Notes for Cryptography

Professor Brian Sittinger

1 Introduction

HW problem 6

$$\mathbb{Q}_P = \{a/b | b \nmid a, a, b \in \mathbb{Z}, b \neq 0\}$$

this is a subset of $\mathbb{Q}$. A:

$$(\mathbb{Q}_{(p)})^* = \{\frac{a}{b} | p \nmid a, b\}$$

B: Only irreducible in $\mathbb{Q}_{(p)}$ come from factors whose num are divisible by p. Therefore

$$p^k m/n, p \nmid m, n$$

$$k = 1$$

for irreducible s.

2 Chapter 5 — Factorization into Prime Ideals

$$6 = 2 \cdot 3 = (1 + \sqrt{5})(1 - \sqrt{5})$$

Is a non-unique factorization into irreducibles. To restore factors, we will pass to prime ideals.

Let I be a proper ideal in a ring R. Then we define I as a *prime ideal* iff whenever

$$JK \subseteq I$$

for some ideals $J, K \subseteq R$, we have $J \subseteq I$ or $K \subseteq I$. Furthermore, we define I to be *maximal* iff there are no ideals strictly between I and R.

If R is an integral domain (no zero divisors and $ab = 0 \implies a = 0$ or $b = 0$) then

$$\langle p \rangle \text{ is a prime ideal } \iff p \text{ is prime or } p = 0$$

The only ideals in a field F are $\{0\}$ or $\langle 1 \rangle = F$. Lemma: let I be an ideal of R. Then I is maximal iff R/I is a field. Also, iff I is prime, R/I is an integral domain. A corollary of this is that maximal ideals are prime. The converse is not necessarily true. For example $\langle x \rangle$ is prime in $\mathbb{Z}[x]$ but not maximal. Note that

$$\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$$

We may now approach the following theorem. $\mathcal{O}$ is a "Dedicand Domain." That is, $\mathcal{O}$ is an integral domain with field of fractions K. One example of this is $\mathbb{Z}$ and $\mathbb{Q}$. Furthermore, $\mathcal{O}$ is Noetherian. Additionally, if $\alpha \in K$ satisfies a monic polynomial $f(x) \in \mathcal{O}[x]$ (with coeficients in $\mathcal{O}$) then $\alpha \in \mathcal{O}$. That is $\mathcal{O}$ is "integrally closed." For example

$$\mathbb{Z}[-\sqrt{3}] \neq \mathcal{O} \text{ but } \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \mathcal{O}_k$$

Every nonzero prime ideal of $\mathcal{O}$ is maximal (within Dedicand Domains). This final statement is basicailly theorem 2.10 from the book. I prove it below: let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Let $\alpha \in \mathfrak{p}$ be nonzero. Let $n = [K : \mathbb{Q}]$. So $N := N(\alpha) = \alpha_1(\alpha_2 \ldots \alpha_n) \in \mathfrak{p}$ where $a_i, 1 \leq i \leq n$ are the conjugates of n. So $\langle n \rangle \subseteq \mathfrak{p}$ Then $\mathcal{O}/\mathfrak{p}$ is finite because $\mathcal{O}/\langle p \rangle$ is finite, because $\mathcal{O}/\langle N \rangle$ is finite of order N^n and $\langle N \rangle \subseteq \mathfrak{p}$. Moreover $\mathcal{O}/\mathfrak{p}$ is an integral domain. Therefore $\mathcal{O}/\mathfrak{p}$ is a field (because finite integral domains are fields). And so we see that $\mathfrak{p}$ is maximal as required.

Some reminders:

1. $\mathfrak{a}|\mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals.
2. $\mathfrak{a} + \mathfrak{b} = \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\}$
3. $\mathfrak{a}\mathfrak{b} = \{\sum_{k=1}^{n} a_k b_k | a_k \in \mathfrak{a}, b_k \in \mathfrak{b}\}, n \in \mathbb{N}$. In the finitely generated case,

$$\mathfrak{a} = \langle a_1, a_2, \ldots, a_j \rangle$$

$$\mathfrak{b} = \langle b_1, \ldots, b_l \rangle$$

Then $\mathfrak{a}\mathfrak{b} = \langle a_i b_k | i = 1, \ldots, j, k = 1, \ldots, l \rangle$.

We now move onto our unique factorization theorem. Every ideal $\mathfrak{a} \in \mathcal{O}$ different from $\langle 0 \rangle, \langle 1 \rangle$ admits a unique factorization $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ into prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}$ (see pages 107-110). Which is unique up to order of the factors. The proof is in the book, but I give a sketch here. Let $\mathfrak{a} \subseteq \mathcal{O} \neq \langle 0 \rangle, \langle 1 \rangle$. Then there exist prime ideals in $\mathcal{O}$ such that $\mathfrak{p}_i \subseteq \mathfrak{a}$. For an ideal $\mathfrak{a} \subseteq \mathcal{O}$ we define $\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq \mathcal{O}\}$. This is called a "Fractional Ideal." Check $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} = \langle 1 \rangle = 0$. If

$$\mathfrak{a} \not\subseteq \mathcal{O}$$

Then

$$\mathfrak{a}^{-1} \not\supseteq \mathcal{O}$$

If $\mathfrak{a} \neq \{0\}$ and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset S of K. Then $S \subseteq \mathcal{O}$. $\mathfrak{p}$ maximal, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. For all nonzero $\mathfrak{a}$, $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}$. Define the fractional ideal of K as follows. A finitely generated $\mathcal{O}$ submodule $\mathfrak{A} \neq \{0\}$ of K iff there does not exist non-zero $c \in \mathcal{O}$ such that $c\mathfrak{a} \subseteq \mathcal{O}$ is an ideal of $\mathcal{O}$. Every fractional ideal $\mathfrak{a}$ has an inverse $\mathfrak{a}^{-1}$ such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. Note that J is the set of all fractional ideals of K is an Abelian group. Every nonzero $\mathfrak{a}$ is a product of prime ideals. Thus, the prime factorization is unique. Furthermore, fractional ideals have unique factorization.

An example: $\mathbb{Z}[\sqrt{-5}]$ revisited. Let $\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle, \mathfrak{q} = \langle 3, 1+\sqrt{-5}\rangle, \mathfrak{r} = \langle 3, 1-\sqrt{-5}\rangle$ We claim that the ideals are maximal and so prime. Note that for $\mathfrak{p}$

$$\left|\mathbb{Z}[\sqrt{-5}]/\langle 2\rangle\right| = 4$$

Since $\langle 2\rangle \not\subseteq \langle 2, 1+\sqrt{-5}\rangle$

$$\left|\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}\right|$$

has order *dividing* 4 by Lagrange theorem. The only possibility for

$$\left|\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}\right|$$

is 2 because

$$\langle 2\rangle \not\subseteq \mathfrak{p} \text{ and can't be } \mathbb{Z}[\sqrt{-5}]$$

Therefore, $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{Z}_2$, is a field. In other words, a ring with p elements with prime p is a field, and so that $\mathfrak{p}$ is maximal since $\mathbb{Z}[\sqrt{-5}]$ is a dedicand domain.

Our second claim is that these ideals are *not* principle. Suppose that $\mathfrak{p}$ are not principle. Suppose that $\mathfrak{p} = \langle a + b\sqrt{-5}\rangle$, $a, b \in \mathbb{Z}$. $\langle 1, 1+\sqrt{-5}\rangle$. So $2 = (a+b\sqrt{5})(c+d\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$ and $1+\sqrt{-5} = (a+b\sqrt{-5})(m+n\sqrt{-5})$. Take the norms to get

$$N(2) = 2^2(a^2+5b^2)(c+5d^2)$$

$$N(1+\sqrt{-5}) = (a^2+5b^2)(c^2+5d^2)$$

Thus

$$(a^2+5b^2) \mid 4 \text{ and } (a^2+5b^2) \mid 6$$

and so

$$(a^2+5b^2) \mid 6-4 = 2$$

Thus $(a^2+5b^2) = 1, 2$, but if it is 1, then it is a unit. But there are no solutions if it is 2. Thus no a, b exist, and $\mathfrak{p}$ is not principal. Claim 3:

$$\mathfrak{p}^2 = \langle 2\rangle, \mathfrak{q}\mathfrak{r} = \langle 3\rangle, \mathfrak{p}\mathfrak{q} = \langle 1+\sqrt{-5}\rangle, \mathfrak{p}\mathfrak{r} = \langle 1-\sqrt{-5}\rangle$$

The upshot of this is that

$$\langle G\rangle = \langle 2\rangle\langle 3\rangle = \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle = p^2qr = pqpr$$

Proof for $p^2 = \langle 2\rangle$ is

$$p^2 = \langle 2\cdot 2, 2(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle$$

$$p^2 = \langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}+-(2+2\sqrt{-5})\rangle$$

$$p^2 = \langle 4, 2+2\sqrt{-5}, 6\rangle$$

Since units don't matter and -6 can be replaced by 6. Furthermore we can use $6-4=2$. Thus this is $\langle 2\rangle$. We can add, subtract or multiply be other generators.

2.1 The Norm of an Ideal

Consequences:

1. Ideal GCD $\mathfrak{g}$ and LCM $\mathfrak{l}$. Let

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i} \text{ and } \mathfrak{b} = \prod_i \mathfrak{p}_i^{f_i}$$

   GCD $\mathfrak{g}|\mathfrak{a}, \mathfrak{b}$. And if $\mathfrak{g}'$ has the same properties then $\mathfrak{g}'|\mathfrak{g}$. Rule

$$\mathfrak{g} = \prod_i \mathfrak{p}_i^{\min(e_i, f_i)}, \mathfrak{l} = \prod_i \mathfrak{p}_i^{\max(e_i, f_i)}$$

   Lemma:

$$\mathfrak{g} = \mathfrak{a} + \mathfrak{b}$$

$$\mathfrak{l} = \mathfrak{a} \cap \mathfrak{b}$$

2. We define the Norm of an ideal $\mathfrak{N}$.

$$\mathfrak{N}(\mathfrak{a}) := |\mathcal{O}/\mathfrak{a}|$$

   Also, fyi,

$$\Phi(\mathfrak{a}) = |(\mathcal{O}/\mathfrak{a})^*|$$

   but we won't need this here.

Recall that for every nonzero ideal, $\mathfrak{a}$ of $\mathcal{O}$ has a $\mathbb{Z}$-basis $\{\alpha_1, \dots, \alpha_n\}$ where $n = [K : \mathcal{O}]$. Then

$$\mathfrak{N}(\mathfrak{a}) = \left[\frac{\Delta[\alpha_1, \dots, \alpha_n]}{\Delta_k}\right]^{1/2}$$

This is used in the homework.

A corollary, suppose that $\mathfrak{a} = \langle \alpha \rangle$. Then

$$\mathfrak{N}(\mathfrak{a}) = |N(\alpha)|$$

Proof, we let $\{\omega_1, \dots, \omega_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}$. Then, $\{\alpha\omega_1, \dots \alpha\omega_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$. Therefore,

$$\mathfrak{N}(\mathfrak{a}) = \left[\frac{\Delta[\alpha\omega_1, \dots, \alpha\omega_n]}{\Delta[\omega_1, \dots, \omega_n]}\right]^{1/2} = \left[\frac{N(\alpha)^2 \Delta_k}{\Delta_k}\right]^2 = |N(\alpha)|$$

Some facts:

$$\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$$

If $\mathfrak{N}(\mathfrak{a})$ is prime, then $\mathfrak{a}$ is prime. Also, $\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$. This is because $\mathfrak{N}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|i \in \mathfrak{a}$ by lagrange. If $\mathfrak{a}$ is prime then, $\mathfrak{N}(\mathfrak{a}) = p^m$ for some prime p and $m \leq [K : \mathbb{Q}]$. Theorem: finiteness results.

1. Any nonzero ideal $\mathfrak{a} \subseteq \mathcal{O}$ has a finite number of divisors.

2. Any nonzero "rational integer" in $\mathbb{Z}$ belongs to finitely many ideals. This comes down to a norm calculation.

3. Only finitely many ideals (false for numbers) of $\mathcal{O}$ have a given fixed norm. This flows from the finiteness of the number of ideals in $\mathcal{O}$.

Fact, let $\mathfrak{a}$ be an ideal. Then $\mathfrak{a} = \langle \alpha, \beta \rangle$ for some $\alpha, \beta \in \mathcal{O}$. At most 2 generators. For example, $\mathbb{Z}[\sqrt{-5}]$.

$$\langle 6 \rangle = \mathfrak{p}^2 \mathfrak{q} \mathfrak{r}$$

as previously defined. Suppose $6 \in \mathfrak{a}$. Then $\langle 6 \rangle \subseteq \mathfrak{a}$, which is equivalent to $\mathfrak{a} | \langle 6 \rangle = p^2 q r$. So, $\mathfrak{a} = \mathfrak{p}^a \mathfrak{q}^b \mathfrak{r}^c, a \in \{0, 1, 2\}, b, c \in \{0, 1\}$. So 6 belongs to finitely many ideals. How many ideals have norm $\langle 6 \rangle$. This can only happen when $\mathfrak{a} | \langle 6 \rangle$ by fact 3. Writing $\mathfrak{a} = \mathfrak{p}^a \mathfrak{q}^b \mathfrak{r}^c$, implies that $N(\mathfrak{a}) = 2^a 3^b 3^c$ implies that $\mathfrak{a} = \mathfrak{p}\mathfrak{q}$ or $\mathfrak{p}\mathfrak{f}$.

Theorem: $\mathcal{O}$ factors into irreducible elements iff every ideal in $\mathcal{O}$ is principle. First, PIDs are UIDs. Going the other way, it suffices to show that every prime ideal is principal. Let $\mathfrak{p}$ be a nonzero prime in $\mathcal{O}$ Then $\mathfrak{p} | \langle \mathfrak{N}(\mathfrak{p}) \rangle$. Note $n = \pi_1 \pi_2 \ldots \pi_s$. Since $\mathfrak{p}$ is prime, $\mathfrak{p} | \langle \pi_i \rangle$ for some i. Since we have factors in $\mathcal{O}$, π_i is prime. Therefore $\langle \pi_i \rangle$ is prime, and so $\mathfrak{p} = \langle \pi_i \rangle$.

Read/skim through chapters 6—8 from the book.