Matehmatical Tools For Cryptography

Disclaimer

This contains lessons from Mr. Zaimi, with contents that are either added, changed or rearranged, written by HADIOUCHE Azouaou.

Chapter 1

Remainders

This part will just be a remainder of the important definitions, propositions and theorems of the field extension course that are needed for this course. We assume that rings in this case are commutative rings with unity.

1.1. Rings & Homomorphisms

Definition 1.1.1 (Ring Homomorphism/Kernel/Image): *Let R, R' be two rings and $f : R \to R'$ a map. We say that f is a ring homomorphism if*

$$f(a+b) = f(a) + f(b). \qquad f(ab) = f(a)f(b).$$

define $\operatorname{Ker} f = f^{-1}(\{0\})$ *and* $\operatorname{Im} f = f(R)$.

Proposition 1.1.2: *Let $f : R \to R'$ be a ring homomorphism*

- $\operatorname{Ker} f$ *is an ideal of R and* $\operatorname{Im} f$ *is a subring of R'.*
- $\operatorname{Ker} f = \{0\} \Leftrightarrow f$ *injective and* $\operatorname{Im} f = R' \Leftrightarrow f$ *surjective.*
- *If R, R' are fields then $f \equiv 0$ or $f(1) = 1$.*

Theorem 1.1.3 (First Isomophism Theorem): *Let $f : A \to B$ be a ring homomorphism, then* $\operatorname{Im} f \cong A/\operatorname{Ker} f$ *and for $I \subseteq \operatorname{Ker} f$ is an ideal then there exists a unique isomorphism $f_* : A/I \to B, f_*(x+I) = f(x)$ with $f = f_* \circ \pi$ and $\pi(x) = x + I$ the cannonical surjection.*

$$\begin{tikzcd} A \arrow[r, "\pi"'] \arrow[rr, bend left, "f"] & A/I \arrow[r, "f_*"'] & B \end{tikzcd}$$

1.2. Ideals, UFDs, PIDs & EDs

Definition 1.2.4 (Elements): *Let R be a ring, we have the following:*

- ***Unit:*** *$x \in R$ is a unit if $\exists y \in R, xy = 1$, denoted R^*.*
- ***Zero Divisor:*** *$x \in R \setminus \{0\}$ is a zero divisor if $\exists y \in R, xy = 0$.*
- ***Irreducible:*** *$x \in R$ is irreducible if $x = x_1 x_2 \Rightarrow x_1 \in R^* \vee x_2 \in R^*$.*

Definition 1.2.5 (Ideals): *Let R be a ring, $I \subseteq R$ ideal, we have:*

- ***Prime Ideal:*** *I is prime if $\forall a, b \in R, ab \in I \Rightarrow a \in I \vee b \in I$.*
- ***Principal Ideal:*** *I is principal if $\exists x \in R, I = (x) = xR$.*
- ***Maximal Ideal:*** *I is maximal if $\forall M$ ideal, $I \subseteq M \subseteq R \Rightarrow M = I$ or R.*

Proposition 1.2.6: *Let $f : R \to R'$ be a ring homomorphism and let I' be an ideal of R' then $I = f^{-1}(I')$ is an ideal of R, if I' is prime then I is prime.*

Theorem 1.2.7: *Let R be a ring and I, J ideals of R*

- *I is a prime ideal $\Leftrightarrow R/I$ is an integral domain.*
- *I is a maximal ideal $\Leftrightarrow R/I$ is a field.*
- *if $I \subseteq J$ then $(A/I)/(J/I) \cong A/J$.*

Definition 1.2.8 (Domains): *Let R be a ring, we have the following:*

- ***Integral Domain:*** *R is an integral domain if $xy = 0 \Rightarrow x = 0$ or $y = 0$.*
- ***Principle Ideal Domain:*** *R is a PID if for any ideal I in R, I is principle.*
- ***Euclidean Domain:*** *R is said to be an ED if $\exists \nu : R/\{0\} \to \mathbb{N}$ a valuation function, $\forall a, b \in R, \exists q, r \in R, a = bq + r, r = 0$ or $\nu(r) < \nu(b)$.*
- ***Unique Factoriation Domain:*** *R is a UFD if any element can be decomposed into a unique product of irreducible elements.*

Theorem 1.2.9:

- *If R is a UFD and $x \in R$ is irreducible, then (x) is prime.*
- *If R is an integral domain and a PID, every prime ideal is maximal.*
- *ED ⇒ PID ⇒ UFD.*

1.3. Ring Of Polynomials

Definition 1.3.10 (Ring Of Polynomials): *Let R be a ring, we define*

$$R[X] = \left\{\sum_{i\in I} a_i X^i \mid I \text{ finite}, \{a_i\}_{i\in I} \subseteq R\right\}.$$

to be the ring of polynomials on R, and for any $P \in R[X]$ we set

$$\deg P = \max\{i \in \mathbb{N} \mid X^i \text{ has a non-zero coefficent in } P\}.$$

Definition 1.3.11 (Polynomials): *Let L/K be a field extension and $P \in K[X]$*

- ***Minimal:*** *P is the minimal polynomial of $\alpha \in L$ if it is the unique monic polynomial with the smallest degree which vanishes at α denoted $\operatorname{Irr}(\alpha, K, x)$.*

Proposition 1.3.12: *Let K be a field, $P(X) \in K[X]$ with $\deg P \in \{2, 3\}$ then we have that P is reducible over K ⇔ P has a zero in K.*

Theorem 1.3.13: *Let R be a ring*

- *R is an integral domain ⇒ $R[X]$ is an integral domain.*
- *$P = \sum a_i X^i$ is a unit in $R[X]$ ⇔ $a_0 \in R^*$ and $\forall i \geq 1, a_i$ nilpotent.*
- *$P \in R[X]$ irreducible ⇒ $R[X]/(P) = \left\{\sum_{i=0}^{\deg P-1} a_i\alpha^i \mid a_i \in R\right\}$.*
- *Let α a root of $P \in R[X]$ then $\operatorname{Irr}(\alpha, K, X)$ divides P.*
- *if R is a field, $R[X]$ is a Euclidean domain with the valuation $\nu(P) = \deg P$.*

Proposition 1.3.14 (Eisenstein's Criterions):

- *Let $P(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[X]$, if there is a prime p such that $p \mid a_0, \ldots, p \mid a_{n-1}, p^2 \nmid a_0$ and $p \nmid a_n$ then P is irreducible over $\mathbb{Q}[X]$.*
- *Let $P(X) \in \mathbb{Z}[X]$ and $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_{n[X]}$ the extension of $k \mapsto k \bmod n$, if $\deg \varphi(P) = \deg P$ and $\varphi(P)$ is irreducible in $\mathbb{Z}_{n[X]}$ then P is irreducible in $\mathbb{Q}[X]$.*

1.4. Field Extensions

Definition 1.4.15 (Extension/Degree Of Extension): *Let L, K be two fields such that $K \subseteq L$, we call L a field extension of K and we denote it L/K, we define the degree of extension of L on K as $\dim_K L$ if it is finite and $+\infty$ if it is infinite, and we denote it $[L : K] = \dim_K L$.*

Definition 1.4.16 (Elements): *Let K be a field and $x \in K$.*

- ***Algebraic:*** *x is said to be algebraic if $\exists P \in K[X], \deg P > 0, P(x) = 0$.*
- ***Transcendental:*** *x is said to be transcendental if it is not algebraic.*
- ***Conjugate:*** *α is said to be the conjugate of β if β is a root of $\operatorname{Irr}(\alpha, K, x)$.*

Proposition 1.4.17: *If α, β are conjugates then $\operatorname{Irr}(\alpha, K, X) = \operatorname{Irr}(\beta, K, X)$.*

Definition 1.4.18 (Fields): *Let K be a field*

- ***Algebraically Closed:*** *K is said to be algebraically closed if any algebraic extension of K is K.*

Definition 1.4.19 (Extensions):

- ***L/K Algebraic Extension:*** *$\forall x \in L$, x is algebraic over K.*
- ***L/K Transcendental Extension:*** *if it is not an algebraic extension.*
- ***Algebraic Closure:*** *$\overline{K}$ is an algebraic closure of K if $\overline{K}/K$ is an algebraic extension and $\overline{K}$ is algebraically closed.*

Theorem 1.4.20: *Let L/K be a field extension and $\alpha_1, ..., \alpha_n \in L$ and set $\alpha = (\alpha_1, ..., \alpha_n)$ then*

- *$K[\alpha_1][\alpha_2]...[\alpha_n] = K[\alpha_1, ..., \alpha_n] = \{P(\alpha) \mid P \in K[X_1, ..., X_n]\}$ is the smallest ring containing K and $\alpha_1, ..., \alpha_n$.*
- *$K(\alpha_1)(\alpha_2)...(\alpha_n) = K(\alpha_1, ..., \alpha_n) = \{P(\alpha)/Q(\alpha) \mid P, Q \in K[X_1, ..., X_n], Q(\alpha) \neq 0\}$ is the smallest field containing K and $\alpha_1, ..., \alpha_n$.*
- *any extension of finite degree is algebraic.*

Theorem 1.4.21 (Steinitz):

1. *Any field is contained inside of an algebraically closed field.*
2. *Any two algebraic closures of a field are isomorphic.*

Chapter 2

Embeddings

Consider in this chapter, K, L, E, Ω denote fields, the lower-case elements are used for elements of fields.

2.1. Embedding

Definition 2.1.22 (Embedding): *Let $\sigma : K \to L$ a homomorphism, if $\sigma \not\equiv 0$ then σ is an embedding from K to L.*

Definition 2.1.23 (Extension/Restriction): *Suppose E is an extension of K, τ is an embedding of E into L such that $\forall k \in K, \tau(k) = \sigma(k)$, then τ is called an extension σ and σ is called a restriction of τ to K. Moreover if $\sigma = \mathrm{Id}_K$ then τ is called a K-embedding of E into L.*

Example:

- The unique embedding $\sigma : \mathbb{Q} \to \mathbb{C}$ is the identity, we prove $\sigma(1) = 1$, $\sigma(n) = n$, $\sigma(-n) = -n$, $\sigma(a/b) = \sigma(a)/\sigma(b)$ by induction, then $\sigma = \mathrm{Id}$.
- The embeddings $\tau : \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{C}$ has only two forms, given that $\tau|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$ then $\tau\left(a + b\sqrt{2}\right) = a + b\tau\left(\sqrt{2}\right)$ and since $\tau\left(\sqrt{2}\right)^2 = \tau\left(\sqrt{2}^2\right) = \tau(2) = 2 \Rightarrow \tau(\alpha) = \sqrt{2}$ or $\tau(\alpha) = -\sqrt{2}$.

Proposition 2.1.24: *Let τ be a K-embedding of L into E where $K \subseteq L$ and let $\alpha \in L$ be algebraic over K, then $\tau(\alpha)$ is a conjugate of α over K.*

Proof. Suppose α algebraic of degree d over K and let $P = \mathrm{Irr}(\alpha, K, x)$, we have $P(\alpha) = 0$ and $\tau(P(\alpha)) = \tau\left(\sum k_i \alpha^i\right) = \sum \tau(k_i)\tau(\alpha)^i = \sum k_i \tau(\alpha)^i = P(\tau(\alpha)) = 0$ then $\tau(\alpha)$ is a conjugate of α.

We used the fact that τ is a K-embedding in the evaluation $\tau(k_i) = k_i$.

Proposition 2.1.25: *Let K be a field, $\overline{K}$ an algebraic closure of K, $\alpha \in \overline{K}$ and let $\beta \in \overline{K}$ be a conjugate of α over K, then there is a K-embedding $\tau : K(\alpha) \to \overline{K}$ which is a K-isomorphism of $K(\alpha)$ into $K(\beta)$ sending α to β.*

Proof. Let α, β conjugates over K, then we have that $\mathrm{Irr}(\alpha, K, X) = \mathrm{Irr}(\beta, K, X)$. Define $I = (\mathrm{Irr}(\alpha, K, X))$, $\nu_\alpha : K[X] \to K[\alpha]$ and $\nu_\beta : K[X] \to K[\beta]$ such that $\nu_\alpha(P(X)) = P(\alpha)$ and $\nu_\beta(P(X)) = P(\beta)$ which are surjective by definition. We have that $\mathrm{Ker}(\nu_\alpha) = \mathrm{Ker}\left(\nu_\beta\right) = (\mathrm{Irr}(\alpha, K, X))$. From the first isomorphism theorem we have that there exists two isomophisms $(\nu_\alpha)_\star : K[X]/I \to K[\alpha]$ and $\left(\nu_\beta\right)_\star : K[X]/I \to K[\beta]$ such that $v_\alpha = (v_\alpha)_\star \circ \pi$ and $v_\beta = \left(v_\beta\right)_\star \circ \pi$. We also have that $K[\alpha] = K(\alpha)$ and $K[\beta] = K(\beta)$ since α, β are algebraic.

Set $\varphi : K(\alpha) \to K(\beta), x \mapsto \left(\left(v_\beta\right)_* \circ (v_\alpha)_*^{-1}\right)(x)$, φ is the composition of isomophisms then it is an isomorphism, let $x \in K, \varphi(x) = \left(v_\beta\right)_*\left((v_\alpha)_*^{-1}(x)\right) = \left(v_\beta\right)_*(x + I) = x$ so φ is a K-isomorphism and $\varphi(\alpha) = \left(v_\beta\right)_\star\left((v_\alpha)_*^{-1}(\alpha)\right) = \left(v_\beta\right)_\star(I) = \beta$.

Example: Let $\alpha = \sqrt[3]{2}$ we have $\mathrm{Irr}(\alpha, \mathbb{Q}, X) = X^3 - 2$, the conjugates of α over $\mathbb{Q}$ are $\alpha, j\alpha, j^2\alpha$, there are the following embeddings:

- $\tau_1 : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(\sqrt[3]{2}\right)$ which is the identity.
- $\tau_2 : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(j\sqrt[3]{2}\right)$ with $\tau_2\left(\sqrt[3]{2}\right) = j\sqrt[3]{2}$ an isomorphism.
- $\tau_3 : \mathbb{Q}\left(\sqrt[3]{2}\right) \to \mathbb{Q}\left(j^2\sqrt[3]{2}\right)$ with $\tau_3\left(\sqrt[3]{2}\right) = j^2\sqrt[3]{2}$ an isomorphism.

so there are exactly three embeddings.

Corollary 2.1.26: *Let α be algebraic over K of degree n, $\alpha \in \overline{K}$ an algebraic closure of K and let s be the number of distinct conjugates of α over K, then there are exactly s embeddings of $K(\alpha)$ into $\overline{K}$ sending α to its distinct conjugates.*

Proof. Follows immediatly from applying the previous two propositions.

Proposition 2.1.27: *Let L/K be an algebraic extension and σ a K-endomorphism of L, then σ is surjective.*

Proof. Let $\sigma : L \to L$ a K-embedding and $\alpha \in L$. Take $P = \operatorname{Irr}(\alpha, K, X)$ and set $C = \{\beta \in L \mid P(\beta) = 0\}$ so C is the set of conjugates of α over K, $\alpha \in C \neq \emptyset$ and C is finite since P has finite roots. For any $\beta \in C, \sigma(\beta) \in C$ since $P(\sigma(\beta)) = \sigma(P(\beta)) = 0$, σ is an injection from a finite set to itself so $\sigma(C) = C$ thus $\exists \beta \in C, \sigma(\beta) = \alpha$ so σ is surjective.