Algebra

COURSE NOTES

Fall 2009, Math 145

Contents

Professor: A. Menezes

1. Commutative Rings and Fields

1.1. **Characteristics of commutative rings.**

A commutative ring, denoted by $(R, +, \cdot)$ consists of a set R and two binary operations.

The characteristics of a commutative ring are:

i. Addition and multiplication are commutative and associative.
ii. There exists additive and multiplicative identities.
iii. There exists an additive inverse.
iv. The distributive law holds.

A commutative ring is a field if $1 \neq 0$ and multiplicative inverses exist.

1.2. **The integers.**

The properties of divisibility for the integers, for $a, b, c \in \mathbb{Z}$, are:

i. If $a|b$ and $b|c$ then $a|c$
ii. If $a|b$ and $a|c$ then $a|bx + cy$ for all $x, y \in \mathbb{Z}$
iii. If $a|b$ and $b|a$ then $a = \pm b$
iv. If $a|b$ and $a, b \in \mathbb{N}$ then $b \geqslant a$

Let $a, b, x \in \mathbb{N}$ with $x \geqslant 2$.
Then $x^a - 1 | x^b - 1$ if and only if $a|b$

Let $a, b, x \in \mathbb{N}$ with $x \geqslant 2$.
Then $gcd(x^a - 1, x^b - 1) = x^{gcd(a,b)} - 1$

2. The Fundamental Theorem of Arithmetic

2.1. **Greatest Common Divisor properties.**

Let $a, b, q, r \in \mathbb{Z}$ with $b = qa + r$
Then $gcd(a, b) = gcd(a, r)$

By the GCD characterization theorem, if $a, b \in \mathbb{Z}$ then $d = gcd(a, b)$ if and only if

i. $d \geqslant 0$
ii $d|a$ and $d|b$
iii. There exist $x, y \in \mathbb{Z}$ such that $ax + by = d$
iv. If $c|a$ and $c|b$ then $c|d$

2.2. **Linear Diophantine equations.**

Let $a, b, c \in \mathbb{Z}$
Then $ax + by = c$ has an integer solution if and only if $gcd(a, b)|c$

Let $a, b \in \mathbb{Z}$, not both zero.
Then $gcd(a, b)$ is the smallest positive integer d for which $ax + by = d$ has a solution

Let $a, b, c, \in \mathbb{Z}$ with $a|b$, not both zero.
Let $d = gcd(a, b)$ and suppose that $d|c$
Then, given that a particular solution to the Diophantine equation $ax + by = c$ is (x_o, y_o), the complete integer solution to this equation is given by:
$x = x_o + \frac{b}{d}k \quad , \quad y = y_o - \frac{a}{d}k \quad , \quad k \in \mathbb{Z}$

2.3. **The Fundamental Theorem of Arithmetic.**
An integer $p \geqslant 2$ is prime if its only positive divisors are 1 and p. Otherwise p is composite.

If $a, b \in \mathbb{Z}$ and p is prime and $p|ab$, then $p|a$ or $p|b$.

Every integer $n \geqslant 2$ can be expressed as the product of primes. This is termed the prime factorization of n. Moreover, this expression is unique up to rearrangement of prime factors.

Let $n, k \in \mathbb{Z}$
Then $\sqrt[k]{n}$ is either an integer or an irrational.

If $a, b \in \mathbb{Z}$ with $gcd(a, b) = 1$, then there are infinitely many primes of the form $an + b$.

3. Congruences

3.1. **Properties of congruences.**
Let $n \in \mathbb{N}$ be fixed and let $a, b \in \mathbb{Z}$
If $n|(a - b)$, then a and b are congruent modulo n, and we write $a \equiv b \pmod{n}$

Let $n \in \mathbb{N}$ be fixed and let $a, b, c, a', b' \in \mathbb{Z}$
i. $a \equiv a \pmod{n}$ [Reflexivity]
ii. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ [Symmetry]
iii. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ [Transistivity]
If $a \equiv b \pmod{n}$ and $a' \equiv b' \pmod{n}$, then
iv. $a + a' \equiv b + b' \pmod{n}$
v. $aa' \equiv bb' \pmod{n}$
vi. $a - a' \equiv b - b' \pmod{n}$
vii. If $k \in \mathbb{N}$, then $a^k \equiv b^k \pmod{n}$

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then a is congruent modulo n to exactly one of $x \in [1, n - 1]$.

The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a, n)|b$

The following are equivalent:

i. $a \equiv b \pmod{n}$
ii. $n|(a-b)$
iii. $a = b + kn$ for some $k \in \mathbb{Z}$
iv. a, b leave the same remainder upon division by n
v. $[a] = [b]$ in $\mathbb{Z}_n$

3.2. **Equivalence relations.**

A relation on a set S is a subset $R \subseteq S \times S$
For $a, b \in S$ we write aRb if $(a, b) \in R$.

A relation R on S is an equivalence relation if for all $a, b, c \in S$

i. aRa (Reflexivity)
ii. $aRb \Rightarrow bRa$ (Symmetry)
iii. $aRb \wedge bRc \Rightarrow aRc$ (Transistivity)

Let R be an equivalence relation on S and let $a \in S$. Then the equivalence class of a is $[a] = \{x \in S : xRa\}$, where a is called the representative of $[a]$.

Let R be an equivalence relation on S. Then

i. $a \in [a]$ for all $a \in S$
ii. If $\neg(aRb)$, then $[a] \cap [b] = \emptyset$
iii. $[a] = [b]$ if and only if aRb

Equivalence classes are either equal or completely disjoint.

3.3. **Least Common Multiple.**

Let $a, b \in \mathbb{N}$
Then $\operatorname{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$

3.4. **The integers modulo n.**

The equivalence classes of the relation "congruence mod n" are called "congruence classes mod n". The integers mod n ($\mathbb{Z}_n$) is the set of all congruence classes mod n.

Let $n \geqslant 2$. Then $\mathbb{Z}_n$ is a finite commutative ring.
Additive identity: $[0]$
Multiplicative identity: $[1]$
Additive inverse: $[a] + [-a] = 0$

If p is prime, then $\mathbb{Z}_p$ is a finite field. The converse also holds.

3.5. **Fermat's Little Theorem.**
Let p be prime, and let a be any integer with $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod p$

If p is prime and $a \in \mathbb{Z}$ with $p \nmid a$, and $k \in \mathbb{Z}$, then $a^k \equiv a^{k \pmod{p-1}} \pmod p$

3.6. **Chinese Remainder Theorem.**
Let $m_1, m_2, m_3 \dots m_k$ be pairwise relatively prime natural numbers, and $a_1, a_2, a_3 \dots a_k \in \mathbb{Z}$
Then the set of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $m_1 \cdot m_2 \cdot m_3 \dots m_k$

Let $n \in \mathbb{N}_{\geqslant 2}$ and $a \in \mathbb{Z}_n$
Then $[a]^{-1}$ exists in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$

4. Cryptography

4.1. **Background.**
The bit length of $n \in \mathbb{R}$ is $\lfloor \log_2 n \rfloor + 1$

Let f and g be functions such that $f, g : \mathbb{N} \to \mathbb{R}_{>0}$
Then $f(n) = O(g(n))$ if there exists $c > 0$ and $n_o \in \mathbb{Z}$ such that $f(n) \leqslant c \cdot g(n)\ \forall\ n \geqslant n_o$

Let a, b be $k-$bit numbers. Then we have the following running time for algorithms:

Operation	Running time
$a + b, a - b$	$O(k)$ bit operations
$a \cdot b$	$O(k^2)$ bit operations
$a = bq + r$	$O(k^2)$ bit operations
$\gcd(a, b)$	$O(k^2)$ bit operations (by EEA)

4.2. **Primality testing.**

Wilson's Theorem.
Let $n \in \mathbb{N}_{\geqslant 2}$
Then p is prime if and only if $(p-1)! \equiv -1 \pmod p$

Fermat's test.

Repeat the following ℓ times:

1. Select a at random in $[1, n-1]$
2. Compute $t = a^{n-1} \mod n$
3. If $t \neq 1$ then output "n is COMPOSITE" and STOP

Output "n is PROBABLY PRIME"

The worst-case running time for Fermat's test is $O(k^2)$ bit operations.

Define $\mathbb{Z}_n^* = \{a : 1 \leqslant a \leqslant n-1 \ , \ \gcd(a,n) = 1\}$
$= \{a : a^{-1} \mod n \text{ exists } \}$

Let n be composite.
Suppose there exists at least 1 Fermat witness, $b \in \mathbb{Z}_n^*$ for n
Then at least half of all $n \in \mathbb{Z}_n^*$ are also Fermat witnesses for n

Let n be odd and composite.
Then n is a Carmichael number if $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \mathbb{Z}_n^*$

Miller-Rabin test.

Write $n-1$ as $2^s \cdot d$ by factoring powers of 2 from $n-1$.
Repeat the following ℓ times:

1. Select a at random in $[1, n-1]$
2. If $\gcd(a,n) > 1$ then output "n is COMPOSITE" and STOP
3. Compute $t = a^{n-1} \mod n$. If $t = 1$ or $t = n-1$ then go to the next iteration.
4. For j from 0 to $s-1$ do:
  i. Compute $t = a^{2^j d} \mod n$
  ii. If $t = n-1$ then go to next iteration
5. Output "n is COMPOSITE" and STOP

Output "n is PROBABLY PRIME"

The worst-case running time for the Miller-Rabin test is $O(k(\log n)^3)$ bit operations.

Agrawal-Kayal-Saxena test.

Let $n, a \in \mathbb{Z}$ with $n \geqslant 2$ and $\gcd(a,n) = 1$
Then n is prime if and only if $(x+a)^n \equiv x^n + a^n \pmod{n}$
$\equiv x^n + a \pmod{n}$
where x is indeterminate.

4.3. **RSA public-key encryption scheme.**

Used so that two parties can engage in confidential communications over an unsecured channel, having never before used a secure channel.

Created by Ron Rivest, Adi Shamir and Leonard Adleman in 1976.

Key generation works when each user, A and B, does the following:
1. Randomly select two large distinct primes p and q.
2. Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$
3. Select an arbitrary $e, 1 < e < \phi(n)$ such that $\gcd(e, \phi(n)) = 1$
4. Compute $d, 1 < d < \phi(n)$ such that $ed \equiv 1 \pmod{\phi(n)}$
Then the public key of A is (n, e) while the private key of A is d.

To *encrypt* a message m for Bob, Alice does the following:
1. Obtains an authenticated copy of Bob's public key.
2. Represents m as an integer in $[0, n-1]$
3. Computes $c \equiv m^e \pmod{n}$
4. Sends c to Bob.

To *decrypt* a message m from Alice, Bob does the following:
1. Computes $r \equiv c^d \pmod{n}$. Then $r = m$.

To ensure that Alice has an *authenticated* public key, the following happens:
1. Bob obtains a "certificate" from VeriSign.
2. Bob sends Alice the certificate.
3. Alice verifies VeriSign's signature, and then is assured she has Bob's public key.
4. Alice can encrypt any message m to Bob, and only he can decrypt it.

5. Quadratic Number Domains

5.1. **Background.**
Let $d \neq 1$ be a square free integer. Then
$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$
$$\mathbb{Z}[\sqrt{d}\,] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

Properties of $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Z}[\sqrt{d}\,]$:
i. $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d}\,]$ and $\mathbb{Q}, \mathbb{Z}[\sqrt{d}\,] \subseteq \mathbb{Q}(\sqrt{d})$
ii. If $r_1 + s_1\sqrt{d}, r_2 + s_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$,
then $r_1 + s_1\sqrt{d} = r_2 + s_2\sqrt{d}$ if and only if $r_1 = r_2$ and $s_1 = s_2$.
iii. If $d > 0$, then $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R} \subseteq \mathbb{C}$
iv. If $d < 0$, then $\mathbb{Q}(\sqrt{d}) \nsubseteq \mathbb{R}$, but $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$

$\mathbb{Q}(\sqrt{d})$ is a field.

$\mathbb{Z}[\sqrt{d}\,]$ is a commutative ring.

Let $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$.
Then $a + b\sqrt{d}$ is a unit if there exists $x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$ such that $(a + b\sqrt{d})(x + y\sqrt{d}) = 1$.

Let $x = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.
Then the conjugate of x is $\widetilde{x} = r - s\sqrt{d}$
Then the norm of x is $N(x) = x\widetilde{x}$.

Properties of the norm:
i. $N(x) = 0 \iff x = 0$
ii. $\widetilde{(x + y)} = \widetilde{x} + \widetilde{y}$
iii. $\widetilde{(xy)} = \widetilde{x} \cdot \widetilde{y}$
iv. $N(xy) = N(x)N(y)$

Let $x \in \mathbb{Z}[\sqrt{d}\,]$. Then
i. $N(x) \in \mathbb{Z}$
ii. x is a unit if and only if $N(x) = \pm 1$

A commutative ring R is an *integral domain* if
i. $1 \neq 0$
ii. $ab = 0$, with $a, b \in R$, implies $a = 0$ or $b = 0$.

5.2. **Prime Factorization in $\mathbb{Z}[\sqrt{d}\,]$.**

Every nonzero $x \in \mathbb{Z}[\sqrt{d}\,]$ can be expressed as the product of a unit and finitely many primes.

If $d \equiv 1 \pmod 4$, then $\mathbb{Z}[\sqrt{d}\,]$ is not a unique factorization domain (UFD).
If $d < 0$, then $\mathbb{Z}[\sqrt{d}\,]$ is a unique factorization domain only if $d = -1$ or $d = -2$.
If $d > 0$ and $d \not\equiv 1 \pmod 4$, $\mathbb{Z}[\sqrt{d}\,]$ is a UFD for (at least) $d = \{2, 3, 6, 7, 11, 14, 19, 22, 23, 31 \ldots\}$.

Let $x, y \in \mathbb{Z}[\sqrt{d}\,]$. Then $x|y$ if $y = xz$ for some $z \in \mathbb{Z}[\sqrt{d}\,]$

An element $x \in \mathbb{Z}[\sqrt{d}\,]$ is prime if
i. x is not a unit
ii. If $x = yz$ for $y, z \in \mathbb{Z}[\sqrt{d}\,]$, then either y or z is a unit.

Let $x \in \mathbb{Z}[\sqrt{d}\,]$.
If $|N(x)|$ is prime, then x is prime.
Note that the converse is not true in general.

Let $x, y \in \mathbb{Z}[\sqrt{d}\,]$.
Then x is an associate of y if $x = yu$ for some unit $u \in \mathbb{Z}[\sqrt{d}\,]$.

Properties of the associate:

i. The relation "x is an associate of y" is an equivalence relation of $\mathbb{Z}[\sqrt{d}\,]$
ii. If x and y are associates, then $N(x) = \pm N(y)$
iii. If $x|z$, then $y|z$ for all associates y of x.
iv. If $p \in \mathbb{Z}[\sqrt{d}\,]$ is prime and $u \in \mathbb{Z}[\sqrt{d}\,]$ is a unit, then pu is prime.

5.3. **Gaussian Integers.**

The Gaussian integers are a quadratic number domain with $d = -1$

· $\mathbb{Z}[i] = \{x + yi \,|\, x, y \in \mathbb{Z}\}$
· $N(x + yi) = x^2 + y^2 \geqslant 0$
· Units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$

By convention, $\gcd(a, b)$ for $a, b \in \mathbb{Z}[i]$ must have an argument in the first quadrant.

If $p \equiv 3 \pmod 4$ is an integer prime, then it is also a Gaussian prime.

If $p \equiv 1 \pmod 4$ then there exists a unique expression $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$.

The Gaussian primes are:

i. $1 + i$
ii. $p \in \mathbb{Z}$ such that p is prime, $p \equiv 3 \pmod 4$
iii. $a \pm bi$, where $a^2 + b^2 = p$ for p prime and $p \equiv 3 \pmod 4$.

6. Polynomial Rings

6.1. **Background.**

Let R be a commutative ring. Then a polynomial in x over R is an expression

$f(x) = a_d x^d + \ldots a_2 x^2 + a_1 x + a_0 \qquad \text{where } d \geqslant 0 \text{ and } a_i \in R$

The set of all such polynomials is denoted by $R[x]$
If the leading coefficient is 1, then f is said to be *monic.*

The degree of $f \in R[x]$, denoted by $deg(f)$, is the highest power of any variable in f.
The degree of the zero polynomial is $-\infty$
If f, g are polynomials in $R[x]$, then $deg(f + g) \leqslant max\{deg(f), deg(g)\}$

Associations between polynomial rings and other domains:

i. If R is a commutative ring, then $R[x]$ is a commutative ring.
ii. If R is an integral domain, then $R[x]$ is an integral domain.
iii. If F is a field, then then only invertible elements in $F[x]$ are are the constant polynomials (for which the degree is 0), denoted by F^*

6.2. **Polynomial factorization.**

Note that $\mathbb{Z}[x]$ has no division algorithm.

If d is a gcd of $f, g \in F[x]$, then d must be monic.
Also the gcd of any two polynomials is unique.

Let $p \in F[x]$. Then p is irreducible over F if
i. $deg(p) \geqslant 1$
ii. p cannot be expressed as $p = fg$ where $f, g \in F[x]$, with $1 \leqslant deg(f), deg(g) < deg(p)$

The factor theorem states that:
i. $(x-a)|f(x)$ if and only if $f(a) = 0$
ii. $a \in F$ is a root of $f \in F[x]$ if $f(a) = 0$

Let F be a field. Then $F[x]$ is a UFD. More precisely, every nonzero polynomial $f \in F[x]$ has a unique factorization $f = ap_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$ where p_i's are distinct monic irreducible polynomials in $F[x]$, and a is some nonzero constant in F, and $e_i \in \mathbb{N}$.

If $f \in F[x]$ is of degree $n \neq 0$, then f has at most n roots in F.

6.3. **Polynomial congruences.**

The basic properties of congruences over polynomial fields are:
i. Congruence modulo f is an equivalence relation on F.
ii. The equivalence class of $g \in F[x]$ is denoted by $\{h \in F[x] : h \equiv g \pmod{f}\}$.
iii. The set of all equivalence classes is denoted by $F[x]/(f)$.
iv. Addition and multiplication in $F[x]/(f)$ is denoted in the usual way.

$F[x]/(f)$ is a commutative ring.
If $f \in F[x]$, $deg(f) \geqslant 1$, is irreducible over F, then $F[x]/(f)$ is a field; the converse also holds.

6.4. **Galois Fields.**
The *order* of a finite field is the number of elements in the field.

Let F be a finite field of order q. Let $f \in F[x]$ of degree $n \geqslant 1$ be irreducible over F. Then $F[x]/(f)$ is a finite field of order q^n .

Two fields F_1 and F_2 are isomorphic if there exists a bijection $\phi : F_1 \to F_2$ such that $\underbrace{\phi(\alpha+\beta)}_{\text{addition in } F_1} = \underbrace{\phi(\alpha)+\phi(\beta)}_{\text{addition in } F_2}$ for all $\alpha, \beta \in F_1$. Similarly, $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$.
Any two fields of the same order are isomorphic.

The finite field of order q is denoted by $GF(q)$, where GF indicates a Galois Field.

Fermat's Little Theorem for finite fields.

Let F be any finite field of order q.
Then when α is a nonzero element in F, $\alpha^{q-1} \equiv 1 \pmod q$ for all $q \in F^* = F \setminus \{0\}$.

Corollary:
$\alpha^q = \alpha$ for all $\alpha \in F$

Corollary:
In $F[x]$, $x^q - x = \displaystyle\prod_{\alpha \in F} (x - \alpha)$

Let F be a field.
Then the *characteristic* of F is denoted by $m = char(F)$, such that m is the smallest positive integer such that $\underbrace{1 + 1 + 1 + \cdots + 1}_{\text{m}} = 0$. If no such m exists, we define $char(F) = 0$.

If $char(F) = 0$, then F is an infinite field.

Let F be a finite field with $char(F) = m$. Then m is prime.

If F is an infinite field with $char(F) = m \neq 0$, then m is prime.

Freshman's Dream.

If F is a field with $char(F) = p$, then $(\alpha + \ \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ for all $\alpha, \beta \in F$ and $n \geqslant 1$.

Every finite field F with $char(F) = p$ has $\mathbb{Z}_p$ as a subfield.

Vector space corollaries for finite fields.

Every finite field has p^n elements, where p is the (prime) characteristic of the field, and $n \geqslant 1$.

If F is a finite field of order q, where q is a prime power, and $n \geqslant 2$, there exists a finite field of order q^n.
Hence if p is prime and $n \geqslant 1$, then there exists a finite field of order q^n.

6.5. **Irreducible polynomials over $\mathbb{Q}$.**

It is much easier to determine if polynomials with integer coefficients are irreducible, so we have to devise a way to convert polynomials in $\mathbb{Q}$ to polynomials in $\mathbb{Z}$.

There exists an efficient (polynomial time) algorithm for deciding whether $f \in \mathbb{Q}[x]$ is irreducible.

An efficient (polynomial time) deterministic algorithm for deciding irreducibility of $f \in \mathbb{Z}_p[x]$ is not known.

Gauss's Lemma.

Let $f(x)$ be a polynomial such that $f \in \mathbb{Q}$.
Let λ be the lcm of all denominators of the nonzero coefficients of f.
Then let $\widetilde{f}(x) = \lambda f(x)$
Gauss's Lemma states that $\widetilde{f}$ is irreducible over $\mathbb{Q}$ if and only if $\widetilde{f}$ is irreducible over $\mathbb{Z}$.

Rational Root Theorem.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} \dots a_1 x + a_0 \in \mathbb{Z}[x]$ such that $deg(f) = n \geqslant 1$
Then if $c = \frac{s}{t}$, where $s, t \in \mathbb{Z}, t > 0, s \neq 0, \gcd(t, s) = 1$ is a root of f, then $s|a_0$ and $t|a_n$.

Eisenstein's Criterion.

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, with $deg(f) = n$.
Suppose p is prime such that:

i. $p|a_i$ such that $0 \leqslant i \leqslant n-1$
ii. $p \nmid a_n$
iii. $p^2 \nmid a_0$

Then f is irreducible over $\mathbb{Q}$.

Factoring modulo primes.

Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime.
Let $\bar{f}(x) \in \mathbb{Z}[x]$ be obtained from f by reducing it coefficients modulo p.
Then if $\bar{f}$ is irreducible over $\mathbb{Z}_p$, then f is irreducible over $\mathbb{Q}$.

Number domains.