Putnam preparation

Polynomials, Abstract Algebra

We follow very closely outside sources, in many places we copy literally. I make no claim of originality.

Algebraic identities.

Some factorization formulas:

$$a^2 - b^2 = (a-b)(a+b) \ ;$$

$$a^2 + 2ab + b^2 = (a+b)^2 \ ;$$

$$a^2 + b^2 + c^2 + 2ab + 2ac + 2bc = (a+b+c)^2 \ ;$$

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \ ;$$

If n is odd, we can replace b by $(-b)$ in the last formula to get

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}) \ , n \text{ odd.}$$

Polynomials.

A polynomial of degree n (n a nonnegative integer) in the variable x is an expression of the form

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

where $a_0, a_1, \ldots, a_n$ are constants (called the *coefficients*), and $a_n \neq 0$. A polynomial all whose coefficients are zero is called the *zero polynomial*; no degree is assigned to the zero polynomial. The coefficient a_n is called the *leading coefficient*; if it is equal to 1 we say $P(x)$ is a *monic polynomial.* Two polynomials are called (identically) *equal* if their coefficients are equal term for term, that is their coefficients for the same power of the variable are equal.

If the coefficients of the polynomial $P(x)$ are integers, we say that $P(x)$ is a polynomial *over the integers*; similarly if the coefficients are rationals, we say that $P(x)$ is a polynomial *over the rationals*, and so forth.

In many respects polynomials are like integers. They can be added, subtracted, and multiplied; there is a division algorithm (more on this later). A polynomial F *divides* a polynomial G (exactly) if there is a polynomial Q such that $G = QF$ (i.e. G is a multiple of F.) A polynomial H is a *greatest common divisor* of polynomials F and G if and only if (1) H divides F and G and (2) if K is another polynomial that divides F and G, then K divides H. It can be shown that H is unique up to a constant multiple.

Theorem. (Division Algorithm for Polynomials.) If $F(x)$ and $G(x)$ are polynomials over a field K (e.g. K might be $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ for p prime), there exist unique polynomials $Q(x)$ and $R(x)$ over the field K such that

$$F(x) = Q(x)G(x) + R(x) \ ,$$

where $R(x) \equiv 0$ or $\deg R(x) < \deg G(x)$ (deg denotes degree.)

Moreover, if K is an integral domain (such as $\mathbb{Z}$), the same result holds provided $G(x)$ is a monic polynomial. (The definition of integral domain is recalled in p.10 below.)

For example, if $F(x) = 3x^5 + 2x^2 - 5$, and $G(x) = 2x^3 + 6x + 3$, then $Q(x) = \frac{3}{2}x^2 - \frac{9}{2}$ and $R(x) = \frac{1}{2}x^2 + 27x - \frac{1}{2}$.

As with the integers, the division algorithm can be used to find the greatest common divisor of two polynomials. Moreover, if F and G are polynomials (over a field K), there are polynomials S and T (over K) such that

$$\gcd(F, G) = SF + TG \ ,$$

where $\gcd(F, G)$ denotes the greatest common divisor of F and G.

Definition. Let $F(x)$ be a polynomial over an integral domain D. If an element $a \in D$ is such that $F(a) = 0$, we say a is a *root* of $F(x) = 0$, or that a is a *zero* of $F(x)$.

Theorem. The quadratic equation $ax^2 + bx + c = 0$ ($a, b, c \in \mathbb{R}$, $a \neq 0$) has solutions

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \ .$$

The discriminant D of the quadratic equation is defined as $D = b^2 - 4ac$. For $D < 0$ the solutions are complex and conjugate to each other, for $D = 0$ the solutions degenerate to one real solution, and for $D > 0$ the equation has two distinct real solutions.

Definition. *The binomial coefficients* $\binom{n}{k}$, $n, k \in \mathbb{N}_0$, $k \leq n$, are defined as

$$\binom{n}{i} = \frac{n!}{i!(n-i)!} \ .$$

They satisfy $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$ for $i > 0$ and also

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n \ ,$$

$$\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n \binom{n}{n} = 0 \ ,$$

$$\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i} \binom{m}{k-i} \ .$$

Theorem. (Newton's binomial formula.) For $x, y \in \mathbb{C}$ and $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i \ .$$

Theorem. (Bezout's theorem.) A polynomial $P(x)$ (over an integral domain D) is divisible by the binomial $x - a$ ($a \in \mathbb{C}$) if and only if $P(a) = 0$. Moreover, the remainder from the division of the polynomial $P(x)$ by $x - a$ is equal to $P(a)$.

By repeated application of Bezout's theorem, we can prove that there is a unique non-negative integer m and a unique polynomial $G(x)$ over D such that

$$P(x) = (x-a)^m G(x) \ ,$$

where $G(a) \neq 0$. In this case we say a is a *zero of multiplicity m.*

The unique factorization theorem for integers states that every integer can be written uniquely as a product of primes. There is a similar theorem for polynomials: every polynomial over a field can be written uniquely as a product of irreducible polynomials (i.e. prime factors.) In the case of $\mathbb{C}$, the irreducible factors are the linear polynomials. In the case of $\mathbb{R}$, the irreducible factors are the linear polynomials and the quadratic polynomials with negative discriminant (i.e. those of the form $ax^2 + bx + c$, where $b^2 - 4ac < 0$.)

Theorem.(The rational root theorem.) If $x = \frac{p}{q}$ is a rational zero of a polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with integer coefficients and $(p, q) = 1$ (i.e. the greatest common divisor of p and q is 1), then $p|a_0$ and $q|a_n$.

Theorem.(Gauss' lemma.) Let $P(x)$ be a polynomial with integer coefficients. If $P(x)$ can be factored into a product of two polynomials with rational coefficients, then $P(x)$ can be factored into a product of two polynomials with integer coefficients.

Theorem.(The fundamental theorem of algebra.) Every nonconstant polynomial with coefficients in $\mathbb{C}$ has a complex root.

In a related fashion, if P is a nonzero polynomial of degree n over an integral domain D, and a is a root of $P(x) = 0$, by Bezout's theorem, there is a polynomial Q of degree $n - 1$ such that $P(x) = (x - a)Q(x)$. Using this fact, an easy induction shows that P has at most n zeros. As a consequence we get (since the polyomial $F - G$ would have degree less than $n + 1$ and would have $n + 1$ zeros)

Identity theorem. Let $F(x)$ and $G(x)$ be two polynomials over an infinite integral domain, both of degree $\leq n$. If $F(x)$ and $G(x)$ have equal values for more than n distinct values of x, then $F(x)$ and $G(x)$ are identical.

Note that polynomials over $\mathbb{Z}_n$ can be added, subtracted and multiplied in the usual manner except that the arithmetic (on the coefficients) is done within $\mathbb{Z}_n$ (i.e. modulo n.) If n is a prime number, say $n = p$, then $\mathbb{Z}_p$ is a field, so all the results concerning polynomials over fields (e.g. Bezout's theorem, the identity theorem) continue to hold. This is not the case if n is not a prime. For example, $2x^3 - 2x$, as a polynomial over $\mathbb{Z}_4$, has four distinct roots in $\mathbb{Z}_4$, namely $0, 1, 2$, and 3, whereas it would have at most three if the arithmetic were carried out in a field.

Let p be a prime, and consider the binomial theorem modulo p

$$(1+x)^p \equiv \sum_{k=0}^{n} \binom{p}{k} x^k \ (mod\ p) \ ,$$

where each side is regarded as a polynomial over $\mathbb{Z}_p$. For $1 \leq k \leq p - 1$, we have that $\binom{p}{k} \equiv 0 \ (mod\ p)$, since none of the factors in $k!(p - k)!$ divide the factor of p in $p!$. Thus, as polynomials over $\mathbb{Z}_p$,

$$(1+x)^p \equiv 1 + x^p \ (mod\ p) \ .$$

More generally, for each positive integer n,

$$(1+x)^{p^n} \equiv 1 + x^{p^n} \ (mod\ p) \ .$$

The proof is by induction. We know it is true for $n = 1$, and we assume it is true for k. Then

$$\begin{aligned}
(1+x)^{p^{k+1}} &\equiv \underbrace{(1+x)^{p^k}(1+x)^{p^k}\cdots(1+x)^{p^k}}_{p \text{ times}} \ (mod\ p) \\
&\equiv (1+x^{p^k})(1+x^{p^k})\cdots(1+x^{p^k}) \ (mod\ p) \\
&\equiv (1+x^{p^k})^p \ (mod\ p) \\
&\equiv 1+(x^{p^k})^p \ (mod\ p) \\
&\equiv 1+x^{p^{k+1}} \ (mod\ p) \ .
\end{aligned}$$

By equating coefficients of x^i on each side, we get

$$\binom{p^n}{i} \equiv 0 \ (mod\ p) \ , \qquad 1 \le i < p^n$$

Irreducible polynomials.

A polynomial is irreducible if it cannot be written as a product of two polynomials in a nontrivial manner. The question of irreducibility depends on the ring of coefficients. When the coefficients are complex numbers, only linear polynomials are irreducible. For real polynomials some quadratic polynomials are irreducible as well (the ones with negative discriminant.) When the coefficients are rationals or integers, there is an interplay between polynomials and arithmetic. The cases of rational and integer coefficients are more or less equivalent, with minor differences such as the fact that $2x + 2$ is irreducible over $\mathbb{Q}[x]$, but reducible over $\mathbb{Z}[x]$ (since 2 is invertible in $\mathbb{Q}$ but not in $\mathbb{Z}$). (See also Gauss' lemma.) So the formal definition is as follows.

Definition. Assume that $P(x) \in \mathbb{Z}[x]$ is a polynomial such that the greatest common divisor of its coefficients is 1. $P(x)$ is called irreducible over $\mathbb{Z}[x]$ if there do not exist polynomials $Q(x), R(x) \in \mathbb{Z}[x]$ different from ± 1, such that $P(x) = Q(x)R(x)$. Otherwise, $P(x)$ is called reducible.

Theorem. (Eisenstein 's criterion (extended).) Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients. If there exist a prime p and an integer $k \in \{0, 1, 2, \ldots, n-1\}$ such that $p|a_0, a_1, \ldots, a_k$, $p \nmid a_{k+1}$, and $p^2 \nmid a_0$, then there exists an irreducible factor $Q(x)$ of $P(x)$ whose degree is at least k. In particular, if p can be chosen such that $k = n - 1$, then $P(x)$ is irreducible.

Reciprocal or palindromic equations. If an equation has the form $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$ and $a_j = a_{n-j}$ for all $j = 0, \ldots, n$, it is called *palindromic*. For even n, the transformation $z := x + \frac{1}{x}$ reduces the equation to a new one of degree $\frac{n}{2}$. After finding all solutions z_j, the solutions of the original equation are found by solving quadratic equations $x + \frac{1}{x} = z_j$.

Definition. The *symmetric polynomials* in $x_1, x_2, \ldots, x_n$ are polynomials that do not change on permuting the variables $x_1, x_2, \ldots, x_n$. The *elementary symmetric polynomials* are $\sigma_k(x_1, x_2, \ldots, x_n) = \sum x_{i_1} x_{i_2} \cdots x_{i_n}$ (the sum is over all -unordered- k-element subsets $\{i_1, i_2, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$).

Theorem. Every symmetric polynomial in $x_1, x_2, \ldots, x_n$ can be expressed as a polynomial in the elementary symmetric polynomials $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Theorem. (Vieta's formulas.) Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $c_1, c_2, \ldots, c_n$ be complex numbers such that

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n \ .$$

Then $c_k = (-1)^k \sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for $k = 1, 2, \ldots, n$.

Theorem. (Newton's formulas on symmetric polynomials.) Let $\sigma_k = \sigma_k(x_1, x_2, \ldots, x_n)$ and let $s_k = x_1^k + x_2^k + \cdots + x_n^k$, where $x_1, x_2, \ldots, x_n$ are arbitrary complex numbers. Then

$$k\sigma_k = s_1 \sigma_{k-1} - s_2 \sigma_{k-2} + \cdots + (-1)^k s_{k-1} \sigma_1 + (-1)^{k+1} s_k \ .$$

Another way of writing them is that, if $x_1, x_2, \ldots, x_n$ are the roots of

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0 \ ,$$

then

$$\begin{aligned}
s_1 + c_1 &= 0 \\
s_2 + c_1 s_1 + 2c_2 &= 0 \\
s_3 + c_1 s_2 + c_2 s_1 + 3c_3 &= 0 \\
\cdots\cdots & \\
s_n + c_1 s_{n-1} + \cdots + c_{n-1} s_1 + n c_n &= 0 \\
s_p + c_1 s_{p-1} + \cdots + c_n s_{p-n} &= 0 \ , \quad p > n \ .
\end{aligned}$$

Theorem. (Lagrange interpolation formula.) For any sequence $y_1, \ldots, y_n$ of complex numbers and a set of n distinct points $x_1, \ldots, x_n$ from $\mathbb{C}$, there exists a unique polynomial $f(x)$ of degree at most $n-1$ with the property that $f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_n) = y_n$.

The proof consists of two steps: if $g(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$, then

$$\frac{g(x)}{(x - x_1) g'(x_1)} \left(= \frac{(x - x_2)(x - x_3) \cdots (x - x_n)}{(x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n)} \right)$$

is a polynomial of degree $n - 1$ with zeros $x_2, \ldots, x_n$ and which equals 1 at $x = x_1$.

Then

$$f(x) = \frac{g(x)}{(x - x_1) g'(x_1)} y_1 + \frac{g(x)}{(x - x_2) g'(x_2)} y_2 + \cdots + \frac{g(x)}{(x - x_n) g'(x_n)} y_n$$

takes the values $y_1, \ldots, y_n$ at the points $x_1, \ldots, x_n$ respectively.

It is often convenient (and often hard!) to get some information about the location of the roots of polynomials. Here are a few tools.

Definition. Given a finite sequence $a_0, a_1, \ldots, a_n$, we call index $m \geq 1$ the location of a *sign change* if

$$a_{m-1}a_m < 0$$

or

$$a_{m-1} = \cdots = a_{m-k+1} = 0\ , \qquad a_{m-k}a_m < 0,\ , \qquad m \geq k \geq 2.$$

The elements a_{m-1} and a_m in the former case, and a_{m-k} and a_m in the latter case form a *sign change.* The number of sign changes of a sequence does not change if its zero elements are omitted.

Theorem. (Descartes' rule of signs.) Let N be the number of positive zeroes (counted with multiplicity) of a polynomial $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ and let W be the number of sign changes in the sequence of its coefficients. Then $W - N$ is an even nonnegative integer.

In particular, a polynomial cannot have more positive zeroes counting multiplicity than there are sign changes in the coefficients.

As a consequence, the number of negative zeroes is bounded by the number of sign changes in $P(-x)$.

For example, $P(t) = t^{11} - t^6 + t + 1$ has
(1) at most 2 positive roots,
(2) at most 1 negative root,
(3) at least 8 complex roots.

Modulus estimates. In $\mathbb{C}$, let $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$. Set $K = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}$. Then $P(w) = 0$ implies that $|w| < K + 1$.

The proof goes as follows: It is immediate for $|w| \leq 1$. Assume $|w| > 1$. Then

$$0 = P(w) = w^n \left(1 + \frac{a_{n-1}}{w} + \frac{a_{n-2}}{w^2} + \ldots\right)\ ,$$

hence

$$\begin{aligned} 0 = |P(w)| \ &\geq\ |w|^n \left(1 - K\left(\frac{1}{|w|} + \frac{1}{|w|^2} + \ldots\right)\right) \\ &>\ |w|^n \left(1 - K\left(\frac{\frac{1}{|w|}}{1 - \frac{1}{|w|}}\right)\right) \end{aligned}$$

and thus

$$1 - \frac{1}{|w|} - \frac{K}{|w|} < 0\ .$$

For example, $z^4 + 3z^3 + 2z^2 + z + 1$ has all roots satisfying $|z| < 4$.

Rouche's Theorem. Let C be a simple closed curve in the plane. Suppose $p(z)$ and $q(z)$ are polynomials satisfying

$$|q(z)| < |p(z)| \ , \qquad \text{for } z \text{ on } C \ .$$

Then $p(z) + q(z)$ and $p(z)$ have the same number of zeroes inside C.

For example, $z^6 + 10z + 8$ has exactly one zero for $|z| < 1$ (set $p(z) = 10z$ on $|z| = 1$), and as a consequence has five zeroes in $1 < |z| < 2$ (set $p(z) = z^6$ on $|z| = 2$.)

The derivative of a polynomial.

The derivative of a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

is the polynomial

$$P'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1 \ .$$

If $x_1, x_2, \ldots, x_n$ are the zeros of $P(x)$, then by the product rule,

$$\frac{P'(x)}{P(x)} = \frac{1}{x - x_1} + \frac{1}{x - x_2} + \cdots + \frac{1}{x - x_n} \ .$$

If a zero of $P(x)$ has multiplicity greater than 1, then it is also a zero of $P'(x)$, and the converse is also true. By induction, $x = a$ is a zero of $P(x)$ with multiplicity $m > 1$ if and only if $x = a$ is a zero of $P(x), P'(x), \ldots, P^{(m-1)}(x)$ and not a zero of $P^{(m)}(x)$.

By Rolle's theorem, if all the zeros of $P(x)$ are real, then so are those of $P'(x)$.

A famous result for the complex plane $\mathbb{C}$ is the following

Lucas' theorem. The zeros of the derivative $P'(z)$ of a polynomial $P(z)$ lie in the convex hull of the zeros of $P(z)$.

In particular, if the zeros of $P(z)$ lie in an open half-plane, then the zeros of $P'(z)$ lie in that half-plane as well.

Chebyshev polynomials.

The nth Chebyshev polynomial $T_n(x)$ expresses $\cos n\theta$ as a polynomial in $\cos\theta$. This means that $T_n(x) = \cos(n \arccos x)$, for $n \geq 0$. These polynomials satisfy the recurrence

$$T_0(x) = 1, \qquad T_1(x) = x, \qquad T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x) \ , \qquad \text{for } n \geq 1 \ .$$

For example, $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$.

One usually calls these Chebyshev polynomials of the first kind, to distinguish them from the Chebyshev polynomials of the second kind $U_n(x)$ defined by $U_0(x) = 1$, $U_1(x) = 2x$, $U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$, for $n \geq 1$ (same recurrence relation but different initial condition.) Alternatively, $U_n(x)$ can be defined by the equality $U_n(\cos\theta) = \frac{\sin(n+1)\theta}{\sin\theta}$.

Chebyshev's theorem. For fixed $n \geq 1$, the polynomial $2^{-n+1}T_n(x)$ is the unique monic nth-degree polynomial satisfying

$$\max_{-1\leq x\leq 1} |2^{-n+1}T_n(x)| \leq \max_{-1\leq x\leq 1} |P(x)| \ ,$$

for any other monic nth-degree polynomial $P(x)$.

One says that among all monic nth-degree polynomials, $2^{-n+1}T_n(x)$ has the smallest variation away from zero on $[-1,1]$. This variation is $\frac{1}{2^{n-1}}$.

Recurrence Relations.

Definition. A *recurrence relation* is a relation that determines the elements of a sequence x_n, $n \in \mathbb{N}_0$, as a function of previous elements. A recurrence relation of the form

$$(\forall n \geq k) \ \ x_n + a_1 x_{n-1} + \cdots + a_k x_{n-k} = 0$$

for constants $a_1, a_2, \ldots, a_k$ is called a *linear homogeneous recurrence relation of order k*. We define the *characteristic polynomial* of the relation as $P(x) = x^k + a_1 x^{k-1} + \cdots + a_k$.

Theorem. Using the notation introduced in the above definition, let $P(x)$ factorize as $P(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_r)^{k_r}$ where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are distinct complex numbers and $k_1, k_2, \ldots, k_r$ are positive integers. The general solution of this recurrence relation is in this case given by

$$x_n = p_1(n)\alpha_1^n + p_2(n)\alpha_2^n + \cdots + p_r(n)\alpha_r^n \ ,$$

where p_i is a polynomial of degree less than k_i. In particular, if $P(x)$ has k distinct roots, then all p_i are constant. If $x_0, x_1, \ldots, x_{k-1}$ are set, then the coefficients of the polynomials are uniquely determined.

Abstract Algebra.

Definition. A *binary operation* $*$ on a set S associates to each pair $(a,b) \in S \times S$ an element $a * b \in S$. The operation is called *associative* if $a*(b*c) = (a*b)*c$ for all $a,b,c \in S$, and *commutative* if $a*b = b*a$ for all $a,b \in S$. If there exists an element e such that $a*e = e*a = a$ for all $a \in S$, then e is called *identity element.* If an identity element exists, it is unique. In this case, if for an element $a \in S$ there exists $b \in S$ such that $a*b = b*a = e$, then b is called *the inverse* of a and is denoted by a^{-1}. If an element has an inverse, the inverse is unique.

Definition. A *group* is a nonempty set G equipped with an operation $*$ satisfying the following conditions (as you will see, we are repeating many conditions from the definitions just given):

(i) $a*(b*c) = (a*b)*c$ for all $a,b,c \in G$.

(ii) There exists a (unique) *additive identity* $e \in G$ such that $a*e = e*a = a$ for all $a \in G$.

(iii) For each $a \in G$ there exists a (unique) *additive inverse* $a^{-1} = b \in G$ such that $a * b = b * a = e$.

The isometries of the plane, the permutations of a set, the continuous bijections on a closed bounded interval all form groups.

If $n \in \mathbb{Z}$, we define a^n as $a * a * \cdots * a$ (n times) if $n \geq 0$, and as $(a^{-1})^{-n}$ otherwise.

When working with groups we sometimes think of the operation $*$ as "multiplication", and in this case we often supress the $*$ in writing products. Thus, $a * b$ is written as ab, and $a * (b * c)$ is written as $a(bc)$, or abc, and so forth. When we think of the operation $*$ as a product, we sometimes denote the identity element as "1".

It is easy to see that the usual laws of exponents hold in a group, namely,

$$a^n a^m = a^{n+m} \ , \qquad (a^n)^m = a^{nm} \ , \qquad n, m \text{ integers.}$$

Definition. A group $\mathcal{G} = (G, *)$ is commutative or abelian if $a * b = b * a$ for all $a, b \in G$.

An example of a non-commutative group is the set of n-by-n nonsingular matrices over the real numbers with multiplication of matrices.

In any group G, we have that

$$(ab)^{-1} = b^{-1} a^{-1} \ , \qquad a, b \in G$$

If the group G is commutative, it is easy to show that

$$(ab)^n = a^n b^n \ , \qquad a, b \in G, \qquad n \text{ an integer.}$$

Cancellation property. For all $a, b, c \in G$,

$$ab = ac \qquad \text{implies} \qquad b = c \ ,$$

$$ba = ca \qquad \text{implies} \qquad b = c \ .$$

This follows immediately by multiplying on the left (or right) by a^{-1}.

Definition. A set A *generates* a group $(G, *)$ if every element of G can be obtained using powers of the elements of A and the operation $*$. In other words, if A is the generator of a group G then every element $g \in G$ can be written as $g = a_1^{i_1} * \cdots * a_n^{i_n}$, where $a_j \in A$ and $i_j \in \mathbb{Z}$ for every $j = 1, 2, \ldots, n$.

Definition. The *order* of $a \in G$ is the smallest $n \in \mathbb{N}$ such that $a^n = e$, if it exists. The *order* of a group is the number of its elements, if it is finite. Each element of a finite group has a finite order.

This can be easily seen since in the sequence $e, a, a^2, a^3, \ldots,$ either all the elements are different (in which case a has infinite order) or there is a smallest integer n such that $a^n = e$ and $e, a, a^2, a^3, \ldots, a^{n-1}$ are distinct.

Definition. Let G be a group. We say that H is a *subgroup* of G if H is a subset of G which is itself a group (under the operation of G.) The *order* of H is the number of its elements, denoted by $\operatorname{ord}(H)$.

An important class of subgroups are the following. Let $a \in G$, and let

$$\langle a \rangle = \{a^n : n \text{ is an integer.}\}$$

It is easy to check that $\langle a \rangle$ is a subgroup of G; it is called the *cyclic subgroup generated by* a. Note that $\mathrm{ord}(\langle a \rangle) = \mathrm{ord}(a)$.

Theorem. (Lagrange's theorem.) In a finite group G, the order of a subgroup H divides the order of the group G.

There are three important corollaries:

(i) If G is a group of order n and $a \in G$, then $a^n = 1$.

(ii) If G is a group of order p, where p is a prime, then G is a cyclic group (i.e. $G = \langle a \rangle$ for some $a \in G$).

(iii) If G is a group and $a^n = 1$, then the order of a divides n.

The first corollary to Lagrange's theorem states that $a^{ord(G)} = 1$ for each element in the finite group G. This has a number of interesting and important consequences when applied to particular groups. For example, let V_n denote the set of positive integers less than n that are relatively prime to n. The elements of V_n form a group under multiplication modulo n. Let $\phi(n) = ord(V_n)$. (The function ϕ is called the Euler ϕ-function.) Then Lagrange's theorem implies the following theorem that we already saw when dealing with congruences.

Theorem. (Euler's theorem.) If a is any integer relatively prime to n, then

$$a^{\phi(n)} \equiv 1 \ (mod\ n) \ .$$

When n is a prime number, say $n = p$, we have $\phi(p) = p - 1$, so that $a^{p-1} \equiv 1 \ (mod\ p)$ whenever a is not a multiple of p. If we multiply each side by a, we get $a^p \equiv a \ (mod\ p)$. This congruence holds even when a is a multiple of p, and thus we get

Theorem. (Fermat's little theorem.) If a is an integer and p is a prime, then

$$a^p \equiv a \ (mod\ p) \ .$$

Definition. A *ring* is a nonempty set R equipped with two operations $+$ and $\cdot$ such that $(R, +)$ is an abelian group and for any $a, b, c \in R$,

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(ii) $(a + b) \cdot c = a \cdot c + b \cdot c$ and $c \cdot (a + b) = c \cdot a + c \cdot b$.

A ring is *commutative* if $a \cdot b = b \cdot a$ for any $a, b \in R$ and *with identity* if there exists a *multiplicative identity* $i \in R$ such that $a \cdot i = i \cdot a = a$ for all $a \in R$. An element $a \in R$ is called *invertible* if there exists $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = i$.

Rings mimic in the abstract setting the properties of the sets of integers, polynomials, or matrices.

Definition. An *integral domain* D is a commutative ring with identity in which for $a, b \in D$, $ab = 0$ implies $a = 0$ or $b = 0$.

The cancellation property holds in an integral domain. For suppose $ab = ac$ and $a \neq 0$. Then $a(b - c) = 0$, so $b - c = 0$, or equivalently, $b = c$. Similarly, $ba = ca$, $a \neq 0$ implies $b = c$.

Definition. A *field* is a commutative ring with identity in which every element a other than the additive identity has a *multiplicative inverse* a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = i$.

Examples. The following are common examples of groups, rings, and fields (recall that the polynomials with integer, rational, real or complex coefficients are denoted, respectively, by $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$):

Groups: $(\mathbb{Z}_n,+)$, $(\mathbb{Z}_p\setminus\{0\},\cdot)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{R}\setminus\{0\},\cdot)$.

Rings: $(\mathbb{Z}_n,+,\cdot)$, $(\mathbb{Z},+,\cdot)$, $(\mathbb{Z}[x],+,\cdot)$, $(\mathbb{R}[x],+,\cdot)$.

Fields: $(\mathbb{Z}_p,+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{Q}(\sqrt{2}),+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$.

Let p be a prime number. It is easy to see that $0,1,2,\ldots,p-1$ are the zeros of x^p-x (considered as a polynomial over $\mathbb{Z}_p$). Hence, $x^p-x=x(x-1)(x-2)\cdots(x-(p-1))\ (mod\,p)$. As a consequence, comparing the coefficients in x, we obtain

Theorem. (Wilson's theorem.) Let p be a prime number. Then

$$(p-1)!\equiv -1\ (mod\ p)\ .$$

The real numbers have the following nice property.

Theorem. A nontrivial subgroup of the additive group of real numbers is either cyclic or it is dense in the set of real numbers.

Disclaimer: Most (if not all) the material here is from outside sources, I am not claiming any originality.