Summary of fields

1. Facts true for all fields

If F is any field, then $F[x]$ has essentially the same algebraic properties as $\mathbb{Z}$. In particular,

- $F[x]$ is a ring. (Recall that $F[x]$ with the square brackets is the set of all polynomials with coefficients in F. Be sure not to confuse $F[x]$ and $f(x)$.)
- The units of $F[x]$ are the nonzero constant polynomials.
- The degree of a polynomial is used as a kind of measure of its size, unlike the integers where the absolute value is a measure of size.
- If $a(x)$ and $f(x)$ are in $F[x]$ and $a(x) \neq 0$ then we can divide to get $f(x) = q(x)a(x) + r(x)$ for some quotient $q(x)$ and remainder $r(x)$ with $\deg r(x) < \deg a(x)$.
- The Euclidean algorithm works to find the greatest common divisor of two polynomials.

  (The gcd is unique up to multiplying by a unit.)
- Bezout works: If $d(x) = \gcd(f(x), g(x))$ then there exist $u(x)$ and $w(x)$ with $d(x) = u(x)f(x) + w(x)g(x)$.
- If $f(x)$ is an irreducible polynomial and $f(x)|a(x)b(x)$ then $f(x)|a(x)$ or $f(x)|b(x)$.
- Factorization:
  - For polynomials that can't be factored into smaller ones, meaning into polynomials of lower degree, we say "irreducible" instead of "prime", but it's the same idea.
  - Every polynomial can be factored into irreducibles. This factorization is unique up to order and up to unit factors.
  - Usually we write a factorization as (say) $f(x) = cf_1(x)^{e_1} \dots f_k(x)^{e_k}$, where c is a nonzero constant (i.e., a unit), and each of the $f_i(x)$ is monic (has leading coefficient 1).

    Example: In $\mathbb{R}[x]$, $4x^5 + 8x^4 + 4x^3 = 4x^3(x+1)^2$.
- Roots:

- To say that r in F is a **root** of $f(x)$ means that $f(r) = 0$. Notice that when you say "root" you don't need to write " $= 0$"; we can just say "r is a root of $f(x)$" instead of "r is a root of $f(x) = 0$", although that's OK.
- r in F is a root of $f(x) \Leftrightarrow (x - r) | f(x)$.
- A polynomial $f(x)$ of degree n can have at most n roots.

  Reason: For each distinct root $r_1, r_2, \ldots$, divide $f(x)$ by $(x - r_1)$, then by $(x - r_2)$, and so on; the degree of what is left keeps going down so no more than n linear factors are possible.
- It is possible for $f(x)$ of degree n to have fewer than n roots, for two reasons:

  (i) There might be a repeated linear factor such as $(x-1)^3$. Then the root 1 is called a "multiple root", or more specifically , a "root of multiplicity 3". We think of it as having the root 1 three times.

  (ii) There might be a nonlinear irreducible factor, such as (x^2+1) in $\mathbb{R}[x]$.
- An irreducible polynomial $f(x)$ in $F[x]$ of degree > 1 does not have any roots in F. (However, $f(x)$ could have a root in a larger field containing F. In fact, there *is* such a field.)

- Congruences:
  - Congruences in $F[x]$ modulo $f(x)$ work the way we are used to for integers.
  - Congruence classes (our "boxes") work and make a ring, $F[x]/f(x)F[x]$.
  - If $f(x)$ is irreducible, then $F[x]/f(x)F[x]$ is a field, just as $\mathbb{Z}/p\mathbb{Z}$ is a field if p is prime.

    Example: $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is a field.
  - In fact, if $f(x)$ is irreducible, then $F[x]/f(x)F[x]$ is a field containing F, in which $f(x)$ now has a root, namely the class ("box") of x modulo $f(x)$.

    Example: $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$ is a field in which x^2+1 has a root, which we can call i; this field is isomorphic to $\mathbb{C}$. In fact, this is one way to construct $\mathbb{C}$.

    Note: There isn't time left in the course to do much with constructing fields from polynomial congruences, so questions on the final will be restricted to knowing examples from lecture and homework.

    Even so, do be aware of these larger ideas:

* If $f(x)$ in $F[x]$ is irreducible and doesn't have a root in F, it is always possible to construct a larger field in which $f(x)$ *does* have a root. An example is that x^2+1 has no root in $\mathbb{R}$ but does in $\mathbb{C}$.
* The idea of constructing new mathematical objects by using "boxes" (equivalence classes) occurs frequently in advanced mathematics courses.
* The idea of regarding two objects as the same if they are isomorphic is also very common in advanced mathematics courses. So it doesn't matter whether we think of $\mathbb{C}$ as being made from 2×2 real matrices, or as being made from congruence classes, or as consisting of expressions $a+bi$ that are added and multiplied in a certain way. The first two ways assure us that $\mathbb{C}$ is possible and is a field; the last way is for everyday use.

2. Facts about finite fields

1. $\mathbb{Z}/p\mathbb{Z}$ is a field (which we'll call $\mathbb{F}_p$ when talking about it as a field).
2. Each finite field has a prime characteristic.
3. If the characteristic of a finite field F is p, then
   - $\mathbb{F}_p$ is contained in F as a subfield;
   - F is a vector space over $\mathbb{F}_p$;
   - if the vector-space dimension of F over $\mathbb{F}_p$ is n, then F has p^n elements.
4. For each possible prime power p^n,
   - there *is* a finite field of size p^n;
   - there is only one field of size p^n, "up to isomorphism". (This means that any two fields of that size must be isomorphic.)
   - Our name for this field is $\mathbb{F}_{p^n}$. (Some books call the field $\mathrm{GF}(p^n)$ for "Galois field".)
   - We have discussed the specific examples
     - $\mathbb{F}_p$ ($= \mathbb{Z}/p\mathbb{Z}$) for each prime p.
     - $\mathbb{F}_4$
     - $\mathbb{F}_8$
     - $\mathbb{F}_{2^8}$ (in connection with Rijndael)

– $\mathbb{F}_9$

5. The nonzero elements of a finite field (in other words, the units) have a generator α (also called a "primitive element"). Equivalent ways to describe α:
   - The powers of α are all the nonzero elements;
   - the order of α is $p^n - 1$, if the field has p^n elements;
   - $1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}$ are all the nonzero elements. (Why $p^n - 2$ and not $p^n - 1$?)
6. If the field has p^n elements, the generator α is also a root of some irreducible polynomial of degree n in $\mathbb{F}_p[x]$.
7. The powers $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ (the first n powers) can be used as a basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$.

   The next power α^n can be re-expressed as a linear combination of lower powers using the irreducible polynomial.
8. In $\mathbb{F}_{p^k}$, the function ϕ given by $\phi(a) = a^p$ is an "automorphism"—an isomorphism of the field with itself.

3. Problems[1]

Problem O-1. For the field $\mathbb{F}_8$, it is a fact that there is a generator α that is a root of the irreducible polynomial $x^3 + x + 1$, so $\alpha^3 = 1 + \alpha$. Also, since α is a generator of the seven nonzero elements, we know $\alpha^7 = 1$.

(a) Make a table showing how to write each power of α as a linear combination of the basis $1, \alpha, \alpha^2$. In the table, use blank spaces to indicate 0 coefficients. The table will start

$$\begin{array}{rcccccc} 1 & = & 1 & & & & \\ \alpha & = & & & \alpha & & \\ \alpha^2 & = & & & & & \alpha^2 \\ \alpha^3 & = & 1 & + & \alpha & & \\ \alpha^4 & = & & & \alpha & + & \alpha^2 \end{array}$$

From there on, multiply through by α and simplify using what we know about α^3.

It is handy to use the powers of α when multiplying and the linear combinations when adding.

(b) Find $(1 + \alpha + \alpha^2)^2$ as a linear combination of $1, \alpha, \alpha^2$ by using the table.

(c) Find $\alpha^3 + \alpha^4$ as a power of α by using the table.

[1] To be handed in only if an assignment says to do so.

Problem O-2. (a) For $a \neq 0$ in $\mathbb{F}_{p^k}$, show that $a^{p^k-1} = 1$.

(Method: Like Fermat and Euler.)

(b) Show that $a^{p^k} = a$ for any a in $\mathbb{F}_{p^k}$.

(Method: Start with (a) and multiply through by a.)

(c) Let $\phi : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be given by $\phi(a) = a^p$. Show that $\phi^k(a)$, meaning $\phi(\phi(\ldots(\phi(a))\ldots))$ k times, equals a for every a in the field.

Problem O-3. Show that in a finite field F of characteristic p, the map $\phi : F \to F$ given by $\phi(a) = a^p$ is an automorphism—an isomorphism of the field with itself. You will need to show

(i) $\phi(ab) = \phi(a)\phi(b)$

(ii) $\phi(a+b) = \phi(a)+\phi(b)$. (What do you know about binomial coefficients?)

(iii) ϕ is one-to-one from F onto F.

(Method for (iii): You may quote (c) of the preceding problem, whether or not the problem was assigned. If ϕ is not one-to-one, could a composition of ϕ with itself be one-to-one? Similary for onto?)

Problem O-4. (a) Show that if a unit a in $\mathbb{Z}/m\mathbb{Z}$ has order r and $r'|r$ then $a^{r/r'}$ has order r'.

(b) Show that if r and s are positive integers and $\ell = \text{lcm}(r, s)$ then there are divisors r' and s' of r and s respectively such that $\ell = r's'$ and r' and s' are coprime.

(Method: Use prime factorizations.)

(c) Prove (g)-(ii) on p. H 2: If a commutative ring R has a unit a of order r and a unit b of order s, then R has a unit of order ℓ where[2] $\ell = \text{lcm}(r, s)$. (Note that this element is not necessarily ab, since for example if $b = a^{-1}$ then a and b have the same order r and $\text{lcm}(r, r) = r$, but $ab = 1$, which is an element of order 1.)

(Method: Use (a) and (b) and N-3.)

(d) Show that in $\mathbb{Z}/m\mathbb{Z}$ if the maximum order of a unit is r then the order of every unit actually *divides* r.

Then by (a), the possible orders of units are r and all its divisors.

(Method: If a has the maximum possible order, r, and another unit b has order s, what about $\text{lcm}(r, s)$?)

[2] (g)-(ii) had the letter d for the lcm, but that sounds like a gcd so let's use ell instead.

Problem O-5. Prove that a finite field has a generator for the nonzero elements.

(Method: You may quote (d) of the preceding problem, whether or not it was assigned. If the maximum order of an element is r, show that $a^r = 1$ for every nonzero element a. In that case, every nonzero element is a root of $x^r - 1$. You know how to compare the number of roots and the order. So how large must r be? And remember, there *is* an element of order r.)