Notes: Abstract Algebra

Martin Sig Nørbjerg

Project, Group , Mathematics

Contents

1 Groups

The following chapter will be notes on chapter 1 of Serge Langs algebra book.

1.1 Monoids

A *monoid* is a set G together with a *binary operation* $\cdot : G \times G \to G$ such that there exists $e \in G$ (called the *neutral element*) such that $e \cdot g = g \cdot e = g$ for all $g \in G$ and the operation is *associative* meaning $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in G$.

The binary operation is said to be *commutative* if $x \cdot y = y \cdot x$ for all $x, y \in G$. If G is a monoid with a commutative binary operation $\cdot$, then G is said to be *abelian*.

Example 1.1. $\mathbb{N}$ is an example of an additive monoid (the neutral element (e) is 0), this is also an example of an abelian monoid. $\square$

Proposition 1.2. *Let G be a abelian monoid, and $x_1, x_2, \ldots, x_n$ be elements of G, and let π be a permutation of $\{1, 2, \ldots, n\}$, then*

$$\prod_{i=1}^{n} x_{\pi(i)} = \prod_{i=1}^{n} x_i$$

We will omit the proof, however it can be proved by induction. Let G be a monoid under the binary operation $\cdot$, then the subset $H \subseteq G$ is called a *submonoid* if H is closed under $\cdot$.

1.2 Groups

A *group* G is a monoid G, such that for all $x \in G$ there exists an *inverse element* [1] $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = e$. Furthermore we write $x^{-n} := (x^{-1})^n$. The group G is called *trivial* if $G = \{e\}$, in this case we denote G with 1.

Example 1.3. Let $Perm(S)$ be the set of permutations on S, that is the bijective mappings from $S \to S$, then $Perm(S)$ forms a group under the operation $\circ$, defined as $\sigma \circ \tau = \sigma(\tau)$ for all $\sigma, \tau \in Perm(S)$ $\square$

A group G is said to be *cyclic* if there exists a $g \in G$ such that for all $h \in G$ there exists $n \in \mathbb{N}$ such that $h = g^n$. In this case g is said to be a *cyclic generator* of G.

[1] it can be shown that these inverse elements are unique

Example 1.4. The simplest example of a cyclic group, is $\mathbb{Z}$ together with $+$, it is generated by 1. $\square$

Suppose $G_1, G_2, \ldots, G_n$ are groups with operations $\cdot_1, \cdot_2, \ldots, \cdot_n$, then $G = G_1 \times G_2 \times \cdots \times G_n$ forms a group, together with the operation $\cdot : G \times G \to G$, defined by

$$(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_n) = (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2, \ldots, x_n \cdot_n y_n)$$

this group is called the *direct product group* of $G_1, G_2, \ldots, G_n$.

Example 1.5. Consider the group $\mathbb{R}$ together with $+$, then $\mathbb{R}^n$ is a direct group, with respect to addtion (this time of vectors). $\square$

Let G be a group, a *subgroup* H is a subset of G, that is it self a group.

Proposition 1.6. *Let $H_1, H_2, \ldots, H_n$ be subgroups of G, then $\bigcap_{i=1}^n H_i$ is a subgroup of G.*

Proof. Suppose H_1 and H_2 are both subgroups of G, then $H_1 \cap H_2$ is a subgroup: Since $e \in H_i$, and if $g \in H_i$, then we must have $g^{-1} \in H_i$, and since H_1 and H_2 are both closed under the binary operation, then $H_1 \cap H_2$ will also be (as $g \in H_i \implies g \cdot h \in H_i$ for all $h \in H_i$). The rest now follows by induction. $\blacksquare$

Suppose G is a group, then we say that $S \subseteq G$ *generates* G if $g \in G$ can be writen as $\prod_{i=1}^n x_i$, where every x_i or x_i^{-1} is in S. The group G generated by S is the smallest group (with respect to $\subseteq$) that contains S. If $S = \{x_1, x_2, \ldots, x_k\}$ is a generator of G, then we write

$$G = \langle x_1, x_2, \ldots, x_k \rangle = \left\{ \prod_{r=1}^n x_{i_r}^{k_{i_r}} \middle| k_{i_r} \in \mathbb{Z}, (i_r)_{r=1}^n \subseteq (1, 2, \ldots, k) \right\}.$$

Example 1.7. We consider the group generated by the elements i, j such that if $k = ij$ and $m = i^2$, then

$$i^4 = j^4 = k^4 = e, \quad i^2 = j^2 = k^2 = m, \quad ij = mji$$

This group will be denoted $\mathbb{H} := \langle i, j \rangle$ and called the group of *quaternions.* $\square$

Let G, G' be groups / monoids, then $f : G \to G'$ is called a *(group / monoid) homeomorphism* between G and G' if $f(xy) = f(x)f(y)$, it can be shown that $f(e) = e'$. A bijective homeomorphism is called a *(group / monoid) isomorphism.* Furthermore a homeomorphism from G to G is called a *endomorphism* and a isomorphism from G to G is called an *automorphism.*

Finally if there exists a isomorphism between G and G', then G and G' is said to be *isomorphic*[2] and we write $G \cong G'$. If $f : G \to G'$ is a homeomorphism, such that $\tilde{f} : G \to Im(f)$, is a isomophism, then f is called an *embedding.* If f is an injective homeomorphism, we sometimes write $f : G \hookrightarrow G'$.

Proposition 1.8. *Let $f : G \to G'$ be a homeomorphism, such that $ker(f) = \{e\}$, then f is injective.*

[2] In this case G and G' behave essencially the same (up to a relabeling of the elements).

Proof. Let $y, x \in G$ such that $f(x) = f(y)$, then $f(xy^{-1}) = f(x)f(y^{-1}) = e$, hence $xy^{-1} \in ker(f)$, so $xy^{-1} = e$ which implies $y^{-1} = x^{-1} \iff y = x$. ■

Remark 1.9. A injective homeoporhism is an embedding.

Proposition 1.10. *Let G be a group and H, K subgroups of G, such that $H \cap K = e$, $HK = G$ and $xy = yx$ for all $x \in H, y \in K$. Then $(H \times K) \ni (x, y) \mapsto xy \in G$ is an isomorphism.*

Let G be a group and H a subgroup, then $aH, a \in G$ is called a *left coset* H in G, the *right cosets* are defined similarly. The number of left cosets of H in G is denoted $(G : H)$ and is called the *index* of H in G. The index of the trivial subgroup is called the *order* of G.

Proposition 1.11. *Let G be a group and H, K be subgroups, st $K \subseteq H$, then let $\{x_iH\}$ be the set of left cosets of H in G and $\{y_jK\}$ be the set of left cosets of K in H, then $\{x_iy_jK\}$ is the set of cosets of K in G*

Proof. Note that $H = \bigcup_i x_iK$ and $G = \bigcup_j y_jH$ (both disjoint unions, as $x \in yH' \implies xH' = yH'$ for all subgroups H') Hence $G = \bigcup_j y_j \bigcup_i x_iK = \bigcup_{j,i} y_jx_iK$, also a disjoint union since if exists two distinct pair of indicies (i, j) and (i', j') such that $y_jx_iK = y_{j'}x_{i'}K$, then $y_jH = y_{j'}H$ (by multiplying by H on the right), thus $y_j = y_{j'}$ and it follows that $x_iK = x_{i'}K$, and thus $x_i = x_{i'}$. ■

The proposition below is a natural consequence.

Proposition 1.12. *Let G be a subgroup and H, K be subgroups such that $K \subseteq H$, then $(G : K) = (G : H)(H : K)$. In particular we have $(G : H)(H : 1) = (G : 1)$ in the sense that if two of these indicies, then the third is also finite. If order of G is finite then the order of H divides it.*

Corollary 1.13. *Every group G of prime order is cyclic.*

Proof. Suppose $(G : 1) = p$, let H be a subgroup generated by $a \in G \setminus \{e\}$, by Proposition 1.12, $(G : H)$ divides p, however H has atleast two elements, so we must have $|H| = p$. Thus G is cyclic. ■

2 Miscilanius

This chapter includes some miscilanius theories.

2.1 Category Theory

A *category* $\mathcal{C}$ consists of a collection of *objects* $Obj(\mathcal{C})$, for each $A, B \in Obj(\mathcal{C})$, there exists a set $Mor(A, B)$ of *morphisms* (maps between A and B), such that for all $A, B, C \in Obj(\mathcal{C})$ there exists a law of composition (ie. map):

$$\circ : Mor(B, C) \times Mor(A, B) \to Mor(A, C)$$

that satisifies:

(i) $Mor(A, B) \cap Mor(A', B') = \emptyset$ unless $A = A' \wedge B = B'$, in that case they are equal.

(ii) for all $A \in Obj(\mathcal{C})$ there exists a morphism $id_A \in Mor(A, A)$, which acts as a left and right identity for the elements in $Mor(A, B)$ and $Mor(B, A)$, for all $B \in Obj(\mathcal{C})$.

(iii) Law of composition is associative meaning if $f \in Mor(A, B), g \in Mor(B, C), h \in Mor(C, D)$, then

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Every morphism in $\mathcal{C}$, is called an *arrow* and the collection of all arrows is denoted $Ar(\mathcal{C})$. The morphism $f \in Mor(A, B)$ is called an *isomorphism* if there exists a $g \in Mor(B, A)$ such that $f \circ g = id_A$ and $g \circ f = id_B$ if $A = B$, then f is called an *automorphism*, automorphisms of A will be denoted $Aut(A)$, these together with the law of composition forms a group. .

Example 2.1. The groups form a category, whose morphisms are the group-homomorphisms. $\square$

3 Division of multivariate polynomials

The following notes are based on Chapter 5 and appendix A, of "Concrete Abstract Algebra From Numbers to Gröbener bases".

3.1 Relations

Definition 3.1. Let S be a set and let $R \subseteq S \times S$ then R is called a *relation* on S and we write xRy to mean $(x, y) \in R$.

Definition 3.2. These relations can have certain properties, for instance R is called *reflective* if xRx, *symmetric* if $xRy \implies yRx$, *antisymmetric* if $xRy \wedge yRx \implies x = y$ and *transitive* if $xRy \wedge yRz \implies xRz$ for every $x, y, z \in S$

Definition 3.3. If R is reflective, symmetric and transitive, then R is called an *equivilence relation*. On the other hand if R is reflective, antisymmetric and transitive, then R is called a *partial ordering*

3.1.1 Partial Orderings

Definition 3.4. A partial ordering R on S is called *total ordering* if $x \leq y$ or $y \leq x$ for every $x, y \in S$. If every non-empty $M \subseteq S$ as a *minimum element* $m \in M$, meaning $m \leq x$ for all $x \in M$, then $\leq$ is called a *well ordering* on S

3.2 Orderings

Definition 3.5. A total ordering $\leq$ on $\mathbb{N}^n$ is called a *term ordering* if: 1. $0 \leq v$. 2. $v_1 \leq v_2 \implies v_1 + v \leq v_2 + v$. For all $v, v_1, v_2 \in \mathbb{N}^n$.

Example 3.6. The *lexicographic ordering* $\leq_{lex}$ on $\mathbb{N}^n$ is defined by $v \leq_{lex} w$ if there exists $j \in \mathbb{N}$ such that $v_i = w_i$ for all $i \leq j$ and $v_j < w_j$ or $j = n$. [1]

The *graded lexicographic ordering* $\leq_{glex}$ is defined by $v \leq_{glex} w$ if $\sum_{i=1}^{n} v_i \leq \sum_{i=1}^{n} w_i$ in the case of equality we also require that $v \leq_{lex} w$. □

[1] The lexicographic ordering can be thought of the "alphabetic" ordering of the tuples of natural numbers.

3.2.1 Dicksons Lemma

Lemma 3.7. *[Dickons] Let $S \subseteq \mathbb{N}^n$. Then there exists a finite set of vectors $v_1, v_2, \dots v_m \in S$ such that*

$$S \subseteq \bigcup_{i=1}^{m} v_i + \mathbb{N}^n$$

Proof. We use strong induction, if $n = 1$, then pick $v_1 = \inf S$, then clearly $S \subseteq v_1 + \mathbb{N}$.

Let $\pi : \mathbb{N}^n \to \mathbb{N}^{n-1}$ denote the map $(x_1, x_2 \dots, x_n) \mapsto (x_2 \dots, x_n)$. Using our hypothesis we see that there exists $v_1, v_2, \dots v_m \in \pi(S) \subseteq S$ such that $\pi(S) \subseteq \bigcup_{i=1}^{m} v_i + \mathbb{N}^{n-1}$ (since $\pi(S) \subseteq \mathbb{N}^{n-1}$)

However it is not always the case that $S \subseteq \bigcup_{i=1}^{m} v_i + \mathbb{N}^n$, after all $v_1, v_2, \dots v_m$ wheren't constructed with the first coordinates in mind. Hence let

$$M = \max\{(v_1)_1, (v_2)_1, \dots, (v_m)_1\}$$

and $S_i = \{s \in S | s_1 = i\}$ as well as $S \leq M = \{s \in S | s_1 \leq M\}$. Then $S = \bigcup_{k=0}^{M-1} S_k \cup S_{\leq M}$, now since $S_{\geq M} \subseteq \bigcup_{i=1}^{m} v_i + \mathbb{N}^n$, and S_j can be identified with $\mathbb{N}^{n-1}$ (The first coordinate of each element is fixed.) the result follows from our hypothesis ■

Corollary 3.8. *Every term ordering $\leq$ on $\mathbb{N}^n$ is a well ordering*

Proof. Let $S \subseteq \mathbb{N}^n$ be a non-empty subset, then by Dicksons Lemma there are finitely many elements $v_1, v_2, \dots v_m \in S$ such that $S \subseteq \bigcup_{i=1}^{m} v_i + \mathbb{N}^n$. Now if $v \in v_i + \mathbb{N}^n$, then $v = v_i + w$ for some $w \in \mathbb{N}^n$ which implies $v - v_i \in \mathbb{N}^n$ hence $v = (v - v_i) + v_i \geq v_i$ by Definition 3.5, this means that the smallest element in S is the smallest element in $v_1, v_2 \dots, v_m$. ■

Definition 3.9. Let $f = \sum_{i=1}^{m} a_i X^{v_i} \in \mathbb{F}[X_1, X_2 \dots, X_n]$ then the *leading term* of f with respect to the term ordering $\leq$ is denoted as $LT_{\leq}(f) = a_j X^{v_j}$ where $v_j \leq v_i$ for all i. We also often write $aX_1^v \leq aX^{v_2}$ if $v_1 \leq v_2$.

If R is a domain then $LT_{\leq}(fg) = LT_{\leq}(f) LT_{\leq}(g)$ for all $f, g \in R[X_1, X_2 \dots, X_n]$.

3.3 The Division Algorithm

Proposition 3.10. *Let R be a domain, $\leq$ a term ordering and $f \in R[X_1, X_2 \dots, X_n] \setminus \{0\}$. Suppose that $f_1, f_2 \dots, f_m \in R[X_1, X_2 \dots, X_n] \setminus \{0\}$, then there exists $a_1, a_2 \dots, a_m, r \in R[X_1, X_2 \dots, X_n]$ such that*

$$f = \sum_{i=1}^{m} a_i f_i + r$$

where $r = 0$ or none of the terms in r is divisible by $LT_{\leq}(f_i)$. Furthermore $LT_{\leq}(a_i f_i) \leq LT_{\leq}(f)$ if $a_i \neq 0$.

Here is the algorithm for computing $a_1, a_2 \dots, a_m, r$:

(i) Let $a_1 := a_2 := a_m := r := 0$ and $s := f$ giving: $f \overset{(*)}{=} \sum_{i=1}^{m} a_i f_i + (r + s)$ (The main idea is that this expression, should stay constant during the algorithm.)

(ii) We now iterate. If $s = 0$ we are done with the algorithm otherwise we perform the following steps

(a) If $LT_{\leq}(f_i)|LT_{\leq}(s)$ for some i, then pick the smallest of these i's and let:

$$s := s - \frac{LT_{\leq}(s)}{LT_{\leq}(f_i)} f_i, \quad a_i := a_i + \frac{LT_{\leq}(f_i)}{LT_{\leq}(f_i)}$$

Notice that $(*)$ still holds.

(b) If $LT_{\leq}(s)$ is not divisible by any $LT_{\leq}(f_i)$, we set $r := r + LT_{\leq}(s)$ and $s := s - LT_{\leq}(s)$, again notice that $(*)$ still holds.

We will leave out the proof of the correctness of this algorithm.

3.4 Gröbner bases

The main idea is that we want to have a set, where the remainder of the division algorithm does not depend on the term ordering.

Definition 3.11. Let $f_1, f_2 \ldots, f_m \in \Bbbk[X_1, X_2 \ldots, X_n] \setminus \{0\}$, then the set $F := \{f_1, f_2 \ldots, f_m\}$ is called a *Gröbner basis for an ideal* $I \subseteq \Bbbk[X_1, X_2 \ldots, X_n]$ with respect to the term ordering $\leq$ if $F \subseteq I$ and for every $f \in I \setminus \{0\}$, we have $LT_{\leq}(f_i)|LT_{\leq}(f)$ for some $i = 1, \ldots, m$. Finally F is called a *Gröbner basis* with respect to the term ordering $\leq$ if it is a Gröbner basis of $\langle f_1, f_2 \ldots, f_m \rangle$.

Proposition 3.12. *Let $\{f_1, f_2 \ldots, f_m\}$ be a Gröbner basis with respect to the term ordering $\leq$. Then for $I = \langle f_1, f_2 \ldots, f_m \rangle$ we have $f \in I$ if and only if f divided by $f_1, f_2 \ldots, f_m$ has remainder* 0.

4 Field Theory

The following chapter will be based on "Fields and Galois Theory" by John M. Howie.

Definition 4.1. suppose K, L are fields and $\phi : K \to L$ is a monomorphism (an injective homomorphism), then L is called an **extension field** of K, denoted $L : K$.

Note that since we can identify K with $\phi(K)$, we can regard K as a subfield of L (and L as a vectorspace over K). Hence there exists a basis of L over K. The cardinality of such a basis is called the *dimension* of L, this dimension will be called the *degree of L over K*, which will be denoted $[L : K]$

Example 4.2. The degree $[\mathbb{R} : \mathbb{Q}]$ is infinite since $\mathbb{R}$ is uncountable and any finite extension of $\mathbb{Q}$ is countable. In contrast $[\mathbb{C} : \mathbb{R}] = 2$ as $\{1, i\}$ forms a basis. □

Theorem 4.3. *Let $L : K$, then $L = K$ if and only if $[L : K] = 1$.*

Proof. The proof is relatively trivial, so it is omited. ■

Theorem 4.4. *Let $M : L$ and $L : K$ then $[M : L][L : K] = [M : K]$.*

Proof. The main idea is to show that if $\{a_1, a_2 \ldots, a_r\}$ is linear independent of M over L, and $\{b_1, b_2 \ldots, b_s\}$ is linearly independent of L over K, then $\{a_i b_j | i = 1, \ldots, r, j = 1, \ldots, s\}$ is linearly independent of M over K. ■

Corollary 4.5. *Let $K_1, K_2 \ldots, K_n$ be fields such that $K_{i+1} : K$ for all $i = 1, \ldots, n-1$. Then:*

$$[K_n : K_1] = \prod_{i=0}^{n-2} [K_{n-i} : K_{n-i-1}]$$

Exercise 4.6 (3.2)**.** Let $M : L$ and $L : K$ such that $[M : K] < \infty$ show that $[M : K] = [L : K] \implies M = L$

Proof. We have $[L : K][M : L] = [M : K]$ by Theorem 4.4, hence $[M : L] = 1$ since $[M : K] = [L : K]$, by Theorem 4.3 ■

Exercise 4.7. Let $L : K$ such that $[L : K]$ is prime, show that there exists no subfield E of L such that $K \subset E \subset L$.

Proof. Assume for contradiction that such a subfield exists, then $[K : E][E : L] = [L : K]$, however this would mean that $[L : K]$ is composite afterall, since $[K : E] = 1 \iff K = E$ and $[E : L] = 1 \iff E = L$, which is a contradiction. ■

4.1 Extensions and Polynomials

Definition 4.8. Let $K : L$ and $S \subseteq L$, let $K(S) = \{F \subseteq L | F \text{ is a field and } K \cup S \subseteq F\}$, then $K(S)$ is called the **subfield of** L **generated over** K **by** S. If $S = \{a_1, a_2 \ldots, a_n\}$ is finite we write $K(S)$ as $K(a_1, a_2 \ldots, a_n)$.

Theorem 4.9. *The subfield $K(S)$ coincides with the set E of all elements of L that can be expressed as quotients of finite linear combinations (with coefficients in K) of finite products of elements of S*

Remark 4.10. This is perhaps simply quotients of polynomials?

When $S = \{a\}$ we get that $K(a)$ is simply the set of quotients of polynomails in a with coefficients in K and $K(a)$ is called a *simple extension* of K.

Theorem 4.11. *Let $K : L$ and $a \in L$, then either:*

(i) *$K(a)$ is isomorphic to $K(X)$ the field of rational forms with coefficents in K*

(ii) *there exists a unique monic irreducible polynomial $m \in K[X]$ (this is called the minimal polynomail of a) with the property that for all $f \in K[X]$:*

   (a) $f(a) = 0$ *if and only if* $m|f$.

   (b) $K(a) = K[a]$.

   (c) $[K[a] : K] = \deg(m)$.

Remark 4.12. If we know that $[K[a] : K] = n$ and we find a monic polynomial g of degree n such that $g(a) = 0$ then g is the minimum polynomial of a, the minimum polynomial is unique.

Definition 4.13. If $a \in L$ has a minimum polynomail over K, then a is said to be **algebraic** over K and that $K[a](= K(a))$ by Theorem 4.11 is a **simple algebraic extension** of K. A complex number which is algebraic over $\mathbb{Q}$ is called an **algebraic number**. If $K(a)$ is isomorphic to $K(X)$ (the field of rational functions over K) we say that a is **trancendental** over K and $K(a)$ is called a **simple transcendental extension of** K. The number $a \in \mathbb{C}$ which is trancendental over $\mathbb{Q}$ is called a **trancendental number**.

We will show in Theorem 4.18 that the set of algebraic numbers forms a subfield of $\mathbb{C}$, this subfield will be denoted by $\mathbb{A}$.

Theorem 4.14. *Let $K(a)$ be a simple trancendental extension of K. Then $K(a) : K = \infty$.*

Proof. The elements $1, a, a^2, \ldots$ are linearly independent over K. ∎

Definition 4.15. $L : K$ is called an **algebraic extension** if every element of L is algebraic over K. Otherwise L is called a **transcendental extension.**

Theorem 4.16. *If $[K : L]$ is finite, then $K : L$ is an algebraic extension.*

Proof. Suppose that a is a trancendental element over K, then $1, a, a^2, \ldots$ are linearly independent over K, so $[K : L] = \infty$ afterall. ■

Proposition 4.17. *Let $M : L$ and $L : K$ and $a \in M$, then if a is algebraic over K, then it is also algebraic over L.*

Proof. Follows from the fact that: $K[X] \subseteq L[X]$. ■

Theorem 4.18. *Let $K : L$ and $\mathcal{A}(L) = \{a \in L | a \text{ is algebraic over } K\}$, then $\mathcal{A}(L)$ is a subfield of L.*

Proof. suppose $a, b \in \mathcal{A}(L)$. Then:

$$a - b \in K(a, b) = (K[a])[b]$$

by Theorem 4.17 b is algebraic over $K[a]$, so both $[K[a] : K]$ and $[(K[a])[b] : K[a]]$ are finite. From Theorem 4.4 it follows that $[K(a, b) : K]$ is finite. Hence it follows from Theorem 4.16 that $a - b$ is algebraic over K. A similar argument can be made to show that $a/b \in \mathcal{A}(L)$ for all $a, b(\neq 0) \in \mathcal{A}(L)$. ■

Theorem 4.19. *The field $\mathbb{A}$ is countable.*

The proof relises on the arithmetic of infinite cardinal numbers see (*https://en.wikipedia.org/wiki/Aleph_number*).

Proof. Let $|\mathbb{Q}| = \aleph_0$, since $\mathbb{Q} \subseteq \mathbb{A}$ we know that $|\mathbb{A}| \geq |\mathbb{Q}| = \aleph_0$. Now since the number of monic polynomails of degree n over $\mathbb{Q}$ is $\aleph_0^n = \aleph_0$ (can be relized by a process similar to showing that the set of rational numbers are countable.) Each of these polynomials can have at most n roots, hence the number of roots of these monic polynomails are at most $n\aleph_0 = \aleph_0$. So $|\mathbb{A}| \leq \aleph_0$. ■

Corollary 4.20. $\mathbb{C} \setminus \mathbb{A} \neq \emptyset$.

Proof. The proof relies on the fact that $|\mathbb{C}| = |\mathbb{R}| = 2^{\aleph_0}$ so $|\mathbb{C} \setminus \mathbb{A}| = 2^{\aleph_0} > 0$. ■

5 Galois Theory

Appendices

A Number Theory for Mum

Theorem A.1. *Suppose $n \in \mathbb{Z}$ and that n' is obtained from n by interchanging two digits, that is $n' = n + n_i(10^j - 10^i) + n_j(10^i - 10^j)$ where n_i and n_j are the ith and jth digits of n, with $j > i$. Then $n' - n$ is divisible by 9.*

Proof. By the definition of n' we have:

$$\begin{aligned} n' - n = n_i(10^j - 10^i) + n_j(10^i - 10^j) &= (n_i - n_j) \cdot (10^j - 10^i) \\ &= (n_i - n_j) \cdot 10^i(10^{j-i} - 1) \end{aligned}$$

the rest follows as $10^{j-i} - 1 = 99\ldots9$ which is clearly divisible by 9. ■

Corollary A.2. *Let $n \in \mathbb{Z}$ and n_k be obtained from n by interchanging k of the digits then $n_k - n$ is divisible by 9.*

Proof. Suppose n_k was obtained by interchanging two digits of n_{k-1} and so on until $n_1 = n$ is reached. Observe that:

$$\begin{aligned} n_k - n &= n_k - n_{k-1} + n_{k-1} - n_{k-2} + \cdots + n_2 - n \\ &= (n_k - n_{k-1}) + (n_{k-1} - n_{k-2}) + \cdots + (n_2 - n) \end{aligned}$$

The rest follows as every term in the sum is divisible by 9 by Theorem A.1. ■

Bibliography

[1] Axler, S. (2015). *Linear Algebra Done Right*. Undergraduate Texts in Mathematics. Springer International Publishing, 3rd edition.

[2] Fulton, W. (2008). Algebraic curves: An introduction to algebraic geometry. avalible at https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

[3] Giulietti, M. (2003). Notes on algebraic-geometric codes. Lecture notes from a series of lectures, given in May 2003.

[4] Göttsche, L. (2012). Algebraic geometry lectures. Video recordings of algebraic geometry lectures, given at ICTP Mathematics, can be found at https://www.youtube.com/playlist?list=PLLq_gUfXAnkkeQKfjfWwyJP8eUV08Kygd.

[5] Göttsche, L. (2016). Introduction to algebra. Lecture notes, can be found at: https://users.ictp.it/~gottsche/.

[6] Huffman, W. C. and Pless, V. (2003). *Fundementals of Error-Correcting Codes*. Cambrige University Press, 1st edition.

[7] Lauritzen, N. (2003). *Concrete Abstract Algebra: From Numbers to Gröbner Bases*. Cambridge University Press, 1st edition.

[8] Pellikaan, R., Wu, X.-W., Bulygin, S., and Jurrius, R. (2018). *Codes, Cryptology and Curves with Computer Algebra*. Cambrige University Press, 1st edition.

[9] Shum, K. and Zhang, B. (2016). The singleton bound and reed-solomon code. avalible at https://piazza.com/class_profile/get_resource/isgy6spmwwm3ba/itzo5as3bbw7kk.

[10] Tsfasman, M., Vlăduţ, S., and Nogin, D. (2007). *Algebraic Geometry Codes: Basic Notations*. American Mathematical Society, 1st edition.

[11] Weintraub, S. H. (2020). *Galois Theory*. Springer, 2nd edition.