Notes for Cryptography

Professor Brian Sittinger

2/1/16

1 Introduction to Abstract Algebra

Homework may be submitted by email, but hard-copies are preferred. If not done by the end of class, it may be turned in by the end of the week at the professors box up the stairs in Del Norte Hall. Try to find this mythic location soon.

While last course was a crash-course in elementary number theory, today we review abstract algebra.

Let G be a non-empty set with a binary operation denoted $*$ such that

$$* : G \times G \to G$$

G is an Abelian group if

1. Closure: If $a, b \in G$, then $a * b \in G$
2. Identity $e \in G$ such that $a * g = g \forall g \in G$ and $g * a = g$
3. Inverse $\forall a \in G, \exists a^{-1} \in G$ such that $a * a^{-1} = e$ and $a^{-1} * a = e$
4. Associativity: $\forall a, b, c \in G$
$$a * (b * c) = (a * b) * c$$
5. Commutativity $\forall a, b \in G, a * b = b * a$

Now, $\mathbb{N}$ is not a group on addition, but $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_n$ are. On multiplication, $\mathbb{N}, \mathbb{Z}$ are not groups, but $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Z}_n^* = \{a \in \mathbb{Z} | \gcd(a, n) = 1\}$ are groups. Remember that

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$$

2 Commutative Rings

We define a commutative ring as a set R that contains 0 and 1 $0 \neq 1$ with two binary operations $*$ and $+$ such that R is an Abelian group on $+$. Furthermore, R is a commutative semi-group on $*$, which means that it is closed under $*$, $*$

is commutative, $*$ is associative, it has 1 as the identity. Note the absence of inverses. We also have the distributive axiom/law

$$\forall a, b, c \in \mathbb{R}, a * (b + c) = a * b + a * c$$

$\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_n$, and the set of all polynomials with rational coefficient are all commutative rings. If a commutative ring is also closed under multiplicative inverses, we have a field. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$. If a field has finitely many elements, then the order of the field is p^r for prime p and natural number r. Also, any two finite fields of the same order are isomorphic to each other. When we have polynomials over a field, we have a division algorithm.

The set of Gaussian Integers

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$$

They are, in essence, the lattice points on the Cartesian plane. This is a commutative ring. Also, the set

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}$$

where d is square free is also a commutative ring. Also

$$\mathbb{Q}[d] = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$$

where d is square free is a field.

3 Ideals

$$x + y^p = (x + y)(x + \omega y)(x + \omega^2 y) \ldots (x + \omega^{p-1} y)$$

Where

$$\omega = e^{\frac{2\pi}{p} i}$$

is a root of unity. But this is not a unique factorization.

An ideal is a set of numbers. Let R be a commutative ring (with 1). Then $I \subseteq R$ is called an ideal if:

$$x, y \in I \implies x + y \in I$$

$$x \in I, r \in R \implies rx \in I$$

Note that if we let $x_1, x_2, \ldots, x_n \in R$ then

$$\langle x_1, x_2, \ldots, x_n \rangle = \{r_1 x_1 + r_2 x_2 + \cdots + r_n x_n | r_1, \ldots, r_n \in R\}$$

is an ideal of R. It is an ideal generated by $x_1, \ldots, x_n$. Let us consider

$$\langle 4 \rangle = \{4n | n \in \mathbb{Z}\}$$

$$\langle 4 \rangle \cap \langle 10 \rangle = \langle 20 \rangle$$

since 20 is the LCM of 4 and 10. To prove this, show that each set contains the other.

We now consider the addition of ideals. Let

$$I = \langle x_1, \ldots, x_m \rangle$$

$$J = \langle j_1, \ldots, j_n \rangle$$

then

$$I + J = \langle x_1, \ldots, x_m, y_1, \ldots, y_m \rangle$$

This is noted as follows

$$\langle 4 \rangle + \langle 10 \rangle = \langle 4, 10 \rangle$$

Note that all ideals in $\mathbb{Z}$ are generated by a single element, called the "principle."

$$\langle 4 \rangle + \langle 10 \rangle = \langle \gcd(4, 10) \rangle = \langle 2 \rangle$$

4 Homomorphisms/Isomorphisms

Let R, S be rings. A map ϕ from R to S is satisfied if

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$$

$$\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$$

And possibly?

$$\phi(0_R) = 0_S$$

$$\phi(1_R) = 1_S$$

If ϕ is also 1 to 1 and onto, ϕ is an isomorphism, and

$$R \cong S$$

An example:

$$\pi : \mathbb{Z} \to \mathbb{Z}_n$$

Then π is a ring homomorphism. But π is not an isomorphism. Ask more about why we can't prove this by induction.

4.1 Kernals

The kernal of

$$\ker\pi \equiv \{a \in \mathbb{Z} | \pi(a) = 0\}$$

For our previous definition of π,

$$\ker\pi = m\mathbb{Z}$$

And we can say that

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$$

Note that

$$\mathbb{Z}/m\mathbb{Z} \equiv \{a + m\mathbb{Z} | a \in \mathbb{Z}\}$$

An example:

$$\phi : \mathbb{Z}[i] \to M$$

Where M is the set of matricies. In particular, I define

$$\phi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

And

$$M \equiv \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$$

is closed under multiplication and addition. It is easy to show that ϕ is a ring homomorphism. Furthermore, it is an isomorphism if we restrict M to just the form defined above.

4.2 The First Isomorphism Theorem

Let G and H be groups, and let $\phi : G \to H$ be a homomorphism.

1. The kernel of ϕ is a normal subgroup of G
2. The image of ϕ is a subgroup of H, and
3. The image of ϕ is isomorphic to the quotient group $G/\ker(\phi)$.
4. In particular, if ϕ is surjective then H is isomorphic to $G/\ker(\phi)$

4.3 Algebraic Numbers Over $\mathbb{Q}$

An algebraic number is a complex number which is a zero of a polynomial with integer coeficients. Morover, if the polynomial is “monic” (leading coeficient is 1), then this number is called an algebraic integer. The polynomial of minimal degree is called the “minimal polynomial” of the algebraic number.

For example, 5 is an algebriac number, and since it’s a zero of $x - 5$, it is an algebraic integer. Any integer is an algebraic integer having minimal polynomial of $1 \cdot x - n$. Another example is $1/2$ which is an algebraic number, but not an algebraic integer. i is an algebraic integer because it is a root of $x^2 + 1$. All gaussian intgers are algebraic integers. Yet another is $7^{1/3}$ which is a root of $x^3 - 7$. Finally, consider

$$\frac{-1 + \sqrt{-3}}{2}$$

which is a root of unity. It is a root of $x^3 - 1$, but this is not minimal. It can be factored into

$$(x - 1)(x^2 + x + 1)$$

and since $x \neq 1$, the minimal polynomial is

$$x^2 + x + 1$$

4.3.1 Checking Minimality

- If a polynomial of degree at most 3 has no rational zero, then its automatically irreducible (and thus minimal).

- Eisenstein's Irreducibility Criterion. If

  $$\exists \text{ prime } p$$

  which divides all coefficients but the leading coefficient, and p^2 does not divide the constant term, then the polynomial is irreducible.

  For example, $x^3 - 7$ can be shown to be minimal by using $p = 7$. Another example is

  $$x^4 + 4x^3 + 6x + 14$$

  We can use $p = 2$ to show that it is irreducible.

- Reduction mod p. If $p(x) \in \mathbb{Z}[x]$ is irreducible mod p for some prime p, then $p(x)$ is irreducible (over $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$). Consider

  $$x^4 + x^3 + 2 \mod 3$$

  0, 1, and 2 are not zeros, so it has no linear factors. The only other possibility is

  $$(x^2 + ax + b)(x^2 + cx + d)$$

  Which yields

  $$a + c = 1$$

  $$b + ac + d = 0$$

  $$ad + bc = 0$$

  $$bd = 2$$

  We have only 3 choices per variable. We can do detective work to reduce our search space. This might fail, because this may have factors, which me may have in this case. Verify in Matlab, but this seems to be factorizable, which tells us nothing. This was probably a bad choice of example. Other primes or other methods may do better.