Math 343 - Introduction to Modern Algebra **Notes**

Rings and Special Kinds of Rings

Let R be a (nonempty) set. R is a ring if there are two binary operations $+$ and $\cdot$ such that

(A) $(R, +)$ is an abelian group.

(B) $\cdot$ is an associative operation.

(C) For all $x, y, z \in R$ we have the left- and right-distributive laws, $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

A commutative ring is a ring where the operation $\cdot$ is commutative.

Let's go ahead and immediately verify an important detail for a ring R:

Let 0 be the additive identity in R. Then $0 + 0 = 0$. Let $r \in R$. Then $0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$. Then it follows that $0 \cdot r = 0$. Similarly, $r \cdot 0 = 0$.

ELFY: Show that if R is a ring then for all $x, y \in R$ we have that $x(-y) = -(xy) = (-x)y$ and $(-x)(-y) = xy$.

Hint: Use the distributive laws to simplify the sums $xy + x(-y)$, $(-x)y + xy$, and then conclude that $(-x)(-y) = -(x(-y)) = -(-(xy)) = xy$ since $-(xy) + xy = 0$ and that inverses are unique.

Examples:

(1) $R = \{0\}$ forms the trivial ring with $0 + 0 = 0$ and $0 \cdot 0 = 0$.

(2) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all are commutative rings with the usual addition and multiplication.

(3) Let $n \in \mathbb{N}$. The set $n\mathbb{Z}$ is a commutative ring with the usual addition and multiplication.

(4) Let $n \in \mathbb{N}$. The set $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ is a commutative ring with addition modulo n and multiplication modulo n.

(5) We know that $(\mathbb{Z}_n, +) \cong (\mathbb{Z}/n\mathbb{Z}, +)$ (isomorphic as additive groups) and that $\mathbb{Z}_n$ is a ring (see above). Naturally one can ask whether $\mathbb{Z}/n\mathbb{Z}$ forms a ring.

Let's define $\cdot$ as a binary operation on $\mathbb{Z}/n\mathbb{Z}$ by $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z}$.

We must show that this is well-defined. Suppose $(a+n\mathbb{Z}) = (c+n\mathbb{Z})$ and $(b+n\mathbb{Z}) = (d+n\mathbb{Z})$ where $a, b, c, d \in \mathbb{Z}$. Then $(a-b), (c-d) \in n\mathbb{Z}$. So $a-c = nk$ and $b-d = nj$ for some $k, j \in \mathbb{Z}$. Therefore,

$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z} = ((c + nk)(d + nj) + n\mathbb{Z}) = (cd) + n\mathbb{Z}$

since $cd - (c + nk)(d + nj) = n(-cj - dk - nkj) \in n\mathbb{Z}$.

Associativity, commutativity, and the distribution laws are inherited from $\mathbb{Z}$. Hence, $\mathbb{Z}/n\mathbb{Z}$ forms a commutative ring (that we will see is isomorphic to $\mathbb{Z}_n$ as a ring).

(6) Let $n \in \mathbb{N}$. The set M_{nn} forms a noncommutative ring with the usual matrix addition and matrix multiplication as $(M_{nn}, +)$ is an abelian group, matrix multiplication is associative (but not commutative) and distributes over matrix addition.

(7) Let $R_1, R_2, ..., R_n$ be rings. The direct product $R_1 \times R_2 \times \cdots \times R_n$ forms a ring with addition and multiplication done componentwise.

Special kinds of rings:

A ring R with a multiplicative identity (we will write 1 for the multiplicative identity in general) is called a ring with unity and the identity 1 is called unity. In a ring with unity an element $u \in R$ with a multiplicative inverse $u^{-1} \in R$ is called a unit. Consider the set of units in a ring with unity: $R^X = \{r \in R | \exists r^{-1} \in R, rr^{-1} = r^{-1}r = 1\}$. ELFY: Show that this forms a group under multiplication (it's known as unit group of the ring).

Consider $\mathbb{Z}_{10}$, which is a ring with unity. ELFY: $1, 3, 7, 9$ are units while $2, 4, 5, 6, 8$ are not.

Let R be a ring. Let $r \in R$. r is a zero-divisor if $r \neq 0$ and there exists $s \in R$ such that $s \neq 0$ and $r \cdot s = 0$ (and/or $s \cdot r = 0$).

For example, 2 and 3 are zero-divisors in $\mathbb{Z}_6$ as $2 \cdot 3 = 0$.

A commutative ring with unity is an integral domain if it has no zero-divisors. For example, $\mathbb{Z}$ is an integral domain.

A ring R is a field if it is a commutative ring and $R^* = \{x \in R | x \neq 0\}$ forms a group under multiplication.

For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. So is $\mathbb{Z}_p$ where $p \in \mathbb{N}$ is prime (we shall prove this later).

Let R be a ring [or field]. $S \subseteq R$ is a subring [or subfield] of R if it is a ring [or field] itself (using the same operations). For instance, $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ and $\mathbb{Q}$ are a subfield of $\mathbb{R}$. Notation: in both cases we use $\leq$ (and $<$ if proper). So we write $2\mathbb{Z} < \mathbb{Z}$ and $\mathbb{Q} < \mathbb{R}$.

A ring is always a subring of its polynomial ring:

Let R be a ring and $R[X]$ be its polynomial ring (to be formally defined later; it's the set of polynomials with coefficients from R). Then since $R \subset R[X]$ we have that $R < R[X]$.

Proposition 9.1: Let $n \in \mathbb{N}$. In the ring $\mathbb{Z}_n$ the zero divisors are $\{m \in \mathbb{Z}_n^* | \gcd(m, n) \neq 1\}$.

Proof: Let $m \in \mathbb{Z}_n$ where $m \neq 0$. Let $\gcd(m, n) = d$.

Suppose $d > 1$. Then $\frac{mn}{d} = m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n = 0$. But $m \neq 0$ and $\frac{n}{d} \neq 0$. So m is a zero-divisor.

Suppose $d = 1$. Suppose $s \in \mathbb{Z}_n$ and $ms = 0$. Then n divides ms. Then n divides s showing that $s = 0$. Hence m is not a zero-divisor $\square$

Corollary 9.2: For any prime $p \in \mathbb{N}$, $\mathbb{Z}_p$ forms an integral domain.

Proof: Just apply the previous proposition. For all $m \in \mathbb{Z}_p$, if $m \neq 0$ then $\gcd(m, p) = 1$. Hence $\mathbb{Z}_p$ has no zero-divisors, making it an integral domain $\square$

ELFY: Suppose R is a commutative ring. Show that R is an integral domain iff for all $x, y, z \in R$, $xy = xz$ implies $y = z$.

Proposition 9.3: Every finite integral domain is a field.

Proof: Formally we regard the trivial integral domain $\{0\}$ as the trivial field (where $0 = 1$). Clearly, $D = \{0, 1\} = \mathbb{Z}_2$ is a field. Suppose D is a finite integral domain with at least 3 elements. Let $0, 1, a_1, a_2, ..., a_n$ be all the elements of D (where the order of D is $n + 2 \in \{3, ...\}$). Let $a \in D$ where $a \neq 0$.

Consider the elements $a \cdot 1, a \cdot a_1, a \cdot a_2, ..., a \cdot a_n$.

Since $a \cdot b = a \cdot c$ implies $b = c$ for all $b, c \in D$ we have that the $n + 1$ products above are all distinct and non-zero.

So, they must be $1, a_1, a_2, ..., a_n$ in some new order. Hence either $a \cdot 1 = 1$ or $a \cdot a_i = 1$ for some $i \in \{1, 2, ..., n\}$. In the former case, $a = 1$ is a unit. In the latter case a is a unit with $a^{-1} = a_i$.

So every non-zero element of D is invertible and hence forms a multiplicative group. Hence D is a field $\square$

Corollary 9.4: For any prime $p \in \mathbb{N}$, $\mathbb{Z}_p$ forms a field $\square$

Let R be a nontrivial ring. Suppose every element in R is of finite additive order. Then R is said to be of characteristic n if n is the least positive integer such that $r + r + \cdots + r = n \cdot r = 0$ for all $r \in R$.

Suppose it is not the case that every element in R is of finite additive order. Then R is said to be of characteristic 0.

Obviously $\mathbb{Z}$ is of characteristic 0. Consider $\mathbb{Z}_n$ where $n \in \mathbb{N}$. Clearly n is the least integer such that $nm = 0$ for all $m \in \mathbb{Z}_n$. Hence $\mathbb{Z}_n$ is of characteristic 0.

Here is a cute example: Let $R = \mathbb{Z}_2 \times \mathbb{Z}$ where the addition in the first component is modulo 2 and in the second component is the usual addition on $\mathbb{Z}$. Clearly R has elements of finite additive order, such as $(1, 0)$. But R also has elements that are not of finite additive order, like $(0, 1)$. Consequently, R is of characteristic 0.

In a ring with unity, one can check for the characteristic of the ring by just examining what happens to 1:

Let R be a non-trivial ring with unity. Suppose $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$. Then clearly R is of characteristic 0 as not all elements are of finite additive order.

Now assume 1 is of finite additive order. Let n be the least positive integer such that $n \cdot 1 = 0$. Let $r \in R$. Then adding r to itself n times gives $n \cdot r = (1+1+\cdots 1) \cdot r = (n \cdot 1) \cdot r = 0 \cdot r = 0$. Since $n \cdot r = 0$ for all $r \in R$ and n is the least positive integer such that $n \cdot 1 = 0$ it follows that n is the characteristic of R.

ELFY: Show that the binomial theorem $\left((x+y)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} \cdot x^{n-k} \cdot y^k \right)$ holds for x, y in a commutative ring and any positive integer n. Hint: Use induction.

Fermat's and Euler's Theorems

Let $p \in \mathbb{N}$ be prime. Here is a neat consequence of the fact that $\mathbb{Z}_p$ is a field:

$\mathbb{Z}_p^*$ forms a multiplicative group of order $p-1$. Since the order of any element divides the order of the group, we have that $a^{p-1} = 1$ for all $a \in \mathbb{Z}_p^*$. Using that $\mathbb{Z}_p$ and $\mathbb{Z}/p\mathbb{Z}$ are isomorphic as rings (to be proven later) we have that for all $a \in \mathbb{Z}$, if $a \notin p\mathbb{Z}$ then $(a+p\mathbb{Z})^{p-1} = a^{p-1} + p\mathbb{Z} = 1 + p\mathbb{Z}$. So for $a \in \mathbb{Z}$, if $a \notin p\mathbb{Z}$ then $a^{p-1} - 1 \in p\mathbb{Z}$ which implies $a^{p-1} \equiv 1 \pmod{p}$.

We have just proved the following:

Proposition 10.1 **(Fermat's Little Theorem)**: If $a \in \mathbb{Z}$ and $p \in \mathbb{N}$ is a prime not dividing a then $a^{p-1} \equiv 1 \pmod{p}$ □

Corollary 10.2: If $a \in \mathbb{Z}$ then $a^p \equiv a \pmod{p}$ for any prime $p \in \mathbb{N}$.

Proof: Let $a \in \mathbb{Z}$. Let $p \in \mathbb{N}$ be a prime. We consider two cases.

If p does not divide a then $a^p \equiv a \pmod{p}$ holds by using the previous proposition.

If p divides a then $a^p \equiv a \pmod{p}$ holds as both a and a^p are equivalent to 0 modulo p □

Let's compute the remainder of 14^{163} when divided by 17:

By Fermat's Little Theorem, for any positive integer k, $(14^k)^{16} \equiv 1 \pmod{17}$. Then we can use that $14^{160} = (14^{10})^{16}$ to conclude that $14^{160} \equiv 1 \pmod{17}$.

So modulo 17 we get $14^{163} \equiv 14^3 \equiv (-3)^3 \equiv -27 \equiv 7$. So the remainder of 14^{163} when divided by 17 is 7.

Proposition 10.3: Let $n \geq 2$ be an integer. Let G_n be the set of elements in $\mathbb{Z}_n^*$ that are not zero-divisors. G_n forms a group under multiplication modulo n.

Proof: Let's just use ab to denote the multiplication of $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ modulo n (which is associative).

First we show G_n is closed under multiplication modulo n.

Let $a, b \in G_n$. Suppose $ab \notin G_n$. Then there exists $c \in \mathbb{Z}_n$ such that $c \neq 0$ and $(ab)c = 0$. That implies $a(bc) = 0$. Since $b \in G_n$ and $c \neq 0$, $bc \neq 0$ (by the definition of G_n). But then $a \in G_n$ and $bc \neq 0$ implies $a(bc) \neq 0$ (by the definition of G_n). That contradiction tells us G_n is closed under multiplication modulo n.

Of course $1 \in G_n$ as for all $c \in \mathbb{Z}_n^*$, $1c = c \neq 0$.

Let $a \in G_n$. Let $1, a_1, a_2, ..., a_r$ be the $r+1$ elements of G_n. Then

Consider the elements $a1, aa_1, aa_2, ..., aa_r$.

Since $ab = ac$ implies $a(b-c) = 0$ and since $a \in G_n$ we have that $ab = ac$ implies $b = c$ for all $b, c \in G_n$. So the $r+1$ products above are all distinct and in G_n.

So, they must be $1, a_1, a_2, ..., a_r$ in some new order. Hence either $a \cdot 1 = 1$ or $a \cdot a_i = 1$ for some $i \in \{1, 2, ..., r\}$. In the former case, $a = 1$ is a unit and $a^{-1} = 1 \in G_n$. In the latter case a is a unit with $a^{-1} = a_i \in G_n$. Either way $a^{-1} \in G_n$.

Thus G_n is a group under multiplication modulo n $\square$

Let's solve $7x \equiv 3 \pmod{15}$:

7 is in G_{15} as the $\gcd(7, 15) = 1$. In G_n, we have that $7^{-1} = 13$ (ELFY: Verify this is correct).

So the equation $7x = 3$ in G_{15} has the unique solution $x = 7^{-1}(3) = (13)(3) = 9$ in G_{15}.

Let $n \in \mathbb{N}$. The Euler phi-function, $\phi(n)$, is defined as the number of positive integers $k < n$ that are relatively prime to n (meaning that the $\gcd(k, n) = 1$). By proposition 9.1 we have that $\phi(n)$ is the order of the group G_n (elements of $\mathbb{Z}_n$ that are not zero-divisors).

Proposition 10.4 **(Euler's Theorem)**: If $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ is relatively prime to n then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ be relatively prime to n. Then $a + n\mathbb{Z} = b + n\mathbb{Z}$ for some positive integer $b < n$. Let $d = \gcd(b, n) \in \mathbb{N}$. Then $b = kd$ and $n = jd$ for some positive integers k, j. Since $a - b \in n\mathbb{Z}$ we have that $a - b = \ell n$ for some $\ell \in \mathbb{Z}$. But then $a - kd = \ell jd$ implies that $a = d(k + \ell j)$. Thus $d = 1$ as d is a common divisor of a and n.

b is in G_n and hence is of an order that divides $\phi(n)$. Thus $b^{\phi(n)} = 1$ in G_n. Thus

$$a^{\phi(n)} + n\mathbb{Z} = (a + n\mathbb{Z})^{\phi(n)} = (b + n\mathbb{Z})^{\phi(n)} = b^{\phi(n)} + n\mathbb{Z} = 1 + n\mathbb{Z}.$$

Therefore $a^{\phi(n)} - 1 \in n\mathbb{Z}$ which yields $a^{\phi(n)} \equiv 1 \pmod{n}$ $\square$

Note: Euler's Theorem is a generalization of Fermat's Little Theorem.

ELFY: Show that G_{12} is a non-cyclic group of order 4 (thus isomorphic to the Klein 4-group).

Ring Homomorphisms

Suppose R and R' are rings and $\phi : R \to R'$ satisfies

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in R.$$

Then ϕ is a ring homomorphism.

If $\phi : R \to R'$ is a bijection and a homomorphism then ϕ is an ring isomorphism and the rings R and R' are called isomorphic and write $R \cong R'$.

Example:

Let $n \in \mathbb{N}$. Consider the rings $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$. Recall that we know these are isomorphic as additive groups where an isomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ is given by $\phi(m) = m + n\mathbb{Z}$. To show that they are isomorphic as rings it suffices to show that $\phi(\ell m) = \phi(\ell)\phi(m)$ for all $\ell, m \in \mathbb{Z}_n$.

Let $\ell, m \in \mathbb{Z}_n$. Suppose $\ell m = j$ in $\mathbb{Z}_n$. Then in $\mathbb{Z}$ we have $\ell m = kn + j$ where $k \in \mathbb{Z}$. Then $\phi(\ell)\phi(m) = (\ell + n\mathbb{Z})(m + n\mathbb{Z}) = \ell m + n\mathbb{Z} = j + n\mathbb{Z}$ since $\ell m - j \in n\mathbb{Z}$. Hence $\phi(\ell)\phi(m) = \phi(j) = \phi(\ell m)$. Thus ϕ is a ring isomorphism showing $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ (as rings).

Suppose $\phi : R \to R'$ is ring homomorphism. Since a ring homomorphism is a homomorphism of additive groups, forgetting about the other binary operation, we get that $\phi(0) = 0$ and $\phi(-a) = -\phi(a)$ for free from group theory!

Caution: *Unity need not go to unity.* Consider the function $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$ given by

$$\phi(m) = 3m \pmod 6.$$

Let $m, n \in \mathbb{Z}_6$. Let $m + n = j$ and $mn = k$ in $\mathbb{Z}_6$.

Then

$$\phi(m+n) = \phi(j) = 3j \pmod 6 = 3(m+n) \pmod 6 = 3m + 3n \pmod 6 = \phi(m) + \phi(n).$$

Furthermore

$$\phi(mn) = \phi(k) = 3k \pmod 6 = 3mn \pmod 6 = 9mn \pmod 6 = (3m)(3n) \pmod 6 = \phi(m)\phi(n)$$

So ϕ is a ring homomorphism from $\mathbb{Z}_6$ to itself, but $\phi(1) = 3 \neq 1$.

Note: If ϕ is an onto ring homomorphism (aka a ring epimorphism) from a ring with unity to another ring, then that other ring has unity and $\phi(1) = 1$.

Let's see why: Let $\phi : R \to R'$ be an onto ring homomorphism and $1 \in R$ (unity). Let $y \in R'$. Since ϕ onto, there exists $x \in R$ such that $\phi(x) = y$. Therefore, consider that $\phi(1)y = \phi(1)\phi(x) = \phi((1)x) = \phi(x) = y$ and $y\phi(1) = \phi(x)\phi(1) = \phi(x(1)) = \phi(x) = y$. So therefore R' has unity with $\phi(1) = 1$.

Finally we just mention that the kernel of a ring homomorphism $\phi : R \to R'$ is the kernel of ϕ viewed as an additive group homomorphism: $\text{Ker}(\phi) = \{r \in R | \phi(r) = 0\}$.

Polynomial Rings

Let R be a ring. For convenience, we say $p(x)$ (or just p) is a polynomial over R if

$$p(x) = \sum_{k=0}^{\infty} a_k x^k = \sum_{k} a_k x^k$$

where all but finitely many of the coefficients $a_k \in R$ for $k \in \mathbb{Z}_{\geq 0}$ are equal to 0.

By these definitions, polynomials over R are essentially power series with coefficients from R, but finite sums (of ring products) when evaluated at any $r \in R$.

We define the degree of a polynomial p(x) over R, denoted $\deg(p)$, in two cases:

- The degree of the zero polynomial (all coefficients are 0) is $-\infty$.
- The degree of a non-zero polynomial $p(x) = \sum_{k=0}^{\infty} a_k x^k$ over R is n where n is the largest positive integer such that $a_n \neq 0$.

Polynomial notation: Instead of always writing infinite sums, we write

$$p(x) = a_0 + a_1 x + \cdots a_n x^n \text{ (or } p(x) = 0)$$

when $p(x)$ is of degree n (or $-\infty$).

Define $R[X] = \{a_0 + a_1 x_1 + \cdots + a_n x^n | n \in \mathbb{Z}_{\geq 0}, a_i \in R\}$. By the discussion above, $R[X]$ is the set of all polynomials over a ring R.

We have the following rule for polynomial multiplication in $R[X]$:

If $p(x) = \sum_{k} a_k x^k$ and $q(x) = \sum_{k} b_k x^k$ are in $R[X]$ then the product is in $R[X]$ since

$$p(x)q(x) = \sum_{k=0}^{\infty} d_k x^k \text{ where } d_k = \sum_{i=0}^{k} a_i b_{k-i} \in R.$$

It's pretty clear that $(R[X], +)$ is an abelian group. Associativity and the distributive laws are straightforward to check, but are fairly tedious, so they are left as an ELFY.

So $R[X]$ forms a ring with polynomial addition and polynomial multiplication. We call $R[X]$ the polynomial ring over R.

Consider $x+1$ as polynomial in $\mathbb{Z}_2[X]$. Then $(x+1)^2 = x^2+1$ (since $2x = 0$ as $2 = 0$).

Who said you can't distribute exponents!? [Don't get the wrong idea, generally it's not valid!]

Let $R[X]$ be a polynomial ring over a commutative ring R. Then for any $r \in R$, the function $\phi_r : R[X] \to R$ given by $\phi_r(p) = p(r)$ is a homomorphism called the evaluation homomorphism.

Let's check that it is indeed a ring homomorphism:

Let $r \in R$ and ϕ_r be given as above.

Let $p = a_0 + a_1x + \cdots + a_nx^n$ and $q = b_0 + b_1x + \cdots + b_nx^n$ in $R[X]$ (we aren't assuming they are of equal degree; for instance a_n could be 0 with b_n not 0).

So $\phi_r(p+q) = \phi_r((a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n) = (a_0+b_0)+(a_1+b_1)r+\cdots+(a_n+b_n)r^n =$
$= (a_0 + a_1r + \cdots + a_nr^n) + (b_0 + b_1r + \cdots + b_nr^n) = \phi_r(p) + \phi_r(q)$.

Thus ϕ_r is an additive group homomorphism, which means that it suffices to check that ϕ_r satisfies the multiplicative property $\phi_r(fg) = \phi_r(f)\phi_r(g)$ where f, g are monomials in $R[X]$. So let $f = ax^i$ and $g = bx^j$ in $R[X]$. Then $\phi_r(fg) = \phi(abx^{i+j}) = abr^{i+j} = abr^ir^j = (ar^i)(br^j) = \phi_r(f)\phi_r(g)$.

(ELFY): Let R be a commutative ring. Show that the evaluation homomorphism

$$\phi_0 : R[X] \to R$$

is onto.

Proposition 12.1 **(Division Algorithm)**: Let F be a field (commutative ring where the non-zero elements form a multiplicative group). Let $f = a_0 + a_1x + \cdots + a_nx^n$ and $g = b_0 + b_1x + \cdots + b_mx^m$ be elements in $F[X]$ where $a_n \neq 0$, $b_m \neq 0$, and $m > 0$. Then there exist unique polynomials q, r in $F[X]$ such that $f = gq + r$ and $\deg(r) < m$.

Proof: Consider the set $S = \{f - gs | s \in F[X]\}$ which at least contains f. If $0 \in S$ then $f = gs$ for some $s \in F[x]$ which shows there exists q, r described above by taking $q = s$ and $r = 0$ (which has degree $-\infty$ which we regard as less than m).

Otherwise, let $r \in S$ be of minimal degree. Then $r = f - gs$ for some $s \in F[X]$ and thus $f = gs + r$. We need to show that the degree of r is less than m. Well, suppose $r = c_0 + c_1x + \cdots c_tx^t$ in $F[X]$ with $c_t \neq 0$ and $t \geq m$. Then

$$f - g(s + c_tb_m^{-1}x^{t-m}) = f - gs - g(c_tb_m^{-1}x^{t-m}) = r - (c_tx^t + \text{lower degree terms})$$

must be in S and have degree less than r, contradicting how r was chosen. Hence $\deg(r) < m$.

Now suppose $f = gq_1 + r_1$ and $f = gq_2 + r_2$ where $q_1, q_2, r_1, r_2 \in F[X]$ and the degrees of r_1 and r_2 are less than m.

Then $0 = g(q_1 - q_2) + (r_1 - r_2)$ which implies $r_2 - r_1 = g(q_1 - q_2)$ and the degree of $r_2 - r_1$ is less than m, the degree of g. That implies that $q_1 - q_2 = 0$. Hence $q_1 = q_2$. But then $r_2 - r_1 = 0$. Hence $r_1 = r_2$ finishing the proof $\square$

To actually do this in any field we can use the classic procedure:

Let's work in $\mathbb{Z}_3[X]$. Let $f = x^3 + x + 2$ and $g = 2x + 1$. Let's find q, r such that $f = qg + r$ and r is of degree $-\infty$ or 0.

$$\begin{array}{r} 2x^2 + 2x + 1 \\ 2x+1 \overline{)\, x^3 + 0x^2 + x + 2} \\ \underline{x^3 + 2x^2} \\ x^2 + x \\ \underline{x^2 + 2x} \\ 2x + 2 \\ \underline{2x + 1} \\ 1 \end{array}$$

So we have that $x^3 + x + 2 = (2x + 1)(2x^2 + 2x + 1) + 1$ in $\mathbb{Z}_3[X]$.

(ELFY) The Root-Factor Correspondence: Use the division algorithm to show that $a \in F$ is a root (aka zero) of $f \in F[X]$ iff $f = q(x - a)$ for some $q \in F[X]$.

As a consequence, we get that a non-zero polynomial $f \in F[X]$ of degree n can have at most n roots in F.

A non-constant polynomial $f \in F[X]$ is <u>irreducible over F</u> if it cannot be written as a product $f = gh$ where both $g, h \in F[X]$ have lower degree than $f(x)$. Otherwise (meaning f can be written as such a product) the polynomial f is <u>reducible over F</u>.

Of course the particular field being used matters! Consider that $x^2 - 2$ is irreducible over $\mathbb{Q}$, but reducible over $\mathbb{R}$ or $\mathbb{C}$ as in those fields $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Consider $f = x^2 + x + 1$ as a polynomial in $\mathbb{Z}_2[X]$.

Notice that 0 and 1 are not roots of f as $f(0) = 1 \neq 0$ and $f(1) = 1 \neq 0$ (remember we are working in $\mathbb{Z}_2$ here).

Consequently, f is irreducible over $\mathbb{Z}_2$ as it cannot be written as a product of two degree 1 polynomials in $\mathbb{Z}_2[X]$.

However, if we consider $f \in \mathbb{Z}_3[X]$ the story changes. $f(1) = 0$ which means $x - 1 = x + 2$ is a factor of f in $\mathbb{Z}_3[x]$. However, $f(0) = 1 \neq 0$ and $f(2) = 1 \neq 0$, so thus $x + 2$ is the only factor of f, so $f = (x + 2)^2$. Indeed $(x + 2)^2 = x^2 + x + 1$ in $\mathbb{Z}_3[X]$.

(ELFY) Let F be a field and $f \in F[X]$ be of degree at least 2. Prove that if f is irreducible over F then $f(r) \neq 0$ for all $r \in F$ (that is, f does not have a root in F). Hint: Use the division algorithm with $x - r$ as the divisor!

Proposition 12.2: If R is an integral domain then so is $R[X]$.

Proof: Since R is commutative and contains unity, it is clear that $R[X]$ is commutative and contains unity. Let $f, g \in R[X]$ be non-zero polynomials. Let $a \neq 0$ and $b \neq 0$ be their leading coefficients. Then the product ab is the leading coefficient of fg. Since R is an integral domain $ab \neq 0$. Thus $fg \neq 0$ showing $R[X]$ to be an integral domain $\square$

The following is an easy and useful result related to rational polynomials:

Proposition 12.3 **(Rational Root Theorem)**: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $a_n \neq 0$, be in $\mathbb{Z}[X]$ and nonconstant. Assume $f(x)$ has a root a/b in $\mathbb{Q}$ such that (WLOG) a, b are relatively prime. Then a is an integer factor of a_0 and b is an integer factor of a_n.

Proof: Consider that

$$\begin{aligned} 0 &= b^n f(a/b) \\ &= b^n (a_n (a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_1 (a/b) + a_0) \\ &= a_n a^n + a_{n-1} a^{n-1} b + \cdots + a_1 a b^{n-1} + a_0 b^n. \end{aligned}$$

Then we get that $0 = a(a_n a^{n-1} + a_{n-1} a^{n-2} b + \cdots + a_1 b^{n-1}) + a_0 b^n$. This implies a is an integer divisor of $a_0 b^n$ and hence a must be an integer divisor of a_0 as a and b^n are relatively prime.

Similarly $0 = a_n a^n + b(a_{n-1} a^{n-1} + \cdots + a_1 b^{n-2} a + a_0 b^{n-1})$ implies that b must be an integer divisor of a_n $\square$

Ideals and Quotient Rings

Let R be a ring. A subset $I \subseteq R$ is an ideal of R if both of the following hold:

(1) $(I, +) \leq (R, +)$ (I is an additive subgroup).
(2) For all $x \in I$ and for all $r \in R$ we have that $rx, xr \in I$.

Some like to call property 2 the "sticky" property of an ideal.

As we will see, ideals for rings work like normal subgroups for groups...

Examples:

$\{0\}$ and R are ideals of any ring R as they are both obviously additive subgroups and clearly have the "sticky" property!

Consider the commutative ring $\mathbb{Z}$. Let $n \in \mathbb{N}$. We already know (from group theory) that $n\mathbb{Z}$ forms an additive subgroup (actually better than that, a subring). Let $r \in \mathbb{Z}$ and $x \in n\mathbb{Z}$. Then $x = nk$ for some $k \in \mathbb{Z}$. Thus it follows that $rx = xr = (nk)(r) = n(kr) \in n\mathbb{Z}$. Thus $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Note: Not all additive subgroups of rings are subrings. Consider that $< (1/2) >= (1/2)\mathbb{Z} = \{n(1/2) | n \in \mathbb{Z}\}$ is an additive subgroup of the field $\mathbb{Q}$, but since $(1/2)(1/2) = 1/4 \notin < (1/2) >$ it's not a subring!

Proposition 13.1: Let $\phi : R \to S$ be a ring homomorphism. Then $\text{Ker}(\phi)$ is an ideal of R.

Proof: From group theory, we already have that $\text{Ker}(\phi)$ is an additive subgroup of R since the kernel of ϕ as a ring homomorphisms is the same as the kernel of R as an additive group homomorphism. Let $x \in \text{Ker}(\phi)$ and $r \in R$. Then consider that $\phi(rx) = \phi(r)\phi(x) = \phi(r)(0) = 0$ and $\phi(xr) = \phi(x)\phi(r) = (0)\phi(r) = 0$. So $xr, rx \in \text{Ker}(\phi)$ which tells us that $\text{Ker}(\phi)$ is an ideal of R $\square$

Proposition 13.2: Let R be a ring and I be an ideal in R. Then the binary operation on quotient group R/I defined by $(a + I)(b + I) = ab + I$ is well-defined making R/I into a ring, called a quotient ring. Furthermore, if R is commutative then R/I is commutative.

Proof: We already know that $(R/I, +)$ is an abelian group as $(R, +)$ is an abelian additive group and $(I, +)$ is a normal subgroup (all subgroup of an abelian group are normal).

Let's show that the binary operation is well-defined: Suppose $a+I = a'+I$ and $b+I = b'+I$. Then $a - a', b - b' \in I$, so there exists $x, y \in I$ such that $a - a' = x$ and $b - b' = y$. Then $(a+I)(b+I) = ab+I = (a'+x)(b'+y)+I = a'b'+a'y+xb'+xy+I = a'b'+I = (a'+I)(b'+I)$ since $ab - a'b' = a'y + xb' + xy \in I$ as I is an ideal.

Both associativity and distributive laws are left as $(ELFY)$ as they are inherited from R and are easy and straightforward to show.

So R/I is a ring. Suppose R is commutative. Then for any $a + I, b + I \in R/I$ we get $(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$. Hence R/I is commutative $\square$

(ELFY) Suppose R is a ring with unity and $I \neq R$ is an ideal of R. Show that R/I is a ring with unity with $1 + I$ as the unity.

We have ALREADY seen an example of a quotient ring, namely $\mathbb{Z}/n\mathbb{Z}$. We have also shown that given any ring homomorphism $\phi : R \to S$, $\text{Ker}(\phi)$ is an ideal, therefore $R/\text{Ker}(\phi)$ is a quotient ring.

One thing to be aware of is that structure can be "lost" or "gained" between a ring R and a quotient ring of R.

Consider that $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}_6 \cong \mathbb{Z}/6\mathbb{Z}$ is not. Consider that $\mathbb{Z}_6$ is not even an integral domain, while (ELFY) $\mathbb{Z}_6/\{0, 3\} \cong \mathbb{Z}_3$ is a field.

Proposition 13.3 **(First Isomorphism Theorem)**: Let $\phi : R \to S$ is a ring homomorphism then $\phi(R)$ is a subring of S and $R/\text{Ker}(\phi)$ and $\phi(R)$ are isomorphic (as rings).

Proof: (ELFY) It's easy to show that $\phi(R)$ is a subring, since one just needs to justify that $ab \in \phi(R)$ for all $a, b \in \phi(R)$, as it's already known to be an additive subgroup from group theory.

For convenience, let $I = \text{Ker}(\phi)$.

Let $\mu : R/I \to \phi(R)$ be given by $\mu(r + I) = \phi(r)$. Recall that we've already shown this is well-defined and an isomorphism of R/I and $\phi(R)$ as additive groups (Prop. 8.4).

Let's show that we have the multiplicative property. Let $r + I, s + I \in R/I$. Then

$$\mu((r + I)(s + I)) = \mu(rs + I) = \phi(rs) = \phi(r)\phi(s) = \mu(r + I)\mu(s + I).$$

Thus $R/\text{Ker}(\phi) \cong \phi(R)$ as rings $\square$

Let R be a commutative ring with unity. (ELFY) It's very easy to show that for any $r \in R$, the additive subgroup $(r) = \{ra | a \in R\}$ is an ideal, called a <u>principal ideal generated by r</u>.

Proposition 13.4: Let F be a field. Then every ideal in $F[X]$ is a principal ideal generated by some $f \in F[X]$.

Proof: $F[X]$ is a commutative ring with unity so the concept of principal ideal makes sense. Clearly the <u>zero ideal</u> $\{0\}$ is principal as $(0) = \{0\}$.

Suppose I is a non-zero ideal in $F[X]$. Choose a non-zero polynomial $f \in I$ with minimal degree. Without loss of generality assume the leading coefficient is 1 because otherwise we can multiply by the inverse of the leading coefficient (a constant polynomial in $F[X]$) and thereby remain in the ideal I.

Clearly $(f) \subseteq I$ since I is an ideal. Let's prove that $(f) = I$.

Suppose the degree of f is 0. Then $f = 1$ by our assumption that the leading coefficient is 1. Then for any $g \in F[X]$, we have that $g = g \cdot 1$ so $g \in (f)$. Hence $(f) = F[X]$ since $F[X] \subseteq (f)$. In particular we have $(f) = I = F[X]$.

So assume the degree of f is at least 1. By the division algorithm, for any $g \in I$, it follows that there exists polynomials $q, r \in F[X]$ such that $g = fq + r$ and $\deg(r) < \deg(f)$. Since $g, fq \in I$ it follows that $r = g - fq \in I$. f was picked to the be a non-zero polynomial of minimum degree in I. So $r = 0$ and thus $g = fq \in (f)$ showing that $I \subseteq (f)$ and thus $I = (f)$ is a principal ideal $\square$

We know that $F[X]$ is an integral domain because F is (any field is an integral domain). Consequently $F[X]$ is called a principal ideal domain (aka PID) because it is an integral domain and all ideals are principal.

Consider the ideal $(x^2 + 1)$ in $\mathbb{R}[X]$ (a PID). Let's play around with the quotient ring $\mathbb{R}[X]/(x^2 + 1)$:

For convenience, let's set $I = (x^2 + 1)$. Let $f \in \mathbb{R}[X]$.

If the degree of f is at least two, we can use the division algorithm to find polynomials q, r in $\mathbb{R}[X]$ such that $f = (x^2 + 1)q + r$ and $\deg(r) < 2$. Then $f - r \in (x^2 + 1)$ implies $f + (x^2 + 1) = r + (x^2 + 1)$. So polynomials of degree two or larger aren't needed as coset representatives. Therefore $\mathbb{R}[X]/I = \{a + bx + I | a, b \in \mathbb{R}\}$.

Let's investigate the multiplication in the quotient ring: Let $a + bx + I, c + dx + I \in \mathbb{R}[X]/I$. Then $(a + bx + I)(c + dx + I) = (a + bx)(c + dx) + I = ac + adx + bcx + bdx^2 + I$.

By applying the division algorithm to x^2 divided by $x^2 + 1$ we get $x^2 = (x^2 + 1)(1) - (1)$ which implies that $x^2 + I = -1 + I$.

Using the above we have that $ac + adx + bcx + bdx^2 + I = ac + adx + bcx - bd + I$ since $(ac + adx + bcx + bdx^2) - (ac + adx + bcx - bd) = bd(x^2 + 1) \in I$.

So here is how multiplication works in $\mathbb{R}[X]/I$:

$$(a + bx + I)(c + dx + I) = (ac - bd) + (ad + bc)x + I.$$

Look familiar?

(ELFY) Show that $\phi : \mathbb{C} \to \mathbb{R}[X]/I$ given by $\phi(a + bi) = a + bx + I$ is a ring isomorphism.

Let's look at a finite example. Consider the PID $\mathbb{Z}_2[X]$ and the ideal $I = (x^2 + x + 1)$.

(ELFY) Show that $\mathbb{Z}_2[X]/I = \{0 + I, 1 + I, x + I, x + 1 + I\}$.

Observe that $(x + I)^2 = x^2 + I = x + 1 + I$, $(x + I)^3 = x^2 + x + I = 1 + I$. So the non-zero elements of the commutative quotient ring $\mathbb{Z}_2[X]/I$ is a multiplicative group (the cyclic group of order 3). Thus we have a field $\mathbb{F}_4 = \mathbb{Z}_2[X]/(x^2 + x + 1)$ with 4 elements! It turns out there is a finite field $\mathbb{F}_{p^n}$ of any prime power order.