Let R be a ring with identity, and let U denote the set of units in R. The set U with multiplication in R is a group.

A ring R has two operations: multiplication and addition. It is only a group with respect to addition. Since the group of units in R is a group with respect to the multiplication operation in R and not the addition operation, it does not form a subgroup of R.

The conjugacy class $[a]_m$ in Z/mZ is a unit if and only if $(a, m) = 1$.

Let R be a ring. A nonzero element a in R is a *zero divisor* if there is a nonzero $b \in R$ such that $ab = 0$

If R is a unital ring with finitely many elements, then every nonzero element is either a unit or a zero divisor.

Let R be a ring and suppose $a = 0$ in R is not a zero divisor. Then if $b, c \in R$ are elements for which $ab = ac$, then we must have $b = c$.

For R a commutative ring with identity and $a \in R$ nonzero and not a zero divisor, and $b \in R$ any element, the equation $ax = b$ has either a unique solution or no solutions.

An element a of a ring R with identity cannot be both a zero divisor and a unit.

A field has no zero divisors.

The ring Z/mZ is a field if and only if m is prime

Homomorphisms:

Let R and S be two rings, and $f: R \to S$ a function. The function f is a (ring) homomorphism if

(1) $f(r + r') = f(r) + f(r')$ for any $r, r' \in R$.
(2) $f(r \cdot r') = f(r) \cdot f(r')$ for any $r, r' \in R$.
(3) If R and S are unital, then $f(1_R) = 1_S$, where 1_R is the identity in R, and 1_S is the identity in S.

Properties of Homomorphisms:

Let $f : R \to S$ be a homomorphism. Then,

(1) $f(0) = 0$
(2) $f(-r) = -f(r)$
(3) If $a \in R$ is a zero divisor, then $f(a)$ is a zero divisor in S. (Or $f(a) = 0$.)
(4) If $a \in R$ is a unit, then $f(a)$ is a unit in S and $f(a^{-1}) = f(a)^{-1}$.

Let $f: R \to S$ be a homomorphism.

(1) If whenever $f(r) = f(r')$, we must have $r = r'$, then f is injective
(2) If for any $s \in S$, there is an $r \in R$ such that $f(r) = s$, then f is surjective

Euclid's Algorithm:

$g(x) = f(x)q_1(x) + r_1(x) \qquad \deg r_1(x) < \deg f(x)$
$f(x) = r_1(x)q_2(x) + r_2(x)$
$r_1(x) = r_2(x)q_3(x) + r_3(x)$
.
.
.
$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x)$ where $r_n(x)$ is the last nonzero remainder

$r_n(x)$ is a gcd of $f(x)$ and $g(x)$

If $r(x)|f(x)$ and $r(x)|g(x)$ and if $k \in f(x)$ is nonzero then $k \in F[x]$ is a unit, so $kr(x)|f(x)$ and $kr(x)|g(x)$

If $r(x)$ and $s(x)$ are gcds of $f(x)$ and $g(x)$ in $F[x]$ then there is a scale k such that $s(x) = kr(x)$

The gcd of $f(x)$ and $g(x)$ in $F[x]$ is the monic gcd of Euclid's Algorithm (monic gcd = (f, g))

Bezout's Identity:

Let $f(x), g(x) \in F[x]$ and let $d(x)$ be any gcd of f and g. Then there are polynomials $r(x), s(x) \in F[x]$ such that $d(x) = r(x)f(x) + s(x)g(x)$

A polynomial $p(x)$ in $F[x]$ is irreducible if $p(x)$ is not a unit (i.e. not a nonzero constant polynomial) and if $p(x) = f(x)g(x)$, then either f or g must be a unit.

For polynomials $p(x) \in F[x]$ of degree 2 or 3, $p(x)$ irreducible if and only if $p(x)$ has no roots in F.

If $p(x) = f(x)g(x)$ with neither f nor g a unit, then $0 < \deg f$ and $0 < \deg g$ and $\deg f + \deg g = \deg p = 2$ or 3

Every monic polynomial of positive degree in $F[x]$ is irreducible or factors uniquely into a product of monic irreducibles. If $f \in F[x]$ has leading coefficient a, then f factors into a product of irreducible polynomials, or $f(x) = ag(x)$, where $g(x)$ is monic, and therefore factors uniquely into irreducibles.

Every polynomial of $\deg \geq 1$ is irreducible or factors into a product of irreducibles of lower degree

If $f(x) = p_1(x)p_2(x) \ldots p_s(x) = q_1(x)q_2(x) \ldots q_t(x)$ with all p_i and q_j irreducible then there is a bijection between the p_i's and the q_j's. There is a scalar k such that $q_j = kp_i$.

Alternatively…