Lecture Notes for Math 627B
Modern Algebra
Foundational Material

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
wwww-rohan.sdsu.edu/ ˜ mosulliv

September 1, 2011

1 Rings and Fields

A *ring* is a set R with two operations $+, *$ satisfying the following properties:

1. $+$ and $*$ are both associative. That is $(a + b) + c = a + (b + c)$ and $a * (b * c) = (a * b) * c$.

2. $+$ and $*$ are both commutative. That is $a+b = b+a$ and $a*b = b*a$.

3. $+$ and $*$ both have identity elements. There is some element in R, that we call 0, such that $a + 0 = a$ and there is an element, that we call 1, such that $a * 1 = a$.

4. $+$ admits inverses. That is, for each $a \in R$ there is some other element, that we write $-a$, such that $a + (-a) = 0$.

5. $*$ distributes over $+$. That is $a * (b + c) = a * b + a * c$.

A few comments are in order. Strictly speaking, the definition above is for a *commutative ring with identity.* The modifier "commutative" is referring to commutativity of multiplication, and "with identity" is referring to the multiplicative identity. There is a rich study of rings where multiplication is non-commutative (for example the ring of $n \times n$ matrices over $\mathbb{R}$), but we will rarely discuss them, so a ring for us is assumed to be commutative and have an identity.

There are a bunch of little results one should verify: each identity is unique, the additive inverse of an element is unique, $-(a+b) = (-a)+(-b)$, etc. See §3.1-2 of [1].

Let R, S be rings. A funtion $\phi : R \longrightarrow S$ is a *ring homomorphism* when

1. $\phi(r + s) = \phi(r) + \phi(s)$
2. $\phi(r * s) = \phi(r) * \phi(s)$
3. $\phi(1_R) = 1_S$

Notice that the operations $+$, $*$ on the left-hand side are in R and the operations $+, *$ on the right-hand side are in S. If we want to be careful we specify the ring: we write $+_S$ for the addition in S. We say ϕ *respects addition, multiplication and the identity element.* That is, it respects the ring structure. There are a several little results to establish for homomorphisms: e.g. $\phi(-s) = -\phi(s)$. See [1, §3.3].

The following theorem shows that the Integers are the "original ring."

Theorem 1.1 (The Initial Ring)**.** *For any ring R there is a unique homomorphism from $\mathbb{Z}$ to R.*

Proof. A homomorphism $\phi : \mathbb{Z} \longrightarrow R$ would have to take $1_\mathbb{Z}$ to 1_R. Applying the fact that a homomorphism has to respect addition we see inductively that we must have for $m > 0$,

$$\phi(m) = \phi(\underbrace{1_\mathbb{Z} + \cdots + 1_\mathbb{Z}}_{m \text{ terms}}) = \underbrace{1_R + \cdots + 1_R}_{m \text{ terms}}$$

We also must have $\phi(-m) = -\phi(m)$. Thus, there is at most one way to define a homomorphism from $\mathbb{Z}$ to R. Next, check that this function is indeed a homomorphism by verifying that the other properties of homomorphisms hold. □

The *kernel of a homomorphism* $\phi : R \longrightarrow S$ is the preimage of 0_S: that is $\{r \in R : \phi(r) = 0_S\}$. It is an exercise to show that ϕ is injective (one-to-one) iff the kernel is trivial (just 0_R). A homomorphism that is also a bijection (injective and surjective) is called an *isomorphism.*

We say $a \in R$ is a *zero-divisor* when $a \neq 0$ and there is some nonzero $b \in R$ such that $a * b = 0$. We say a is a *unit* when there is some $b \in R$ such that $ab = 1$. An *integral domain* is a ring that has no zero-divisors. The integers is an integral domain. A *field* is a ring in which every nonzero element is a unit. The rational numbers form a field, $\mathbb{Q}$, as do the real numbers, $\mathbb{R}$, and the complex numbers, $\mathbb{C}$.

2 The Integers

There are five main results for the integers that you should know. I will call them the Division Theorem, the GCD Theorem, The Euclidean Algorithm, the Prime-Irreducible Theorem, and the Unique Factorization Theorem.

Theorem 2.1 (Division). *Let a and b be integers with $b > 0$. There exist unique integers q, r such that*

1. $a = bq + r$, *and*
2. $0 \leq r < b$

It is fairly common in programming languages (in particular in Python and Sage) to write the integer quotient as $a//b$ and the remainder as $a\%b$. We will use this notation as needed.

Let a and b be integers. The *common divisors* of a and b are the integers that divide both a and b. The *greatest common divisor* (gcd) is the largest positive integer dividing both a and b. The *common multiples* of a and b are the integers that are multiples of both a and b. The *least common multiple* (lcm) is the smallest positive integer that is a multiple of both.

A *linear combination* of a and b is an integer that can be expressed as $au + bv$ for some integers u and v.

Theorem 2.2 (GCD). *Let a and b be integers, at least one of them nonzero. The gcd of a and b is the smallest positive linear combination of a and b. In particular,* $\gcd(a, b) = au + bv$ *for some integers u and v.*

The set of all linear combinations of a and b equals the set of multiples of $\gcd(a, b)$*.*

We say two integers are *coprime* (or *relatively prime*) when their gcd is 1.

Given a and b, how do we find their gcd? The answer (for arbitrary large integers) is not to factor each and look for common factors. Rather, use the Euclidean algorithm.

Let $r_{-1} = a$ and $r_0 = b$, and define inductively (while $r_k \neq 0$)

$$\begin{aligned} q_k &= r_{k-1}//r_k \\ r_{k+1} &= r_{k-1}\%r_k, \qquad \text{so that} \\ r_{k+1} &= r_{k-1} - q_k r_k \end{aligned}$$

The r_k are a strictly decreasing sequence of nonnegative integers, so the process must terminate; for some n, $r_{n+1} = 0$. There is a lemma that says:

For integers a, b, c, x such that $a = bx + c$, we have $\gcd(a, b) = \gcd(b, c)$. Let's apply this to the result to the sequence r_k, letting n be minimal such that $r_{n+1} = 0$. We have (since $r_{n+1} = 0$)

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_n, r_{n+1}) = r_n$$

This argument shows that the Euclidean algorithm produces the gcd of a and b. In the following Sage code we only keep two of the remainders at any time, not the whole sequence: after the kth pass through the while loop, r in the algorithm is r_{k-1} and s is r_k.

```
def euclid_alg(a,b):
   if b == 0:
      print "division by zero"
      return false
   else:
      r = a
      s = b
      while s != 0:
         rem =  r %s
         r = s
         s = rem
      return r
```

There is a heftier Euclidean algorithm–often called the Extended Euclidean algorithm–which produces two integers u, v such that $au + bv = \gcd(a, b)$. I like the following matrix version of the algorithm. Let $Q_k = \begin{bmatrix} -q_k & 1 \\ 1 & 0 \end{bmatrix}$ and $R_k = \begin{bmatrix} r_k \\ r_{k-1} \end{bmatrix}$ Where the sequence r_k and q_k are the same as used above in the Euclidean algorithm. Verify that $R_{k+1} = Q_k R_k$. Consequently,

$$R_{n+1} = \begin{bmatrix} 0 \\ r_n \end{bmatrix} = Q_n Q_{n-1} \cdots Q_0 R_0$$

where $R_0 = \begin{bmatrix} b \\ a \end{bmatrix}$. Let $M = Q_n Q_{n-1} \cdots Q_0$. Then we have $M_{2,1} b + M_{2,2} a = r_n = \gcd(a, b)$.

By the way, you can use the following equation, along with a few observations about the Fibonacci numbers to bound the number of steps for the Euclidean algorithm. Ask me, or see [2] for details.

$$\begin{bmatrix} b \\ a \end{bmatrix} = Q_0^{-1} Q_1^{-1} \cdots Q_n^{-1} = \begin{bmatrix} 0 \\ r_n \end{bmatrix}$$

Theorem 2.3 (Euclidean Algorithm). *Let a, b be integers with $b \neq 0$. The Euclidean Algorithm outputs* $\gcd(a,b)$ *in at most* $1+\log_2 b/\log\alpha$ *steps, where α is the golden ratio. The Extended Euclidean Algorithm outputs integers u, v with $|u| < b$ and $|v| < a$ such that $au + bv = \gcd(a,b)$.*

Here is the Sage code for the extended Euclidean algorithm.

```
def ext_euclid_alg(f,h):
   if h == 0:
      print "division by zero"
      return false
   else:
      M = matrix(2, 3, [f,  1, 0, h, 0, 1])
      s = M[0,0]
      r = M[1,0]
      while s != 0:
         q =  r // s
         M  = matrix(2,2,[ -q , 1, 1, 0]) * M
         s = M[0,0]
         r = M[1,0]
      return M
```

Let r be a nonzero integer. We say r is *irreducible* when $r = ab$ implies that either $a = \pm 1$ or $b = \pm 1$. We say r is *prime* when $r|ab$ implies $r|a$ or $r|b$. The definition of irreducible is what we customarily use for primality, but the definitions given here are the accepted ones in more general contexts. Fortunately, we have the following theorem!

Theorem 2.4 (Prime-Irreducible). *A nonzero integer is irreducible iff it is prime.*

The previous theorem is the key ingredient to establishing unique factorization.

Theorem 2.5 (Unique Factorization). *Let a be a nonzero integer. There is a nonnegative integer t, positive prime numbers $p_1, \ldots, p_t$, and positive integers $e_1, \ldots e_t$ and choice of unit, $u = 1$ or -1, such that*

$$a = up_1^{e_1} \cdots p_t^{e_t}$$

Each of t, p_i, e_i and u is uniquely determined.

Here are some computational exercises that will help solidify your understanding of the properties of the integers, and give you some practice programming. Some questions are a bit open-ended, just use them to play around with the ideas.

1. Euclidean algorithm problems. Suppose a and b are fixed (for example $a = 12$ and $b = 7$).

   (a) Fix some $N > 0$ and make a list of the elements in the set $S = \{ax + by : x, y \in \{-N, \dots, N\}\}$. Explore how, as you increase N the set "fills in." How large does N need to be to guarantee that $\gcd(a, b) \in S$? What would the set be if we allowed x and y to vary over all integers?

   (b) Compare the speed of the Euclidean algorithm above with built-in function.

   (c) Amend our gcd funtion to tell how many divisions occurred.

   (d) How many steps does the Euclidean algorithm take in general? Do most a, b take roughly $\log(b)$ steps, or do most take many fewer steps?

   (e) For $t = 1, 2, 3, 4, 5$ find the smallest a, and the smallest b for that a such that the Euclidean algorithm requires t divisions.

2. Prime factorization.

   (a) The Prime Number Theorem states that the number of primes in the range $[2, n]$ is roughly $n/\ln(n)$. Check this result by sampling a lot of integers in the range $[2^k, 2^{k+1}]$ and checking for primality. What proportion should be prime?

   (b) How is the number of prime factors of an integer in $[2^k, 2^{k+1}]$ distributed. Do most integers have lots of factors, or relatively few?

3 Integers modulo n

Let n be an integer. Integers a and b are *congruent modulo n* when n divides $a - b$.

Theorem 3.1. *Congruence modulo n is an eqivalence relation. The set $\{0, 1, \dots, n-1\}$ is a system of representatives for congruence modulo n; each integer is congruent modulo n to exactly one element of $\{0, 1, \dots, n-1\}$.*

Two special cases are worth noting. When $n = 0$, a is congruent to b iff and only if $a = b$. When $n = 1$ (or $n = -1$), a is congruent to b for all integers a and b. The integers n and $-n$ give the same equivalence relation, so we always use positive integers for the modulus.

It is common to write $[a]_n$ for the congruence class of a modulo n, whenever we need to be careful to distinguish between the integer a and the congruence class, or when we have more than one modulus to worry about. Otherwise, if it is clear from context, we may simply write a.

Theorem 3.2 (Arithmetic mod n)**.** *Suppose that $a \equiv b \mod n$ and $r \equiv s \mod n$. Then $a + r \equiv b + s \mod n$ and $ar = bs \mod n$. Thus, arithmetic on congruence classes modulo n is well-defined.*

We will write $\mathbb{Z}/n$ for the set of equivalence classes modulo n, with the operations $+$ and $*$. (It is common to use $\mathbb{Z}_n$, but $\mathbb{Z}/n$ is consistent with notation we will use later.) Usually, we write the equivalence classes as $0, 1, \ldots, n-1$ (without the brackets and using the least nonnegative representatives for each class). But, sometimes it is handy to be a bit flexible. For example it is good to remember that $n - b$ is equal to $-b$ in $\mathbb{Z}/n$. So (in $\mathbb{Z}/n$)

$$b(n-1) = (-1)b = n - b$$

The theorem above also shows that the function taking $a \in \mathbb{Z}$ to $[a]_n \in \mathbb{Z}/n$ is a homomorphism. We actually defined addition and multiplication in $\mathbb{Z}/n$ so that this map is a homomorphism. If d divides m there is a well-defined function from $[a]_m$ to $[a]_d$. This is because $m|(b-a)$ implies $d|(b-a)$, so any two integers that are congruent modulo m are also congruent modulo d. On the other hand if $d \not| m$, there is no well-defined function from $\mathbb{Z}/m$ to $\mathbb{Z}/d$. Since the arithmetic on $\mathbb{Z}/m$ is "inherited" from $\mathbb{Z}$, we have:

Theorem 3.3 (Homomorphism mod m)**.** *There is a homomorphism from $\mathbb{Z}/m$ to $\mathbb{Z}/d$ iff $d|m$. The homomomorphism is unique (since it takes $[1]_m$ to $[1]_d$).*

For any two integers m, n we have a homomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m$ and $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/n$. This gives a homomorphism into the Cartesian product: $\mathbb{Z}/m \times \mathbb{Z}/n$. The CRT says this is an isomorphism when m, n are coprime. See [2][§4.3] or [1][§13.1]for a formula for computing the inverse isomorphism.

Theorem 3.4 (Chinese Remainder Theorem)**.** *Let m, n be coprime. There is an isomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$.*

Recall that $a \in \mathbb{Z}/n$ is a *zero-divisor* when $a \neq 0$ and there is some nonzero $b \in \mathbb{Z}/n$ such that $a * b = 0$ (in $\mathbb{Z}/n$). We also say a is a *unit* when there is some $b \in \mathbb{Z}/n$ such that $ab = 1$ (in $\mathbb{Z}/n$).

Theorem 3.5 (Units, Zero Divisors)**.** *Let $n > 2$ be an integer and let a be an integer.*

1. *$[a]_n$ is a unit iff $\gcd(a, n) = 1$.*
2. *$[a]_n$ is a zero divisor iff $1 < \gcd(a, n) < n$.*

In particular, an element of $\mathbb{Z}/n$ is either 0, a unit, or a zero-divisor (and these are mutually exclusive).

Corollary 3.6. *Let p be a prime number. Then $\mathbb{Z}/p$ is a field; every nonzero element has an inverse.*

When working modulo a prime we usually use the notation $\mathbb{F}_p$ instead of $\mathbb{Z}/p$ to emphasize that we have a field.

Here are some exercises to test your understanding. Doing some computations with Sage may give you some data to work with.

1. Compute $(n-1)! \mod n$ for $n < 100$. Explain the results (as well as you can).

2. An *idempotent* in a ring is an element a such that $a^2 = a$. Clearly, 0 and 1 are idempotents. There is a formula relating the number of idempotents in $\mathbb{Z}/n$ with the number of distinct prime factors that n has. See if you can find this formula. Try easy examples of n first.

3. You should be able to explain why this formula holds for $\mathbb{Z}/n$:

$$\#(\text{units}) + \#(\text{zero divisors}) + 1 = n$$

   Here is a sequence of problems about the number of zero divisors in $\mathbb{Z}/n$. You can get the number of units from the formula above.

   (a) Let $n = pq$ for distinct primes p and q. There is a formula using p and q that tells the number of zero divisors in $\mathbb{Z}/n$. Find it!

   (b) Can you extend to $n = pqr$ with p, q, r distinct primes? Can you extend to arbitrary square-free n?

   (c) Find a formula for the number of zero-divisors in $\mathbb{Z}/p^a$.

   (d) Find a formula for the number of zero-divisors in $\mathbb{Z}/p^a q^b$ for p, q distinct primes.

4. Solve the linear equations.

   (a) $3x + 7 \equiv 5 \mod 17$

   (b) $3x + 7 \equiv 5 \mod 15$

   (c) $3x + 7 \equiv 4 \mod 15$

5. Use the quadratic formula, or completing the square, to find solution(s) if they exist to

   (a) $2x^2 + 7x + 5 \equiv 0 \mod 17.$

   (b) $3x^2 + 16x + 4 \equiv 0 \mod 17$

   (c) $5x^2 + 7x + 14 \equiv 0 \mod 19$

6. Use Maple to find solutions if they exist to

   (a) $7x^4 + 3x^2 + x + 15 \equiv 0 \mod 17.$

   (b) $7x^4 + 2x^2 + x + 15 \equiv 0 \mod 19.$

7. Give an example of a quartic polynomial with three distinct roots modulo 17.

8. An element $a \in \mathbb{Z}/n$ is a square if there is some $b \in \mathbb{Z}/n$ such that $a^2 = b$. Find the number of squares in $\mathbb{Z}/p^n$ ($p = 2$ is a bit different from the others).

9. Find the kernel of the homomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$ when m and n are not coprime.

4 The Univariate Polynomial Ring over a Field

Let F be a field. By $F[x]$ we mean the polynomial ring in the indeterminate x. The key fact about polynomial rings is that all the theorems we discussed for integers hold for polynomial rings as well.

We can think of the polynomial ring as a vector space over F with an infinite basis $1, x, x^2, \ldots$, the additional multiplicative structure defined by $x^i * x^j = x^{i+j}$ and the properties of a ring (e.g. distributivity). Sometimes it is useful to write a polynomial $f(x) \in F[x]$ as a sum $f(x) = \sum_{i=0}^{\infty} f_i x^i$ with the understanding that only a finite number of the f_i are nonzero. Suppose $f(x) \neq 0$ and let d be the largest integer such that $f_d \neq 0$. We call d the *degree* of $f(x)$; $f_d x^d$ is the *leading term* of $f(x)$; x^d is the *leading monomial* of $f(x)$; and f_d is the *leading coefficient* of $f(x)$. If $f_d = 1$ we say $f(x)$ is *monic.* When $d = 0$ we say $f(x)$ is a *constant* polynomial.

It should be clear that $\mathbb{F}[x]$ has no zero-divisors, so it is an integral domain. The product of a polynomial of $f(x)$ of degree α and $g(x)$ of degree β has degree $\alpha + \beta$. In order for $f(x)$ to be a unit it must therefore have degree 0, so the units in $\mathbb{F}[x]$ are the constant polynomials.

Theorem 4.1 (Division)**.** *Let $f(x)$ and $h(x)$ be in $F[x]$ with $g(x) \neq 0$. There exist unique $q(x)$, $r(x)$ such that*

1. *$f(x) = h(x)q(x) + r(x)$, and*

2. $\deg r(x) < \deg h(x)$

We will sometimes omit the (x) to simplify notation. We will write the quotient as $f//h$ and the remainder as $f\%h$. This notation works in Sage for polynomials as well as integers.

The greatest common divisor of two integers was easy to define since the integers are well ordered. It is not obvious that, among the common divisors of $f, h \in F[x]$, there is just one of maximal degree. The following theorem shows the gcd can be uniquely defined, and extends the GCD Theorem to polynomials. A *polynomial combination* of f and h is a polynomial that can be expressed as $fu + hv$ for some $u, v \in F[x]$.

Theorem 4.2 (GCD)**.** *Let $f, h \in F[x]$ with at least one of them nonzero. There is a unique polynomial d satisfying*

1. *d is a common divisor of f and h,*

2. *d is monic,*

3. *d has maximal degree among common divisors of f and h.*

Furthermore, there exist $u, v \in F[x]$ such that $d = fu + hv$. The set of all polynomial combinations of f and h equals the set of multiples of d.

The proof of the theorem can be adapted for any set of polynomials $S \subseteq F[x]$. We may look at the largest degree monic polynomial that divides all the elements of S. You can show that it is also the smallest degree monic polynomial that can be expressed as a combination of the elements of S.

The discussion of the Euclidian algorithm for integers carries over almost verbatim (just think of a and b as polynomials). The r_k are strictly decreasing in degree, so we must eventually get the 0 polynomial. The algorithm takes at most deg(b) steps. The Sage code appearing earlier needs no modification to be used with polynomials.

Let $f \in F[x]$ have degree at least one. As with integers, we say f is *irreducible* when it can't be factored in a nontrivial way: whenever $f = ab$ either $a \in F$ or $b \in F$. We say f is *prime* when $f|ab$ implies $f|a$ or $f|b$. As with integers, we have the equivalence of primality and irreducibility, which is a key step towards proving unique factorization.

Theorem 4.3 (Prime-Irreducible)**.** *Any nonconstant element of $F[x]$ is irreducible iff it is prime.*

Theorem 4.4 (Unique Factorization)**.** *Let $f(x) \in F[x]$ be nonzero. There is a nonnegative integer t, a constant $u \in F$, monic irreducible polynomials $p_1(x), \ldots, p_t(x)$, and positive integers $e_1, \ldots e_t$ such that*

$$f(x) = up_1(x)^{e_1} \cdots p_t(x)^{e_t}$$

Each of t, p_i, e_i and u is uniquely determined.

The polynomial ring has additional properties that make it easier to work with than the integers. Each $f(x) \in F[x]$ defines a function from F to F, which we call *evaluating* f. The function is $c \longmapsto f(c) = f_0 + f_1c + f_2c^2 + \cdots + f_dc^d$ where $d = \deg(f(x))$. When $f(c) = 0$ we say that c is a *root of* $f(x)$.

Let me turn things around now. Fix $c \in F$ and consider the function $\mathrm{ev}_c : F[x] \longrightarrow F$ defined by $f(x) \longrightarrow f(c)$. Show that this function is a homomorphism. Show furthermore that the remainder $f \,\%\, (x - c) = f(c)$.

Theorem 4.5. *Let $f(x) \in F[x]$. Any $c \in F$ is a root of $f(x)$ iff $f(c) = 0$. Consequently, a polynomial of degree d can have at most d roots.*

The computational exercises for the integers have analogues for $F[x]$.

1. Euclidean algorithm problems. Suppose f and h are fixed.
   (a) Fix some $d > 0$ and make a list of the elements in the set $S = \{fu + hv : u, v \in F[x], \deg(u), \deg(v) \leq d\}$. Explore how, as you increase d the set "fills in." How large does d need to be to guarantee that $\gcd(f, h) \in S$? What would the set be if we allowed u and v to vary over all $F[x]$?
   (b) Compare the speed of the Euclidean algorithm above with built-in function.

    (c) Amend our gcd funtion to tell how many divisions occurred.

    (d) How many steps does the Euclidean algorithm take in general? Do most f, h take roughly $\deg(h)$ steps, or do most take many fewer steps?

2. Factorization of polynomials.

    (a) What proportion of the polynomials of degree d are irreducible? Test this first for polynomials over $\mathbb{F}_p$ for p prime. You can do an exhaustive search. For $\mathbb{Q}[x]$, you can sample the coefficients integer $d+1$ integer coefficients from some range (say $[-N..N]$). This, at least, gives some idea.

    (b) How is the number of factors of a polynomial of degree d distributed?

5 Polynomial modulus

We now extend the notion of modular arithmetic to the polynomial ring over a field.

Let $m(x) \in F[x]$ have degree d. Polynomials $f(x)$ and $h(x)$ are *congruent modulo* $m(x)$ when $m(x)$ divides $f(x) - h(x)$.

Theorem 5.1. *Congruence modulo $m(x)$ is an eqivalence relation. The set of polynomials of degree less than $d = \deg(m(x))$ is a system of representatives for congruence modulo $m(x)$. That is, each polynomial is congruent modulo $m(x)$ to its remainder when divided by $m(x)$, which has degree less than d.*

Two special cases are worth noting. When $m(x) = 0$, $f(x)$ is congruent to $h(x)$ iff and only if $f(x) = h(x)$. When $m(x)$ is a constant, $f(x)$ is congruent to $h(x)$ for all $f(x), h(x)$. Any constant multiple of $m(x)$ will define the same equivalence relation as $m(x)$ so we usually take $m(x)$ to be monic.

We will write $[f(x)]_{m(x)}$ for the congruence class of $f(x)$ modulo $m(x)$, whenever we need to be careful to distinguish between $f(x)$ and its congruence class. We hope this rarely occurs!

Theorem 5.2 (Arithmetic mod $m(x)$)**.** *Suppose that $f(x) \equiv h(x) \mod m(x)$ and $r(x) \equiv s(x) \mod m(x)$. Then $f(x)+r(x) \equiv b(x)+s(x) \mod m(x)$ and $f(x)r(x) = b(x)s(x) \mod m(x)$. Thus, arithmetic on congruence classes modulo $m(x)$ is well-defined.*

We will write $F[x]/m(x)$ for the set of equivalence classes modulo $m(x)$, with the operations $+$ and $*$. The theorem also shows that the function taking $f(x)$ to $[f(x)]_{m(x)}$ is a homomorphism from $F[x]$ to $F[x]/m(x)$. If $d(x)$ divides $m(x)$ then there is a well defined function from $F[x]/m(x)$ to $F[x]/d(x)$. This is because $m(x)|(a(x)-b(x))$ implies $d(x)|(a(x)-b(x))$, so any two polynomials that are congruent modulo $m(x)$ are also congruent modulo $d(x)$. On the other hand if $d(x) \not| m(x)$ there is no well defined function from $F[x]/m(x)$ to $F[x]/d(x)$ (e.g. $m(x)$ is congruent to 0 modulo $m(x)$ but is not congruent to 0 mod $d(x)$). Since the arithmetic on $F[x]/m(x)$ is "inherited" from $F[x]$ we have:

Theorem 5.3 (Homomorphism mod $m(x)$)**.** *There is a homomorphism from $F[x]/m(x)$ to $F[x]/d(x)$ iff $d(x)|m(x)$. The homomomorphism is unique (since it takes $[1]_{m(x)}$ to $[1]_{d(x)}$ and $[x]_{m(x)}$ to $[x]_{d(x)}$).*

For any two polynomials $m(x)$, $n(x)$ we have a homomorphism $F[x]/(m(x)n(x)) \longrightarrow F[x]/m(x)$ and $F[x]/(m(x)n(x)) \longrightarrow F[x]/n(x)$. This gives a homomorphism into the Cartesian product: $F[x]/m(x) \times F[x]/n(x)$. There is a straightforward generalization of the CRT (and the associated algorithm).

Theorem 5.4 (Chinese Remainder Theorem)**.** *Let $m(x), n(x) \in F[x]$ be coprime. There is an isomorphism $F[x]/(m(x)n(x)) \longrightarrow F[x]/m(x) \times F[x]/n(x)$.*

Theorem 5.5 (Units, Zero Divisors)**.** *Let $m(x) \in F[x]$, and $f(x) \in F[x]$.*

1. *$f(x)$ is a unit in $F[x]/m(x)$ iff $\gcd(f(x), m(x)) = 1$.*
2. *$f(x)$ is a zero-divisor in $F[x]/m(x)$ iff $0 < \deg(\gcd(f(x), m(x))) < \deg(m(x))$.*

In particular, an element of $F[x]/m(x)$ is either 0, a unit, or a zero-divisor (and these are mutually exclusive).

Corollary 5.6. *Let $p(x)$ be irreducible. Then $\mathbb{Z}/p(x)$ is a field; every nonzero element has an inverse.*

Theorem 5.7 (Chinese Remainder Theorem)**.** *Let m, n be coprime. There is an isomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$*

1. There is a formula relating the number of idempotents in $F[x]/m(x)$ with the number of distinct prime factors that $m(x)$ has. See if you can find this formula.

2. Find a formula relating the number of zero divisors and the number of units in $\mathbb{F}_p[x]/m(x)$.

3. Here is a sequence of problems about the number of zero divisors in $\mathbb{F}_p[x]$. You can get the number of units from the formula above.

   (a) Let $m(x) = q(x)s(x)$ for distinct irreducibles $q(x)$ and $s(x)$ in $\mathbb{F}_p[x]$. There is a formula using $\deg(q(x))$ and $\deg(s(x))$ that tells the number of zero divisors in $\mathbb{F}_p[x]/m(x)$. Find it!

   (b) Can you extend to $m(x) = q(x)r(x)s(x)$ with $q(x)$, $r(x)$, $s(x)$ distinct irreducibles? Can you extend to arbitrary square-free $m(x)$?

   (c) Find a formula for the number of zero divisors in $\mathbb{Z}/q(x)^a$.

   (d) Find a formula for the number of zero divisors in $\mathbb{Z}/(q(x)^a s(x)^b)$ for $q(x)$, $s(x)$ distinct primes.

4. Find the kernel of the homomorphism

$$F[x]/(m(x)n(x)) \longrightarrow F[x]/m(x) \times F[x]/n(x)$$

6 Facts about Fields

There are some fundamental results about fields that take some work to establish, but that are not difficult to understand. One doesn't need to understand the proofs to make effective use of the results, so I summarize them here.

Theorem 6.1 (Fundamental Theorem of Algebra)**.** *Any polynomial over the complex numbers, $\mathbb{C}$, factors completely into linear factors. In other words, every irreducible element of $\mathbb{C}[x]$ has degree one.*

A field F in which every polynomial factors into linear factors is called *algebraically closed.* The following theorem show that there is a well defined field called the *algebraic closure* of F.

Theorem 6.2. *Given a field F there is a field $\overline{F}$ containing F that is algebraically closed. It is unique up to isomorphism. Every element of $\overline{F}$ is a root of some monic polynomial with coefficients in F.*

The field $\overline{Q}$ is a subset of the complex numbers containing most of the numbers you can think of $\sqrt{2}$, $\sqrt[3]{\sqrt[7]{11}+9}$, but not π or e.

We have already seen that $\mathbb{Z}/p$ is a field for p a prime. We can completely characterize finite fields.

Theorem 6.3. *Let F be a field with a finite number of elements.*

1) *F has p^n elements where p is a prime.*

2) *There is an element $\alpha \in F$ whose powers $\alpha^1, \alpha^2, \ldots, \alpha^{p^n-1} = 1$ give all the nonzero elements of F.*

3) *F is isomorphic to $\mathbb{F}_p[x]/m(x)$ for some irreducible polynomial $m(x)$ over $\mathbb{F}_p$.*

For any prime p and any positive integer n,

4) *There exists a field with p^n elements.*

5) *Any two fields with p^n elements are isomorphic.*

As a first step we prove

Proposition 6.4. *A finite field is a vector space over $\mathbb{F}_p$ for some prime p. Consequently, the number of elements of F is a power of p.*

Proof. Suppose that F is a finite field. Consider the additive subgroup generated by 1, i.e. 1, $1+1$, $1+1+1$. Let m be the smallest positive integer such that the sum of m 1's is 0. If m where composite, $m = ab$, then we would have

$$0 = \underbrace{1+1+1+\cdots+1+1}_{m \text{ terms}} = (\underbrace{1+1+\cdots+1}_{a \text{ terms}})(\underbrace{1+1+\cdots+1}_{b \text{ terms}})$$

The two factors on the right would then be zero-divisors, contradicting the assumption that F is a field. Thus m is in fact a prime, which we will now call p. We may think of F as containing a copy of $\mathbb{F}_p$. From the field axioms we see immediately that F satisfies the axioms for a vector space over $\mathbb{F}_p$. If its dimension over $\mathbb{F}_p$ is n then F must have p^n elements. Thus any field has a prime power number of elements. □

Definition 6.5. The prime p in the theorem is called the *characteristic* of the field.

Suppose that $q = p^n$ is the number of elements in F. By the field axioms, the set of nonzero elements of F is a group under multiplication. This group is denoted $F^\star$. Recall that the *order* of an element α in a group G is the smallest positive integer r such that α^r is the identity, or infinity, if no such r exists. As an exercise, review the following properties:

Lemma 6.6. *Let α be an element of order r in a group G.*

1) $\alpha^i = \alpha^j$ iff $i \equiv j \mod r$.

2) The order of α^i is r/d where $d = \gcd(i, r)$.

3) Let $\beta \in G$ have order s, coprime to r. Then $\operatorname{ord}(\alpha\beta) = rs$.

Now we can establish item 2) of the Theorem.

Proposition 6.7. *The multiplicative group of a finite field is cyclic.*

Proof. Let F have p^n elements and let the prime factorization of $p^n - 1$ be $\prod_{i=1}^r q_i^{a_i}$. We will show that for each $i = 1 \ldots, r$ there is an element $b_i \in F^\star$ of order $q_i^{a_i}$. By Lemma 6.6, the order of $b = \prod_{i=1}^r b_i$ is $\prod_{i=1}^r q_i^{a_i} = p^n - 1$. Thus b generates the multiplicative group of F.

Let $q^a || (p^n - 1)$ and let $t = (p^n - 1)/q^a$ and consider the set $S = \{\alpha^t : \alpha \in F^\star\}$. For any $\beta \in S$ the polynomial $x^t - \beta$ has at most t roots so there can be at most t elements of F whose tth power is β. Therefore the cardinality of S is at least $(p^n - 1)/t = q^a$. On the other hand, everything in S is a root of $x^{q^a} - 1$ since

$$(\alpha^t)^{q^a} = \alpha^{p^n - 1} = 1$$

There can be only q^a roots of $x^{q^a} - 1$, so S has at most q^a elements. This shows $|S| = q^a$. Similarly, at most q^{a-1} of the elements in S can be roots of $x^{q^{a-1}} - 1$ so there must be at least $q^a - q^{a-1}$ elements of S whose order in F is q^a. This was what we wanted to show.

□

Definition 6.8. An element of a finite field whose powers generate the nonzero elements of the field is called *primitive*.

The theorem says that every finite field has a primitive element. Furthermore, from the lemma, if α is primitive in a field of p^n elements then α^k is also primitive whenever k is coprime to $p^n - 1$. Thus there are $\phi(p^n - 1)$ primitive elements, where ϕ is the Euler totient function ($\phi(n)$ is the number of positive integers less than n and coprime to n).

Corollary 6.9. *If F is a field with p^n elements then*

$$x^{p^n} - x = \prod_{\alpha \in F} (x - \alpha) \qquad \textit{and,}$$

$$x^{p^n - 1} - 1 = \prod_{\alpha \in F^\star} (x - \alpha)$$

According to the following definition, the corollary shows that a field F of order p^n is a splitting field for $x^{p^n-1}-1$ and for $x^{p^n}-x$ over $\mathbb{F}_p$.

Definition 6.10. Let F be a field and let $f(x) \in F[x]$. A *splitting field* for $f(x)$ is a field K containing F such that

- $f(x)$ factors into linear factors in $K[x]$.
- Every element of K can be written as a polynomial in the roots of $f(x)$.

To prove item 3) of the Theorem we need to use the minimal polynomial of a primitive element (see Definition **??**).

Proposition 6.11. *Let F be a finite field of p^n elements. Let β be any primitive element of F and let $M(x)$ be its minimal polynomial over $\mathbb{F}_p$. Then F is isomorphic to $\mathbb{F}_p[x]/M(x)$. In particular* $\deg M(x) = n$.

Proof. Let $M(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0$ with $a_i \in \mathbb{F}_p$. We will show that $1, \beta, \ldots, \beta^{r-1}$ is a basis for F over $\mathbb{F}_p$. We first observe that $1, \beta, \ldots, \beta^{r-1}$ must be linearly independent over $\mathbb{F}_p$. Suppose on the contrary that some nontrivial linear combination is 0, $b_{r-1}\beta^{r-1} + \cdots + b_1\beta + b_0 = 0$. Let k be the largest positive integer such that $b_k \neq 0$. Then

$$\beta^k + \frac{b_{k-1}}{b_k} \cdots + \frac{b_1}{b_k}\beta + \frac{b_0}{b_0} = 0$$

This shows that β is a root of a polynomial over $\mathbb{F}_p$ of degree less than $\deg M(x)$, contradicting the minimality of $M(x)$.

Next we show that any power of β can be written as a linear combination of $1, \beta, \beta^2, \ldots, \beta^{r-1}$. This is true trivially for β^i for $i = 0, \ldots, r-1$. Assume that for some $k \geq r$, each a^i for $i < k$ can be written as a linear.combination as stated. Since $M(\beta) = 0$, $\beta^r = -a_{r-1}\beta^{r-1} - \cdots - a_1\beta - a_0$. Multiplying by β^{k-r} we can write β^k as a linear combination of lower powers of β. By the induction hypothesis these are all linear combinations of $1, \beta, \ldots, \beta^{r-1}$, so β^k is also. Since every nonzero element of F is a power of β, we have shown that $1, \beta, \ldots, \beta^{n-1}$ span F as claimed.

Since F has p^n elements $r = n$. Furthermore the arithmetic on F is completely determined by its structure as a vector space and $\beta^n = -a_{n-1}\beta^{n-1} - \cdots - a_1\beta - a_0$. This is exactly the same structure that $\mathbb{F}_p[x]/M(x)$ has. In other words the map from $\mathbb{F}_p[x]/M(x)$ to F taking the class of x to β is an isomorphism. □

We can now prove existence and uniqueness for fields of prime power order. We will need the "Freshman's dream":

Proposition 6.12. *Let α, β be elements of a field of characteristic p. Then $(\alpha+\beta)^p = \alpha^p + \beta^p$.*

Proof. Expand $(\alpha+\beta)^p$ using the binomial theorem and we get terms like

$$\binom{p}{k}\alpha^k\beta^{p-k}$$

The binomial coefficient really means 1 added to itself $\binom{p}{k}$ times. Since p divides the binomial coefficient when $1 < k < p$ the coefficient is 0 unless $k = 0$ or $k = p$. That gives the result. □

Proposition 6.13. *For any prime power there exists a unique field of that order.*

Proof. Uniqueness: Let F and F' be two fields with p^n elements. Let α be a primitive element in F and let $M(x)$ be its minimal polynomial over $\mathbb{F}_p$. Since α is a root of $x^{p^n} - x$, Lemma **??** says that $M(x)$ divides $x^{p^n} - x$. By Corollary 6.9, $x^{p^n} - x$ factors into distinct linear factors in both F and F' so there must be a root of $M(x)$ in F'. By Proposition 6.11, both F and F' are isomorphic to $\mathbb{F}_p[x]/M(x)$ so they are isomorphic to each other.

Existence: By successively factoring $x^{p^n} - x$ and adjoining roots of a nonlinear irreducible factor, we can, after a finite number of steps, arrive at a field in which $x^{p^n} - x$ factors completely. I claim that the roots of $x^{p^n} - x$ form a field, which by Proposition **??** must have p^n elements.

We need to show that the sum of two roots is a root, that the additive inverse of a root is a root, that the product of two roots is a root and that the multiplicative inverse of a root is a root. These are all trivial except for the case of the sum of two roots, which can be proved using the "Freshman's dream." □

The following example shows that there are many ways to construct a given field.

Example 6.14. Let $p = 3$. We can construct the field $\mathbb{F}_{3^2}$ by adjoining to $\mathbb{F}_3$ a root α of the irreducible polynomial $x^2 + 2x + 2$. You can check by hand that α is primitive in this field. If we had used $x^2 + 1$, which is also irreducible, we would get still get a field with 9 elements. But the root of $x^2 + 1$ will only have order 4 since $\alpha^= -1$ implies $\alpha^4 = 1$.

Definition 6.15. Let F be a finite field and let $p(x)$ be a polynomial over F. If $p(x)$ is irreducible and the class of x is primitive in $F[x]/p(x)$, then we say $p(x)$ is a *primitive polynomial.*

Example 6.16. We can construct $\mathbb{F}_{3^6}$ by adjoining to the field of the previous example a root β of the primitive polynomial (verified using Magma) $x^3 + \alpha x^2 + \alpha x + \alpha^3$ over $\mathbb{F}_{3^2}$. Elements of $\mathbb{F}_{3^6}$ are uniquely represented as polynomials in α and β whose degree in α is at most 1, and whose degree in β is at most 2.

We could also construct $\mathbb{F}_{3^6}$ by first constructing $\mathbb{F}_{3^3}$ by adjoining a root α' of the primitive polynomial $x^3 + 2x + 1$ and then adjoining a root β' of the primitive polynomial (verified using Magma) $x^2 + x + (\alpha')^7$ over $\mathbb{F}_{3^3}$.

Finally we could construct $\mathbb{F}^{3^6}$ directly by adjoining a root of the primitive polynomial $x^6 + 2x^4 + x^2 + 2x + 2$.

In each of these fields you can find a root of any one of the polynomials, and thereby define isomorphisms between the fields.

1. Construct $\mathbb{F}_{2^6}$ in three ways:
   a) by constructing $\mathbb{F}_4$ using an irreducible polynomial of degree 2 over $\mathbb{F}_2$ and then by constructing $\mathbb{F}_{64}$ using an irreducible polynomial of degree 3 over $\mathbb{F}_4$.
   b) by constructing $\mathbb{F}_8$ using an irreducible polynomial of degree 3 over $\mathbb{F}_2$ and then by constructing $\mathbb{F}_{64}$ using an irreducible polynomial of degree 2 over $\mathbb{F}_8$.
   c) by using an irreducible polynomial of degree 6 over $\mathbb{F}_2$.
   Give isomorphisms between the three representations.

2. Construct $\mathbb{F}_{81}$ in two ways. You may notice that $x^2 + 2x + 1$ and $x^2 + x + 2$ are both irreducible over $\mathbb{F}_3$. Can you construct $\mathbb{F}_{81}$ by using one of these polynomials and then the other?

3. Factor $x^{80} - 1$ over $\mathbb{F}_3$ and explain the relationship between the factors and the elements of $\mathbb{F}_{81}$. Factor $x^{80} - 1$ over $\mathbb{F}_9$ and explain the relationship between the factors and the elements of $\mathbb{F}_{81}$.

4. Factor $x^{15} - 1$ over $\mathbb{F}_2$. Construct $\mathbb{F}_{16}$ in three ways as a degree 4 extension of $\mathbb{F}_2$ and show isomorphisms between the three representations.

5. Make a table showing the possible orders and the number of elements of each order for $\mathbb{F}_{64}$, $\mathbb{F}_{128}$, and $\mathbb{F}_{256}$.

6. Prove that if $r|n$ then $\mathbb{F}_{q^r}$ is a subfield of $\mathbb{F}_{q^n}$.

7. Let $n = 6$. Find all irreducible polynomials over $\mathbb{F}_2$ of $\deg d$ where $d|n$. Find the product of these polynomials.

8. For a given prime p, let $I(d)$ be the set of irreducible polynomials of degree d over $\mathbb{F}_p$. Show that for $n > 0$,

$$\prod_{d|n} \prod_{f \in I(d)} f = x^n - 1$$

9. Show that for any $\alpha \in \mathbb{F}_q$,

$$1 + \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{q-2} = \begin{cases} 1 \text{ if } \alpha = 0 \\ -1 \text{ if } \alpha = 1 \\ 0 \text{ otherwise} \end{cases}$$

References

[1] Hungerford, *Abstract Algebra: An Introduction, 2nd Ed.*

[2] Rosen, *Elementary Number THeory and Its Applications*, 5th Ed.