# MA3218 Applied Algebra

## Basic Number Theory

- **Division algorithm**:
  $\forall a \in \mathbb{R}, b \in \mathbb{N} : \exists! q, r \in \mathbb{Z}$ s.t. $a = bq + r$ and $0 \le r < b$
- **GCD is divisible by other divisors**: $d = \gcd(a,b) \iff$
  $d \mid a$ and $d \mid b$ and $(\forall c : c \mid a \text{ and } c \mid b \implies c \mid d)$
- **GCD is linear combination**:
  $\forall a, b \in \mathbb{Z}^* : d = \gcd(a,b) \implies \exists x, y \in \mathbb{Z}$ s.t. $ax + by = d$
  In particular: $1 = \gcd(a,b) \iff \exists x, y \in \mathbb{Z}$ s.t. $ax + by = 1$
- **Coprime properties**: $\forall a, b, c \in \mathbb{Z}$ :
  $\gcd(a,c) = 1$ and $\gcd(b,c) = 1 \implies \gcd(ab, c) = 1$
  $a \mid bc$ and $\gcd(a,b) = 1 \implies a \mid c$
  $\gcd(a,b) = 1$ and $a \mid c$ and $b \mid c \implies ab \mid c$
- **Multiplicative invertibility**:
  $k \in \mathbb{Z}_n$ and $\gcd(k,n) = 1 \implies \exists x \in \mathbb{Z}_n$ s.t. $kx \equiv 1 \pmod{n}$
  Finding $x$ s.t. $19x \equiv 1 \pmod{391}$:

| | |
|---|---|
| $391 = 19 \times 20 + 11$ | $(7)\,391 + (-144)\,19 = 1$ |
| $19 = 11 \times 1 + 8$ | $(-4)\,19 + (7)\,11 = 1$ |
| $11 = 8 \times 1 + 3$ | $(3)\,11 + (-4)\,8 = 1$ |
| $8 = 3 \times 2 + 2$ | $(-1)\,8 + (3)\,3 = 1$ |
| $3 = 2 \times 1 + 1$ | $(1)\,3 + (-1)\,2 = 1$ |

  $\therefore 19 \times (-144) \equiv 1 \pmod{391}$
  $\therefore x \equiv -144 \equiv 247 \pmod{391}$

## Groups

- **Definition**: Set $G$ with binary op. satisfying:
  0. Closure: Binary operation is well-defined over $G$
  1. Associativity: $\forall a, b, c \in G : (ab)c = a(bc)$
  2. Identity: $\exists e \in G$ s.t. $\forall a \in G, ea = ae = a$
  3. Invertibility: $\forall a \in G : \exists b \in G$ s.t. $ab = ba = e$
- **Abelian group**: Binary op. satisfies commutativity:
  $\forall a, b \in G : ab = ba$
- **Some groups**:
  $\mathbb{Q}^* :=$ multiplicative group of nonzero rationals
  $U(n) := \{m \in \mathbb{Z}_n \mid \gcd(m,n) = 1\} =$ group of units in $\mathbb{Z}_n$
  $Q_8 := \{\pm\mathbf{1}, \pm\mathbf{I}, \pm\mathbf{J}, \pm\mathbf{K}\} =$ quaternion group (non-abelian)
  where $\mathbf{1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{I} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\mathbf{J} = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$, $\mathbf{K} = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$
  $GL_n(F) := \{A \in \mathrm{M}_{n \times n}(F) \mid \det(A) \neq 0\}$ (non-abelian)
  $SL_n(F) := \{A \in \mathrm{M}_{n \times n}(F) \mid \det(A) = 1\}$
  $SL_n(F)$ is a subgroup of $GL_n(F)$
  $T := \{z \in \mathbb{C} \mid |z| = 1\} =$ circle group
- **Product of finite order matrices can have inf. order**:
  $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \implies A^4 = \mathbf{I}$
  $B = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right) \implies B^3 = \mathbf{I}$
  $\forall n \in \mathbb{N} : (AB)^n = \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right) \neq \mathbf{I}$

### Subgroups

- **Basic subgroup test**: Is subset $H$ a subgroup of $G$?
  $\left.\begin{array}{l} e_G \in H \\ \text{Binary op. closed in } H \\ \forall h \in H : h^{-1} \in H \end{array}\right\} \iff H$ is a subgroup of $G$
- **Better subgroup test**: Is subset $H$ a subgroup of $G$?
  $\left.\begin{array}{l} H \neq \varnothing \\ \forall g, h \in H : gh^{-1} \in H \end{array}\right\} \iff H$ is a subgroup of $G$

### Cyclic Groups

- **Definition**: $G$ is cyclic $\iff \exists g \in G$ s.t. $\langle g \rangle = G$
- **Cyclic subgroup generated by a**: $\forall a \in G$ :
  $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\} =$ cyclic subgroup generated by $a$
- Every cyclic group is abelian
- Every subgroup of a cyclic group is cyclic
- **Order of elements**: If $G = \langle a \rangle$ and $n = |G| \neq \infty$ then:
  $\forall 0 \le k \in \mathbb{Z} : o\left(a^k\right) = \frac{n}{\gcd(k,n)}$

- **$n^{\text{th}}$ roots of unity** $= \{z \mid z^n = 1\}$
  $= \left\{\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right) \mid k \in \{0, 1, 2, \ldots, n-1\}\right\}$
  primitive $n^{\text{th}}$ roots of unity $=$ generators of $\{z \mid z^n = 1\}$
  $= \left\{\omega^k \mid \gcd(k,n) = 1\right\}$ where $\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

### Permutation Groups

- $S_X :=$ symmetric group (group of all permutations) of the set $X$; any subgroup of $S_X$ is called a permutation group
- $A_n := \{\sigma \in S_n \mid \sigma \text{ is an even permutation}\}$
  $=$ alternating group on $n$ letters
- **Size of alternating group**: $2\,|A_n| = |S_n|$
- **Transforming a cycle**:
  $\sigma = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \implies \tau\sigma\tau^{-1} = \begin{pmatrix} \tau(x_1) & \cdots & \tau(x_n) \end{pmatrix}$
- $D_n :=$ dihedral group of size n $=$ group of symmetries of a regular $n$-gon $= \{r^x s^y \mid x \in \{0, 1, \ldots, n-1\} \text{ and } y \in \{0,1\}\}$
  where $r^n = id$ and $s^2 = id$ and $srs = r^{-1}$
  $D_n$ is a subgroup of $S_n$
  $D_n = \left\langle r, s \mid r^n = id \text{ and } s^2 = id \text{ and } srs = r^{-1} \right\rangle$
  ($D_n$ is generated by $r$ and $s$ with those relations)
- **Rigid motions** preserve *orientation*; symmetries need not
  (a right hand must remain right in a rigid motion)

## Cosets

- **Definition**: $H$ is any subgroup of $G$. $\forall g \in G$ :
  Left coset containing $g = \{gh \mid h \in H\} = gH$
  Right coset containing $g = \{hg \mid h \in H\} = Hg$
- **Equivalence**:
  $g_1 H = g_2 H \iff g_1 H \subseteq g_2 H \iff g_1 \in g_2 H \iff g_2^{-1} g_1 \in H$
  $\Updownarrow$
  $Hg_1^{-1} = Hg_2^{-1} \iff Hg_1^{-1} \subseteq Hg_2^{-1} \iff g_1^{-1} \in Hg_2^{-1} \iff g_1^{-1} g_2 \in H$
- **Index of a subgroup**: $H$ is any subgroup of $G$ :
  $[G : H] =$ Index of $H$ in $G :=$ number of cosets of $H$ in $G$
- **Lagrange theorem**: $[G : H] = \frac{|G|}{|H|}$  Corollary: $|H| \,\big|\, |G|$
  Corollary: All groups with prime order are cyclic
  Corollary: For finite groups $K \subseteq H \subseteq G$ :
  $[G : K] = [G : H]\,[H : K]$
- **Euler's totient function**: $\varphi : \mathbb{N} \to \mathbb{N}$
  $n \mapsto \begin{cases} 1 & \text{if } n = 1 \\ \text{num. of } m \text{ s.t. } 1 \le m \le n \text{ and } \gcd(m,n) = 1 & \text{otherwise} \end{cases}$
  Note: $|U(n)| = \varphi(n)$
- **Euler's theorem**: $\forall a \in \mathbb{Z}, n \in \mathbb{N}$ where $\gcd(a,n) = 1$ :
  $a^{\varphi(n)} \equiv 1 \pmod{n}$
- **Fermat's little theorem**: $\forall p \in$ primes, $a \in \mathbb{Z}$ where $p \nmid a$ :
  $a^{p-1} \equiv 1 \pmod{p}$

## Cryptography

- **Cryptosystem** $= (\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$
  (plaintexts, ciphertexts, keyspace, encryption rules, decryption rules)
- **Shift cipher**: $e_k(x) \equiv x + k \pmod{n}$
  $d_k(y) \equiv y - k \pmod{n}$
- **Affine cipher**: $key = (a, b)$ where $\gcd(a,n) = 1$
  $e_k(x) \equiv ax + b \pmod{n}$
  $d_k(y) \equiv a^{-1}(y - b) \pmod{n}$
- **Generalized affine cipher**: $key = (A, \mathbf{b})$ where
  $A$ is an invertible matrix and $\mathbf{b}$ is a vector
  $e_k(\mathbf{x}) \equiv \mathbf{x}A + \mathbf{b} \pmod{n}$
  $d_k(\mathbf{y}) \equiv (\mathbf{y} - \mathbf{b})A^{-1} \pmod{n}$
- **RSA**:
  Relies on difficulty of determining $\varphi(n)$ from $n$.
  $n = pq$ (where $p$, $q$ are primes) $\implies \varphi(n) = (p-1)(q-1)$
  $\left.\begin{array}{l} \text{public key} = (n, E) \\ \text{private key} = (D) \end{array}\right\}$ s.t. $DE \equiv 1 \pmod{\varphi(n)}$
  $e_k(x) = x^E$, $d_k(y) = y^D$

## Algebraic Coding Theory

- **Definition**:
  $A = \{a_1, a_2, \ldots, a_q\} =$ set of symbols $=$ code alphabet
  A word of length $n$ over $A$ is a sequence $\mathbf{x} = x_1 x_2 \ldots x_n$ where all $x_i \in A$
  A block code of length $n$ over $A$ is a nonempty subset $C$ of $A^n$
  An element of $C$ is a codeword of $C$
  If $A = \mathbb{Z}_2 = \{0, 1\}$ then $C$ is a binary (block) code
- **Triangle inequality**: $d(\mathbf{x}, \mathbf{y}) \le d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$
- If $d(C) = m$ then: $m - 1$ or fewer errors can be detected, and $\left\lfloor \frac{m-1}{2} \right\rfloor$ or fewer errors can be corrected
- $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$
- **Linear code**: The code alphabet is a finite field $F$, and code $C$ (of length $n$) is a subspace of $F^n$,
  i.e. $C$ is nonempty and $\forall \mathbf{x}, \mathbf{y} \in C$, $\forall a, b \in F : a\mathbf{x} + b\mathbf{y} \in C$
  - If $\dim(C) = m$ then $C$ is called a $[n, m]$-code over $F$
  - Furthermore if $d(C) = d$ then $C$ is a $[n, m, d]$-code over $F$
- **Minimum weight of a code**: $w(C) := \min_{\mathbf{x} \in C \setminus \{\mathbf{0}\}} \{w(\mathbf{x})\}$
- **Generator matrix**: $G = \begin{pmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_m \end{pmatrix} = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & & \vdots \\ g_{m1} & \cdots & g_{mn} \end{pmatrix} \in \mathrm{M}_{m \times n}$
  where $\{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$ is a basis for $C$
  Then $C = \{aG \mid a \in F^m\}$ (i.e. a lin. combin. of rows in $G$)
- **Parity-check matrix**: $H = \begin{pmatrix} \mathbf{h}_1 \\ \vdots \\ \mathbf{h}_{n-m} \end{pmatrix} \in \mathrm{M}_{(n-m) \times n}$
  where $\{\mathbf{h}_1, \ldots, \mathbf{h}_{n-m}\}$ is a basis for the nullspace of $G$
  Then $C = \left\{\mathbf{x} \in F^n \mid H\mathbf{x}^T = \mathbf{0}^T\right\}$
  $\exists \mathbf{c} \in C$ where $w(\mathbf{c}) \le e \iff$
  some $e$ columns of $H$ are linearly dependent
  Single-error-correcting code: In particular, $C$ can correct any single error $\iff$ $H$ has no zero column and no two columns of $H$ are scalar multiple of each other
- **Syndrome**: $s_H(\mathbf{x}) := \left(H\mathbf{x}^T\right)^T \in F^{n-m}$
  If $s_H(\mathbf{x}) = 0$ then no error occurred; if $s_H(\mathbf{x}) = i^{\text{th}}$ column of $H$, then a single error occured at $i^{\text{th}}$ entry of word
- **Syndrome decoding**:
  1. Partition $F^n$ into cosets of $C$
  2. Pick the coset leader (the word $\mathbf{x} \in F^n$ with minimum weight) for each coset
  3. Compute the syndrome of each coset leader (i.e. syndrome look-up table)
  4. For each word $\mathbf{y} \in F^n$ received, use $s_H(\mathbf{y})$ to search the syndrome look-up table for the associated coset leader $\mathbf{e}$, then decode $\mathbf{y}$ to $\mathbf{y} - \mathbf{e}$

## Group Isomorphisms

- **Definition**:
  Bijective mapping where group operation is preserved
- All cyclic groups of infinite order are isomorphic to $\mathbb{Z}$
- All cyclic groups of order $n$ are isomorphic to $\mathbb{Z}_n$
- **Cayley's theorem**: Every group is isomorphic to a permutation group

### Direct Products

- **External direct product**:
  $G \times H :=$ external direct product of groups $G$ and $H$
- **Order of element in external direct product**:
  $\forall (g_1, \ldots, g_n) \in \prod_{s=1}^n G_s$ :
  $o((g_1, \ldots, g_n)) = \operatorname{lcm}\{o(g_1), \ldots, o(g_n)\}$
- **Cyclic group and GCD**:
  $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m,n) = 1$
- **Internal direct product**:
  If $H$, $K$ are subgroups of $G$ s.t.:
  1. $G = HK := \{hk \mid h \in H \text{ and } k \in K\}$
  2. $H \cap K = \{e\}$
  3. $\forall h \in H$, $\forall k \in K : hk = kh$
  Then $G$ is the internal direct product of $H$ and $K$
- **Isomorphism**: Given groups $G$ and $H$ :
  Internal direct product $\cong$ External direct product
- **Internal direct product of $n$ groups**:
  Given group $G$ with subgroups $H_1, \ldots, H_n$ s.t.:
  1. $G = H_1 \cdots H_n := \{h_1 \cdots h_n \mid h_s \in H \text{ where } s \in \{1, \ldots, n\}\}$
  2. $H_s \cap (H_1 \cdots H_{s-1} H_{s+1} \cdots H_n) = \{e\}$ where $s \in \{1, \ldots, n\}$
  3. $\forall h_s \in H_s$, $\forall h_t \in H_t : h_s h_t = h_t h_s$
  Then $G$ is the internal direct product of $H_1, \ldots, H_n$

### Normal Subgroups

- **Definition**: Subgroup $H$ of $G$ is called normal if
  $\forall g \in G : gH = Hg$
  In particular: If $G$ is abelian then all subgroups are normal
- **Equivalence**: $N$ is a normal subgroup of $G$
  $\iff \forall g \in G : gNg^{-1} \subseteq N$
  $\iff \forall g \in G : gNg^{-1} = N$

### Quotient Groups

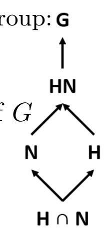
- **Definition**: Given a normal subgroup $N$ of $G$ :
  $G/N := \{gN \mid g \in G\} = \{Ng \mid g \in G\}$
  $G/N$ is a group (of order $[G : N]$) with binary operation $(aN)\,(bN) := abN$
  $G/N$ is called the quotient group of $G$ modulo $N$

### Homomorphisms

- **Definition**: Group operation is preserved
- **Properties of group homomorphisms**:
  $\phi : G \to H$ is a group homomorphism :
  - $\phi(e_G)$ is the identity in H
  - $\forall g \in G : \phi\left(g^{-1}\right) = \phi(g)^{-1}$
  - $K$ is a subgroup of $G \implies \phi[K]$ is a subgroup of $H$
  - $L$ is a subgroup of $H \implies \phi^{-1}[L]$ is a subgroup of $G$
  - $L$ is a normal subgroup $\implies \phi^{-1}[L]$ is a normal subgroup
- **Kernel**: $\ker(\phi) := \{g \in G \mid \phi(g) = e_H\} = \phi^{-1}[\{e_H\}] \subseteq G$
  - $\ker(\phi)$ is a normal subgroup of $G$
  - $\phi$ is injective $\iff \ker(\phi) = \{e_G\}$
- **Canonical/Natural homomorphism**:
  Given a normal subgroup $N$ of $G$ :
  $\phi : G \to G/N$
  $g \mapsto gN$
  is the canonical/natural homomorphism

### Isomorphism Theorems

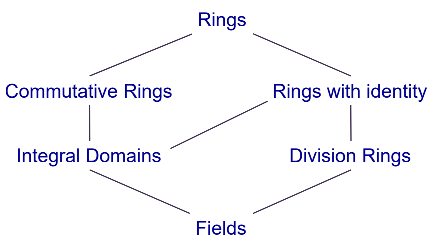
- **First isomorphism theorem**:
  $\phi : G \to H$ is a group homomorphism : $\phi[G] \cong G/\ker(\phi)$
- **Second isomorphism theorem**: Arrow=subgroup:
  $H$ is a (not necessarily normal) subgroup of $G$, and $N$ is a normal subgroup of $G$ :
  - $HN := \{hn \mid h \in H \text{ and } n \in N\}$ is a subgroup of $G$
  - $H \cap N$ is a normal subgroup of $H$
  - $H/(H \cap N) \cong (HN)/N$




- **Third isomorphism theorem**:
  $H$, $N$ are normal subgroups of $G$ s.t. $N \subseteq H$ :
  - $H/N$ is a normal subgroup of $G/N$
  - $G/H \cong (G/N)\,/\,(H/N)$

# Rings

- **Definition**: Abelian group $R$ with additional properties:
  - Multiplication is associative: $\forall a,b,c \in R : (ab)c = a(bc)$
  - Addition and multiplication satisfy distributive laws:
    $\forall a,b,c \in R : \ a(b+c) = ab + ac$ and $(b+c)a = ba + ca$
- **Special rings**:
  Ring with identity: $\exists 1 \in R$ s.t. $\forall a \in R : a1 = a = 1a$
  Commutative ring: multiplication is commutative
  Integral domain: commutative ring with identity s.t.
  $\forall a,b \in R : \ (ab = 0 \implies a = 0$ or $b = 0)$
  Division ring: ring with identity s.t.
  $\forall a \in R \setminus \{0\} : a$ is a unit
  (i.e. $\exists a^{-1} \in R$ s.t. $aa^{-1} = 1 = a^{-1}a$)
  Field: commutative division ring




- **Some rings**: $\forall n \in \mathbb{N} : \mathbb{Z}_n$ is commutative ring with identity
  $n$ is composite $\implies \mathbb{Z}_n$ is not an integral domain
  $\mathrm{M}_{n \times n}(F)$ is a (non-commutative) ring with identity
  $Q_8$ is a (non-commutative) division ring
  $\mathbb{Z} \times 2\mathbb{Z}$ is a ring without identity that has
  a subring $\mathbb{Z} \times \{0\}$ with identity $(1,0)$
- **Zero divisors**: If $a \neq 0$ and $b \neq 0$ but $ab = 0$ then:
  $a$ is a left zero divisor and $b$ is a right zero divisor

  An element that is both a left and right zero divisor
  is called a zero divisor

## Subrings

- **Definition**: A subring $S$ or a ring $R$ is a subset of $R$ s.t. it is a ring using the same addition and multiplication of $R$
- **Subring test**: Is subset $S$ a subring of $R$?
  $$\left.\begin{array}{l} S \neq \varnothing \\ \forall r,s \in S : r - s \in S \\ \forall r,s \in S : rs \in S \end{array}\right\} \iff S \text{ is a subring of } R$$

## Cancellation Law

- Let $D$ is a commutative ring with identity :
  $$D \text{ is an integral domain} \iff \begin{array}{c} \forall a,b,c \in D \text{ with } a \neq 0 : \\ ab = ac \implies b = c \end{array}$$
- **Finite integral domain**:
  Every finite integral domain is a field

## Characteristic of a Ring

- **Definition**: $\mathrm{char}(R) :=$ smallest $n \in \mathbb{N}$ s.t. $\forall a \in R : na = 0$
  where $na := \underbrace{a + a + \cdots + a}_{n \text{ times}}$

  If no such $n$ exists, then $\mathrm{char}(R) := 0$
- **Rings with identity**: In any ring with identity $R$ :
  $o(1) = n \neq \infty \implies \mathrm{char}(R) = n$
  (additive order)
- **Integral domain**: In any integral domain $R$ :
  $\mathrm{char}(R)$ is prime or zero

# Ring Homomorphisms and Ideals

## Ring Homomorphisms

- **Definition**: Addition and multiplication are preserved
- **Properties**: Given a ring homomorphism $\phi \colon R \to S$ :
  - $\phi[R]$ is a subring of $S$
  - $R$ is commutative $\implies \phi[R]$ is commutative
  - $\phi(0_R) = 0_S$
  - Suppose $R$ and $S$ have identities $1_R$ and $1_S$ resp. :
    $\phi$ is surjective $\implies \phi(1_R) = 1_S$
  - Suppose $R$ is a field : $\phi[R] \neq \{0\} \implies \phi[R]$ is a field

## Ideals

- **Definition**: An ideal $I$ of a ring $R$ is a subring of $R$ s.t.
  $\forall r \in R : rI \subseteq I$ and $Ir \subseteq I$
- **Trivial ideals of $R$**: $\{0\}$ and $R$
- **Proper ideals of $R$**: All ideals that are not $R$ itself
- **Ideal test**: Is subset $I$ of $R$ an ideal?
  $$\left.\begin{array}{l} I \neq \varnothing \\ \forall a,b \in I : a - b \in I \\ \forall a \in I \text{ and } r \in R : ra, ar \in I \end{array}\right\} \iff I \text{ is an ideal}$$
- **Principal ideal**: Let $R$ be a commutative ring with identity : Principal ideal of $a \in R := aR$ (it is an ideal)
- **Ideals of $\mathbb{Z}$**: Every ideal of $\mathbb{Z}$ is a principal ideal
- **Kernels of ring homomorphisms**:
  Given any ring homomorphism $\phi$ : $\ker(\phi)$ is an ideal

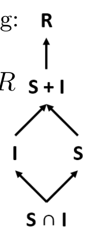
## Quotient Rings

- **Definition**: Given any ideal $I$ of ring $R$ :
  $R/I := \{r + I \mid r \in R\}$ is the quotient ring of $R$ modulo $I$

  $R/I$ is a ring with these operations:
  $(r + I) + (s + I) := (r + s) + I$
  $(r + I)\,(s + I) := rs + I$
- **Canonical/Natural homomorphism**:
  Given an ideal $I$ of $R$ :
  $$\phi \colon R \to R/I$$
  $$r \mapsto r + I$$
  is the canonical/natural homomorphism

## Isomorphism Theorems

- **First isomorphism theorem**:
  $\phi \colon R \to S$ is a ring homomorphism : $\phi[R] \cong R/\ker(\phi)$
- **Second isomorphism theorem**: Arrow=subring:
  $S$ is a subring of $R$, and $I$ is an ideal of $R$ :
  - $S + I := \{s + a \mid s \in S$ and $a \in I\}$ is a subring of $R$
  - $S \cap I$ is an ideal of $S$
  - $S/(S \cap I) \cong (S + I)/I$




- **Third isomorphism theorem**:
  $I$, $J$ are ideals of $R$ s.t. $J \subseteq I$ :
  - $I/J$ is an ideal of $R/J$
  - $R/I \cong (R/J)\,/\,(I/J)$




## Maximal and Prime Ideals

- **Maximal ideal**: A proper ideal $M$ of a ring $R$ is a maximal ideal if $M$ is not a proper subset of any ideal of $R$ except $R$ itself
  i.e. $I$ is an ideal of $R$ s.t. $M \subseteq I \implies I = M$ or $I = R$

  All rings with identity have at least one maximal ideal
- **Field from maximal ideal**: Let $R$ be a commutative ring with identity and $M$ an ideal of $R$ :
  $M$ is a maximal ideal $\iff R/M$ is a field
- **Prime ideal**: A proper ideal $P$ of a ring $R$ is a prime ideal if $\forall a,b, \in R : \quad ab \in P \implies a \in P$ or $b \in P$
- **Integral domain from prime ideal**: Let $R$ be a commutative ring with identity and $P$ and ideal of $R$ :
  $P$ is a prime ideal $\iff R/P$ is an integral domain
- **Maximal $\to$ Prime**: Every maximal ideal in a commutative ring with identity is also a prime ideal
- **Prime ideal that is not maximal**:
  Given an integral domain $R$ that is not a field,
  $R[x]/xR[x] \cong R$ is an integral domain that is not a field,
  so $xR[x]$ is a prime ideal but not a maximal ideal

## Chinese Remainder Theorem

- **Definition**: $\forall n_1, n_2, \ldots, n_k \in \mathbb{N}$ with no common factors
  (i.e. $\forall s \neq t : \ \gcd(n_s, n_t) = 1$) :
  Let $n = n_1 n_2 \ldots n_k$. Then:
  $$\phi \colon \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$
  $$x \mapsto (x \pmod{n_1}, x \pmod{n_2}, \ldots, x \pmod{n_k})$$
  is an isomorphism

  $\therefore \mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$

# Polynomials

$R$ is a commutative ring with identity, $F$ is a field

- **Monic**: leading coefficient is 1
- Degree of zero polynomial is $-\infty$
- $R$ is a commutative ring with identity $\implies R[x]$ is a commutative ring with identity
- $R$ is an integral domain $\implies R[x]$ is an integral domain
- **Evaluation mapping**: $\phi_\alpha \colon R[x] \to R$
  $$p(x) \mapsto p(\alpha)$$
  The evaluation mapping is a ring homomorphism
- **Division algorithm**: $\forall f(x), g(x) \in F[x]$ :
  $\exists! q(x), r(x) \in F[x]$ s.t.
  $f(x) = q(x)g(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$
- **Number of roots**: $\forall 0 \neq p(x) \in F[x]$
  $\deg(p(x)) = n \implies p(x)$ has at most $n$ roots in $F$
- **GCD**: Monic polynomial of highest degree that is a divisor of both polynomials; use the Euclidean algorithm to find
- **GCD is linear combination**: $\forall f(x), g(x) \in F$ :
  $d(x) = \gcd(f(x), g(x)) \implies$
  $\exists a(x), b(x) \in \mathbb{Z}$ s.t. $a(x)f(x) + b(x)g(x) = d(x)$
- **Reducibility**: $f(x) \in F[x]$ is reducible over $F$ if $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ where $0 < \deg(g(x)) < \deg(f(x))$ and $0 < \deg(h(x)) < \deg(f(x))$
- **Principal ideals**: Every ideal of $F[x]$ is principal
- **Maximal ideals**: $\forall p(x) \in F[x]$ (not necessarily monic) :
  $p(x)F(x)$ is maximal ideal $\iff p(x)$ is irreducible over $F$
- **Modulo arithmetic**:
  $F[x; p(x)] := \{f(x) \in F(x) \mid \deg(f(x)) < \deg(p(x))\}$ (with usual addition, and multiplication modulo $p(x)$) is a commutative ring with identity

  Furthermore, $F[x; p(x)] \cong F[x]/p(x)F[x]$
- **Algebraic extension** of fields:
  The polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}$.
  As $\sqrt{2}$ is a root of $x^2 - 2$,
  $\mathbb{Q}(\sqrt{2}) := \{a\sqrt{2} + b \mid a, b \in \mathbb{Q}\}$ is an extension field of $\mathbb{Q}$.

# Finite Fields

- $\mathbb{Z}_p$ is a finite field $\iff p$ is prime $\implies \mathbb{Z}_p^\star$ is cyclic
- **Characteristic** of a finite field is prime
- **Order** (num. of elements) of a finite field is a prime power
- **Polynomial $x^q - x$**: Let $F$ be a finite field of order $q$ :
  $(\forall \beta \in F : \beta^q = \beta)$ and $\prod_{\beta \in F} (x - \beta) \equiv x^q - x$
- **Existence and uniqueness**:
  $\forall p \in$ primes and $k \in \mathbb{N}$ : there exists a unique (i.e. isomorphic) finite field of order $p^k$, denoted as $GF(q)$ or $\mathbb{F}_q$
- **Constructing a finite field of order $p^k$**:
  If $k = 1$, just take $\mathbb{F}_p = \mathbb{Z}_p$
  Else:
  1. Find a monic irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $k$, i.e. $f(x) = x^k + r_{k-1}x^{k-1} + \cdots + r_1 x + r_0$ where $r_0, r_1, \ldots, r_{k-1} \in \mathbb{F}_p$
  2. Let $\beta$ be a new element such that $f(\beta) = 0$, i.e. $\beta^k = -\left(r_{k-1}\beta^{k-1} + \cdots + r_1\beta + r_0\right)$
  3. Then $\mathbb{F}_{p^k} = \mathbb{F}_p(\beta) :=$ $\left\{s_{k-1}\beta^{k-1} + \cdots + s_1\beta + r_0 \mid s_0, s_1, \ldots, s_{k-1} \in F_p\right\}$ is a field of order $p^k$
- **Primitive element**: Given a finite field $F$ :
  the (multiplicative) group $F^\star := F \setminus \{0\}$ is cyclic

  A generator of $F^\star$ is called a primitive element of $F$
- $F$ has order $q$ and $\alpha$ is a primitive element of $F$ :
  $\prod_{s=0}^{q-2} (x - \alpha^s) \equiv x^{q-1} - 1$
- **Primitive polynomial**: Given a finite field $F_0$ :
  $f(x) \in F_0[x]$ is a primitive polynomial over $F$ if:
  1. $f(x)$ is irreducible over $F_0$, and
  2. $\alpha$ is a zero of $f(x) \implies \alpha$ is a primitive element of $F_0(\alpha)$

# Cyclic codes

- **Definition**: $C \in F^n$ is a cyclic code if:
  1. $C$ is a linear code, and
  2. $\mathbf{c} = c_0 c_1 c_2 \ldots c_{n-1}$ is a codeword $\implies$
     cyclic shift $s(\mathbf{c}) := c_{n-1} c_0 c_1 \ldots c_{n-2}$ is also a codeword
- **Polynomial representation**:
  A word $\mathbf{a} = a_0 a_1 \ldots d_{n-1} \in F^n$ is represented by
  $a(x) := a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in F[x; x^n - 1]$

  This mapping is a vector space isomorphism
- **Cyclic code $\leftrightarrow$ ideal**: $C \subseteq F^n$ is a cyclic code $\iff$
  $C' := \{c(x) \mid \mathbf{c} \in C\}$ is an ideal of $F[x; x^n - 1]$
- **Generator polynomial**: Let $C \subseteq F^n$ and
  $C' := \{c(x) \mid \mathbf{c} \in C\} \subseteq F[x; x^n - 1]$ :
  $C$ is a cyclic $[n,\, k]$-code $\iff \exists$ monic $g(x) \in F[x]$ s.t.
  $$\begin{cases} g(x) \mid x^n - 1 \\ \deg(g(x)) = n - k \\ C' = \{f(x)g(x) \mid f(x) \in F[x] \text{ and } \deg(f(x)) \leq k - 1\} \end{cases}$$
- Given a cyclic code $C$, the monic polynomial in $C'$ with least degree is the generator polynomial
- **Constructing cyclic code from generator polynomial**:
  To construct a cyclic $[n,\, k]$-code $C$:
  1. find a polynomial of degree $n - k$ that divides $x^n - 1$
  2. Use it as the generator polynomial
- **Constructing generator and parity check matrices**:
  Given a generator poly. $g(x) = a_0 + a_1 x + \cdots + a_{n-k}x^{n-k}$ with $\deg(g(x)) = n - k$ :
  $$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_{n-k} & 0 & \cdots & 0 & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & a_0 & a_1 & \cdots & \cdots & a_{n-k} \end{pmatrix}$$
  $$H = \begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{n-k-1}h_R(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 & 0 \\ 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{pmatrix}$$
  where $h(x) := \frac{(x^n - 1)}{g(x)} = h_0 + h_1 x + \cdots + h_k x^k$ is the parity check polynomial, and $h_R(x)$ is coef.-reversed monic of $h(x)$

## Reed-Solomon Codes

- **Definition**: Given a finite field $F$ of order $q$, and $\alpha$ a primitive element of $F$ :
  $g(x) := \left(x - \alpha^{a+1}\right)\left(x - \alpha^{a+2}\right) \cdots \left(x - \alpha^{a+\delta-1}\right)$ (where $2 \leq \delta \leq q - 1$) is a generator polynomial (of degree $\delta - 1$) for a cyclic $[q - 1, q - \delta]$-code over $F$

  It is a Reed-Solomon code, denoted by $\mathrm{RS}\,(q - 1, q - \delta)$
- **Minimum distance**:
  $C$ is a Reed-Solomon code $\mathrm{RS}(q - 1, q - \delta)$ : $d(C) = \delta$