variety}[S] = V$

Definition 4.135 (Linear Variety)

Fact 4.136 $\text{Variety}[\emptyset] = k[x_1, \dots, x_n]$

Fact 4.137 $\text{Variety}[k^n] = \{0\}$

Fact 4.138 $\text{Variety}[S] \cap \text{Variety}[T] = \text{Variety}[S \cup T]$

Fact 4.139 $\text{Variety}[S] \cup \text{Variety}[T] = \text{Variety}[\{s \cdot t \mid s \in S \text{ and } t \in T\}]$

Definition 4.140 (Affine Variety of an Ideal I) $\text{Variety}[I] = \{v \mid v \in k^n \text{ and } \forall f \in I : f(v) = 0\}$

Fact 4.141 $S = \{p_1, \dots, p_n\}$ and $I = \langle S \rangle \Rightarrow \text{Variety}[I] = \text{Variety}[S]$

Fact 4.142 $I, J \trianglelefteq k[\vec{x}] \Rightarrow \text{Variety}[I + J] = \text{Variety}[I] \cap \text{Variety}[J]$

Fact 4.143 $I, J \trianglelefteq k[\vec{x}] \Rightarrow \text{Variety}[I \cdot J] = \text{Variety}[I] \cup \text{Variety}[J]$

Remark 4.144 $I, J \trianglelefteq R \Rightarrow I \cdot J \subseteq I \cap J$

Fact 4.145 $I, J \trianglelefteq k[\vec{x}] \Rightarrow \text{Variety}[I \cap J] = \text{Variety}[I] \cup \text{Variety}[J]$

Fact 4.146 $\text{Variety}[\langle 0 \rangle] = k^n$

Fact 4.147 $\text{Variety}[k[\vec{x}]] =$

Remark 4.148 Varieties are determined by ideals.

Definition 4.149 (Ideal of a Set of Points S) $\text{Ideal}[V] = \{f \mid f \in k[x_1, \dots, x_n] \text{ and } \forall v \in S : f(v) = 0\}$

Fact 4.150 (Inclusion Reversion) $S_1 \subseteq S_2 \Rightarrow \text{Ideal}[S_2] \subseteq \text{Ideal}[S_1]$

Definition 4.151 (Ideal of an Affine Variety V) $\text{Ideal}[V] = \{f \mid f \in k[x_1, \dots, x_n] \text{ and } \forall v \in V : f(v) = 0\}$

Fact 4.152 $I = \langle S \rangle \Rightarrow \text{Variety}[I] = \text{Variety}[S]$

Fact 4.153 $I = \langle S \rangle \Rightarrow \text{Variety}[I] = \text{Variety}[S]$

Remark 4.154 $\langle x \rangle \neq \langle x^2 \rangle$ but $\text{Variety}[\langle x \rangle] = \text{Variety}[\langle x^2 \rangle]$

Remark 4.155 V regarded as a mapping from ideals to varieties is not one-to-one.

Fact 4.156 $J \trianglelefteq k[x_1, \dots, x_n] \Rightarrow J \subseteq \text{Ideal}[\text{Variety}[J]]$

Fact 4.157 $V, W \subseteq k^n$ varieties $\Rightarrow V \subseteq W \Leftrightarrow \text{Ideal}[W] \subseteq \text{Ideal}[V]$

Corollary 4.158 $V, W \subseteq k^n$ varieties $\Rightarrow V = W \Leftrightarrow \text{Ideal}[W] = \text{Ideal}[V]$

Corollary 4.159 I regarded as a mapping from varieties to ideals is one-to-one.

Definition 4.160 (Irreducible Variety) V irreducible $:\Leftrightarrow (V_1 \cup V_2 = V \Rightarrow V_1 = V \text{ or } V_2 = V)$

Theorem 4.161 V irreducible $\Leftrightarrow \text{Ideal}[V]$ prime

Definition 4.162 (Rational Parametric Representation of a Variety)

Definition 4.163 (Polynomial Parametric Representation of a Variety)

Definition 4.164 (Implicit Representation of a Variety)

Theorem 4.165 (Weak Nullstellensatz) $I \subseteq k[\vec{x}]$ and k algebraically closed and $\text{Variety}[I] = \emptyset \Rightarrow I = k[\vec{x}]$

Remark 4.166 The Weak Nullstellensatz can be regarded as the Fundamental Theorem of Algebras for polynomials in several variables: Every system of polynomials that generates a proper ideal has a common zero in \mathbb{C}^n .

Remark 4.167 (Consistency Testing) $f_1, \dots, f_k \in \mathbb{C}[\vec{x}] \Rightarrow \text{Variety}[\{f_1, \dots, f_k\}] = \emptyset \Leftrightarrow \langle f_1, \dots, f_k \rangle = \mathbb{C}[\vec{x}] \Leftrightarrow 1 \in \langle f_1, \dots, f_k \rangle \Leftrightarrow \{1\}$ is a reduced Groebner basis.

Fact 4.168 An algebraically closed field is infinite.

Fact 4.169 $f_1, \dots, f_k \in k[\vec{x}]$ and k algebraically closed and $f := f_1 \cdots f_k \Rightarrow \text{Variety}[\{f_1, \dots, f_k, 1 - yf\}] = \emptyset \Rightarrow \exists p_i, q \in k[\vec{x}, y] : 1 = q(1 - yf) + \sum p_i f_i$

Theorem 4.170 (Hilbert's Nullstellensatz) $f_1, \dots, f_k \in k[\vec{x}]$ and k algebraically closed and $f \in \text{Ideal}[\text{Variety}[\{f_1, \dots, f_k\}]] \Rightarrow \exists 1 \leq n : f^n \in \langle f_1, \dots, f_k \rangle$

Fact 4.171 V affine variety and $f^m \in \text{Ideal}[V] \Rightarrow f \in \text{Ideal}[V]$

Fact 4.172 V affine variety $\Rightarrow \text{Ideal}[V]$ radical

Definition 4.173 (Radix of an Ideal I) $\sqrt{I} := \{f : \exists 1 \leq n : f^n \in I\}$

Fact 4.174 $\sqrt{I} \subseteq k[\vec{x}]$

Fact 4.175 $I \subseteq \sqrt{I}$

Fact 4.176 \sqrt{I} radical

Fact 4.177 $I, J \subseteq R \Rightarrow \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$

Theorem 4.178 (Strong Nullstellensatz) $I \subseteq k[\vec{x}]$ and k algebraically closed $\Rightarrow \text{Ideal}[\text{Variety}[I]] = \sqrt{I}$

Fact 4.179 V variety $\Rightarrow \text{Variety}[\text{Ideal}[V]] = V$

Remark 4.180 (Radical Membership Testing) $I = \langle f_1, \dots, f_k \rangle \subseteq k[\vec{x}] \Rightarrow f \in \sqrt{I} \Leftrightarrow \langle f_1, \dots, f_k, 1 - yf \rangle = k[\vec{x}, y] \Leftrightarrow 1 \in \langle f_1, \dots, f_k, 1 - yf \rangle$

Fact 4.181 $I = \langle f \rangle$ principal and $f = p_1^{a_1} \cdots p_k^{a_k}$ and p_i irreducible $\Rightarrow \sqrt{I} = \langle p_1 \cdots p_k \rangle$

Definition 4.182 (Reduction of a Polynomial f) $I = \langle f \rangle$ principal and $\sqrt{I} = \langle g \rangle \Rightarrow g$ square free.

Theorem 4.183 $f \in k[\vec{x}]$ and $\mathbb{Q} \subseteq k \Rightarrow f_{red} = \frac{f}{\text{Gcd}(f, D_{x_1}f, \dots, D_{x_n}f)}$

4.7 Elimination Theory

Remark 4.184 *In the sequel we are working in a polynomial field $k[x_1, \dots, x_n]$.*

Definition 4.185 (*k*-th Elimination Ideal of an Ideal *I*) $I_k := I \cap k[x_{k+1}, \dots, x_n]$

Remark 4.186 $I_0 = I$

Remark 4.187 I_k is an ideal.

Definition 4.188 (G_k) $G_k := G \cap k[x_{k+1}, \dots, x_n]$

Theorem 4.189 (Elimination Theorem) G lex-order Groebner basis of ideal $I \Rightarrow G_k$ is a Groebner basis for I_k

Fact 4.190 $\pi_1(V(I))$ is not necessarily an affine variety.

Fact 4.191 $\pi_1(V(I)) \subseteq V(I_1)$

Theorem 4.192 (Extension Theorem)

k algebraically closed and $I = \langle f_1, \dots, f_k \rangle$ and $(a_2, \dots, a_n) \in V(I_1) \Rightarrow$

$\exists a_1 \in k : (a_1, a_2, \dots, a_n) \in V(I) \Leftrightarrow (a_2, \dots, a_n) \notin V(g_1, \dots, g_k)$

where $g_i \in k[x_2, \dots, x_n]$ is the leading terms of f_i regarded as a polynomial in x_1 .

Corollary 4.193 $V(I_1) = \pi_1(V(I)) \cup (V(g_1, \dots, g_k) \cap V(I_1))$

Remark 4.194 *The extension theorem is false for fields such as \mathbb{R} that are not algebraically closed.*

Remark 4.195 *An extension step from I_1 to I can fail only when the g_i vanish simultaneously.*

Fact 4.196 $V(I_k)$ is the smallest affine variety containing $\pi_k(V(I))$

Fact 4.197 $V(I) \neq \emptyset \Rightarrow \exists$ affine variety $W \subset V(I_k) : V(I_k) - W \subseteq \pi_k(V(I))$

Remark 4.198 *If one of the g_i is a constant the extension step is always successful, ie. $V(I_1) = \pi_1(V(I))$*

Theorem 4.199 $f, g \in k[x] \Rightarrow f, g$ have a common factor $\Leftrightarrow \exists a, b \in k[x] : a \neq 0$ and $b \neq 0$ and $\text{Deg}[a] < \text{Deg}[g]$ and $\text{Deg}[b] < \text{Deg}[f]$ and $af + bg = 0$

Definition 4.200 (Sylvester Matrix of Two Polynomial f, g) $\text{Sylvester}[f, g, x] :=$

Fact 4.201 $f, g \in k[x] \Rightarrow f, g$ have a common factor $\Leftrightarrow \text{Sylvester}[f, g]$ singular.

Definition 4.202 (Resultant of Two Polynomials f, g) $\text{Resultant}[f, g, x] := \text{Det}[\text{Sylvester}[f, g]]$

Theorem 4.203 $f, g \in k[x] \Rightarrow \exists a, b \in k[x] : af + bg = \text{Resultant}[f, g, x]$

Theorem 4.204 $f, g \in k[x_1, \dots, x_n] \Rightarrow \text{Resultant}[f, g, x_1] \in \langle f, g \rangle \cap k[x_2, \dots, x_n]$

Theorem 4.205 $f, g \in k[x_1, \dots, x_n] \Rightarrow \text{Resultant}[f, g, x_1] = 0 \Leftrightarrow f, g$ have a common fact of positive degree in x_1 .

Corollary 4.206 $f, g \in k\mathbb{C}[x_1, \dots, x_n] \Rightarrow \text{Resultant}[f, g, x_1] = 0 \Leftrightarrow f, g$ have a common root in \mathbb{C} .

4.8 Concrete Varieties

Example 4.207 (Twisted Cubic) $\langle y - x^2, z - x^3 \rangle \subseteq \mathbb{R}^3$

Example 4.208 (Parameterization of Twisted Cubic) $\{(t, t^2, t^3) \mid t \in \mathbb{R}\}$

Example 4.209 $k = \mathbb{R} \Rightarrow \text{Variety}[\{x^2 + 1\}] = \emptyset$

Example 4.210 $\{(x, x) \in \mathbb{R}^2 \mid x \neq 1\}$ is not an affine variety.

5 Fields

5.1 Basics

Example 5.1 \mathbb{Z}_n field $\Leftrightarrow n$ prime

Definition 5.2 (Subfield, $k \subseteq K$)

Fact 5.3 $k_1, k_2 \subseteq K \Rightarrow k_1 \cap k_2 \subseteq K$

Remark 5.4 A subring of a field need not be a subfield

Definition 5.5 (Prime Subfield of a Field K) $\text{PrimeSubField}[K] := \bigcap_{k \subseteq K} k$

Fact 5.6 $\text{PrimeSubField}[K] = \mathbb{Q} \vee \text{PrimeSubField}[K] = \mathbb{Z}_p, p$ prime

Definition 5.7 (Superfield, Extension Field, $K \supseteq k$)

Remark 5.8 An extension field may be viewed as a vector space over the extended field.

Definition 5.9 (Dimension of a Subfield k of K) $\text{Dim}[K, k] :=$

Theorem 5.10 $F_1 \subseteq F_2 \subseteq F_3 \Rightarrow \text{Dim}[F_3, F_1] = \text{Dim}[F_3, F_2] \cdot \text{Dim}[F_2, F_1]$

Fact 5.11 A ring-homomorphism from a field into a ring is always injective.

Remark 5.12 (Algebraic Elements) $a \in_F E \Leftrightarrow F \subseteq E$ and $a \in E$ and $\exists p(x) \in F[X] : p(x) \neq 0$ and $p(a) = 0$;

Fact 5.13

$$a \in_E F \Leftrightarrow F[X] \xrightarrow{\text{eval}_a} E \text{ has nonzero kernel (is not injective)}$$

Definition 5.14 (Irreducible Polynomial of $e \in_F E$, $\text{Irr}(e, F, X)$)

Definition 5.15 (Adjoining a Subset S from the Extension Field K to the Extended Field k)
 $k(S) := \langle k \cup S \rangle$

Definition 5.16 (Transcendental)

Definition 5.17 (Algebraically Independent)

5.2 Field Extensions

Definition 5.18 (Finite Extension) $k \subseteq K$ *finite extension* $:\Leftrightarrow \text{Dim}[K, k]$ *finite*

Definition 5.19 (Simple Extension) $k \subseteq K$ *simple extension* $:\Leftrightarrow \exists x \in K : K = k(x)$

Definition 5.20 (Algebraic Extension) $E \supseteq F$ *algebraic extension* $:\Leftrightarrow \forall e \in E : e \in_F E$

Definition 5.21 (Transcendental Extension)

Definition 5.22 (Finitely Generated Extension)

Definition 5.23 *A finite extension is algebraic*

Theorem 5.24

$$e \in_F E \Rightarrow F(a) = F[a] \text{ and } [F(a) : F] = \deg \text{Irr}(a, F, X)$$

Corollary 5.25

$$a_i \in_F E \Rightarrow F(a_1, \dots, a_n) = F[a_1, \dots, a_n]$$

Definition 5.26 (Compositum of $F_1, F_2 \subseteq E, F_1 \cdot F_2$)

$$F_1 \cdot F_2 \text{ smallest subfield of } E \text{ containing } F_1, F_2$$

Fact 5.27 *A finite extension is finitely generated.*

Definition 5.28 (Distinguished Extension Class)

A class C of extension is called distinguished iff it satisfies the following conditions:

- $F_1 \subseteq F_2 \subseteq F_3 : (F_1 \subseteq F_3) \in C \Leftrightarrow (F_1 \subseteq F_2) \in C \text{ and } (F_2 \subseteq F_3) \in C$
- $(k \subseteq F_1) \in C \text{ and } k \subseteq F_2 \text{ and } F_1, F_2 \subseteq E \Rightarrow (k \subseteq F_1 \cdot F_2) \in C$

Remark 5.29

$$(k \subseteq F_1) \in C \text{ and } (k \subseteq F_2) \in C \text{ and } F_1, F_2 \subseteq E \Rightarrow (k \subseteq F_1 \cdot F_2) \in C$$

Theorem 5.30 *The class of finite extension is distinguished*

Theorem 5.31 *The class of algebraic extension is distinguished*

Theorem 5.32 *The class of finitely generated extension is distinguished*

Fact 5.33 $x^2 + 1$ *has no roots in \mathbb{R} .*

Fact 5.34 \mathbb{R} *is not algebraically closed*

Definition 5.35 (Minimal Polynomial)

Theorem 5.36 (Irreducibility of the Minimal Polynomial)

Theorem 5.37 *All simple transcendental extensions are isomorphic.*

Theorem 5.38 $k \subseteq K$ *simple algebraic* $\Rightarrow \text{Dim}[K, k] = \text{Deg}[a]$

Theorem 5.39 $k \subseteq K$ *simple transcendental* $\Rightarrow \text{Dim}[K, k] = \infty$

5.3 Algebraic Closure

Theorem 5.40

F field and $f \in F[X] \Rightarrow \exists E \supseteq F : f$ has a root in E

Corollary 5.41

F field and $f_i \in F[X] \Rightarrow \exists E \supseteq F : \forall f_i : f_i$ has a root in E

Definition 5.42 (Algebraically Closed Field)

Theorem 5.43 (Every field F has an algebraically closed extension: \bar{F})