GRUPPO:
sia $G \neq \phi$, $\cdot$ un'operazione da $G \times G \to G$ t.c.
i) $\cdot$ è associativa
ii) $\exists e_G \in G$ t.c. $ge_G = e_G g = g$ $\forall g \in G$ esiste un elemento neutro
iii) $\forall g \in G$ $\exists g^{-1} \in G$ t.c. $gg^{-1} = g^{-1}g = e_G$ esiste un inverso,
allora $(G, \cdot)$ si dice gruppo.
Inoltre se $\forall g, h \in G$ vale $gh = hg$, $(G, \cdot)$ si dice gruppo abeliano

GRUPPO QUOZIENTE:
sia G gruppo e $\sim$ una rel. di eq. compatibile, si dice gruppo quoziente il gruppo $(G/_\sim, \cdot_\sim)$ dove $\cdot_\sim$ è un'operazione t.c.
$[a]_\sim \cdot_\sim [b]_\sim = [ab]_\sim$

ANELLO:
sia $A \neq \phi$,
$(A, +)$ un gruppo abeliano,
$\cdot$ un'operazione interna e associativa e $+, \cdot$ siano legate da $\forall a, b, c \in A$
i) $a(b+c) = ab + ac$
ii) $(a+b)c = ac + bc$,
allora A si dice anello.
Se $\cdot$ ammette neutro (1_A) e è commutativa $(ab = ba)$ allora A si dice anello unitario commutativo

CARATTERISTICA:
sia $(A, +, \cdot)$ un anello commutativo unitario, posto 1_A il neutro per il prodotto si definisce caratteristica di A l'ordine di 1_A in $(A, +)$, se tale ordine è infinito la caratteristica è 0

LATERALI:
sia G gruppo, H sottogruppo di G l'insieme $gH = \{gh \mid h \in H\}$ con $g \in G$ si dice laterale sinistro, l'insieme $Hg = \{hg \mid h \in H\}$ con $g \in G$ si dice laterale destro.
Se $gH = Hg$ allora H si dice sottogruppo normale

OMOMORFISMO DI GRUPPI:
siano $(G, +)$, $(B, \oplus)$ due gruppi una funzione $\varphi: G \to B$ t.c.
$\varphi(a+b) = \varphi(a) \oplus \varphi(b)$ $\forall a, b \in G$ si dice omomorfismo di gruppi

NUCLEO:
sia $\varphi: A \to B$ omom. di gruppi, si dice nucleo di φ l'insieme
$Ker\varphi = \{a \in A \mid \varphi(A) = e_B\}$

IDEALI:
sia A anello se per $I \subseteq A$ vale
i) $(I, +)$ sottogruppo di A
ii) $\forall a \in A, i \in I$ si ha $ai \in I$
allora I si dice ideale sinistro di A.
Se al posto di ii) c'è
j) $\forall a \in A, i \in I$ si ha $ia \in I$
allora I si dice ideale destro di A.
Se I è ideale sia destro che sinistro, I si dice ideale di A

OMOMORFISMO DI FROBENIUS:
sia K un campo di caratteristica p primo.
L'applicazione $\varphi: K \to K$ t.c. $\varphi(a) = a^p$ $\forall a \in K$ si dice omomorfismo di Frobenius

CAMPO PERFETTO:
sia K campo e φ l'om. di Frobenius. Se φ è isomorfismo K si dice campo perfetto e φ si dice automorfismo di Frobenius

SOTTOGRUPPI CONIUGATI:
sia G gruppo, H e K due sottogruppi di G se esiste $g \in G$ t.c. $H = gKg^{-1}$ dove $gKg^{-1} = \{gmg^{-1} \mid m \in K\}$ allora H e K si dicono sottogruppi coniugati rispetto a g

SOTTOGRUPPO GENERATO:
sia $(G, \cdot)$ gruppo, $g \in G$ si dice sottogruppo generato da g l'insieme $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$

GRUPPO CICLICO:
un gruppo G si dice ciclico se $\exists g \in G$ t.c. $\langle g \rangle = G$

ANELLO QUOZIENTE:
sia A anello e $\sim$ una rel. d'eq. compatibile si definisce l'anello quoziente
$A/_\sim = \{[a]_\sim \mid a \in A\}$ con le operazioni
i) $[a]_\sim +_\sim [b]_\sim = [a+b]_\sim$
ii) $[a]_\sim \cdot_\sim [b]_\sim = [ab]_\sim$ $\forall [a]_\sim, [b]_\sim \in A/_\sim$

DOMINIO D'INTEGRITÀ:
sia A anello unitario commutativo se $\forall x, y \in A$ vale $xy = 0 \Rightarrow x = 0 \vee y = 0$ allora A si dice dominio d'integrità

CAMPO:
sia A anello commutativo unitario, se $\forall a \in A^* \exists \bar{a}' \in A^*$ t.c. $a\bar{a}' = 1_A$ allora A si dice campo, dove $A^* = A \setminus \{0\}$

DERIVATO DI UN POLINOMIO:
sia $A_{[x]}$ anello dei polinomi e $A_{[x]} \ni f = a_0 + a_1x + \ldots + a_nx^n$. Il polinomio $Df = a_1 + 2a_2x + \ldots + na_nx^{n-1}$ si dice derivato del polinomio f

PRIMITIVO:
sia $f = a_0 + a_1x + \ldots + a_nx^n$ un polinomio se $MCD(a_0, a_1, \ldots, a_n) = 1$, ossia se i suoi coefficienti sono coprimi tra loro allora f si dice primitivo

ELEMENTO PRIMITIVO:

ORDINE DI UN GRUPPO:
il numero di elementi di G gruppo si definisce ordine di G e si indica con $|G|$

ORDINE DI UN ELEMENTO:
sia G gruppo, $g \in G$ si dice ordine di G il numero $0 < n \in \mathbb{N}$ t.c. $g^n = e_G$;
se tale n non esiste l'ordine di g si dice infinito

OMOMORFISMO DI ANELLI
siano $(A, +, \cdot)$ e $(B, \oplus, \odot)$ due anelli, una funzione $f: A \to B$ t.c.
i) $f(a+b) = f(a) \oplus f(b)$
ii) $f(ab) = f(a) \odot f(b)$ $\forall a, b \in A$
si dice omomorfismo di anelli

IDEALE GENERATO:
sia A anello e $X \subseteq A$ un suo sottinsieme.
Si dice ideale generato da X il più piccolo ideale di A che contiene X, e si indica con (X)

IDEALE PRINCIPALE:
se I ideale è generato da un solo elemento, tale ideale si dice principale e si denota (x)

IDEALE MASSIMALE:
un ideale I si dice massimale se $\exists J$ ideale t.c. $I \subseteq J \Rightarrow I = J \vee J = A$

IDEALE PRIMO:
un ideale I si dice primo se $\forall a, b \in A$, $ab \in I \Rightarrow a \in I \vee b \in I$

ANELLO GENERATO:
sia B anello e $A \subseteq B$ sottoanello, siano $b_1, \ldots, b_n \in B$. Il più piccolo anello $\bar{A}$ t.c. $A \cup \{b_1, \ldots, b_n\} \subseteq \bar{A}$ è della forma
$\bar{A} = \{\sum_{i_1, \ldots, i_n \in I} a_{i_1 \ldots i_n} b_1^{i_1} \cdots b_n^{i_n} \mid a_{i_1 \ldots i_n} \in A\}$
e si denota con $A[b_1, \ldots, b_n] = \bar{A}$

PARTIZIONE:
una famiglia $\{A_i\}_{i \in I}$ di sottoinsiemi di X insieme si dice partizione se:
i) $A_i \neq \phi$ $\forall i \in I$
ii) $\bigcup_{i \in I} A_i = X$
iii) $A_i \cap A_j = \phi$ $\forall i \neq j$

DOMINIO A IDEALI PRINCIPALI:
sia A dominio d'integrità, se ogni ideale di A è principale A si dice dominio a ideali principali (PID)

ELEMENTO UNITARIO:
sia A un anello, un elemento $a \in A$ si dice unitario o invertibile se $\exists \bar{a}^1 \in A$ t.c. $a\bar{a}^1 = 1_A$

IRRIDUCIBILE:
sia A dominio d'integrità, sia $0 \neq a \in A$ un elemento t.c.
se $a = f \cdot g \Rightarrow f$ unitario $\vee$ g unitario,
un tale elemento è detto irriducibile

PRIMO:
sia A dominio d'integrità, sia $0 \neq a \in A$ un elemento t.c.
se $a \mid f \cdot g \Rightarrow a \mid f \vee a \mid g$,
un tale elemento è detto primo

MASSIMO COMUN DIVISORE:
sia A dominio d'integrità, $a, b \in A$, si dice massimo comun divisore di a, b un elemento $d \in A$ t.c. $d \mid a$, $d \mid b$ e $\forall \delta \in A$ t.c. $\delta \mid a$ e $\delta \mid b \Rightarrow \delta \mid d$

ESTENSIONE:
sia L campo e $L \supseteq K$ sottocampo.
L si dice estensione di K e si scrive $L:K$

ELEMENTI ALGEBRICI E TRANS:
siano L e K due campi t.c. $L:K$.
Un elemento $a \in L$ si dice:
i) algebrico su K se $\exists f \in K[x]$, $f \neq 0$ t.c. $f(a) = 0$ (f ha coefficienti in K)
ii) trascendente su K se $\nexists f \in K[x]$, $f \neq 0$ t.c. $f(a) = 0$ (f ha coefficienti in K)

RELAZIONE:
siano X e Y due insiemi, un sottoinsieme $\mathcal{R} \subseteq X \times Y$ si dice relazione su X e Y, la coppia $(a, b) \in \mathcal{R} \subseteq X \times Y$ si denota con $a\mathcal{R}b$

ELEMENTI ASSOCIATI:
sia A dominio d'integrità, $a, b \in A$ si dicono associati se $\exists u \in A$ unitario t.c. $a = ub$

COPRIMI:
due elementi $a, b \in \mathbb{Z}$ si dicono coprimi se non hanno fattori comuni, ossia $MCD(a, b) = 1$

GRUPPO DI INVERTIBILI DI $\mathbb{Z}_m$:
sia $m \in \mathbb{N}$ si definisce
$U_m = \{[a]_{\rho_m} \in \mathbb{Z}_m \mid \exists [a^{-1}]_{\rho_m}\}$

FUNZIONE DI EULERO:
sia $|U_m|$ la cardinalità degli invertibili di $\mathbb{Z}_m$ definendo $\varphi: \mathbb{N}^* \to \mathbb{N}^*$, dove $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, come
$\varphi(1) = 1$
$\varphi(n) = |U_n|$
tale funzione è detta funzione di Eulero

MASSIMO COMUN DIVISORE:
siano $f, g \in K_{[x]}$, il polinomio $d \in K_{[x]}$ t.c. $d \mid f$, $d \mid g$ e $\forall \delta \in K_{[x]}$ t.c. $\delta \mid f, \delta \mid g \Rightarrow \delta \mid d$ si dice massimo comun divisore

POLINOMIO MINIMO:
sia K campo e $a \in K$ un elemento algebrico allora un polinomio di grado minimo che si annulle in a si dice polinomio minimo

GRADO DELL'ESTENSIONE:
la dimensione di L come K-spazio vettoriale si dice grado dell'estensione e si indica con $[L:K]$

ESTENSIONE ALGEBRICA:
siano K e L due campi t.c. $L:K$,
L si dice estensione algebrica di K se $\forall a \in L$ a è algebrico su K

RELAZIONE D'EQUIVALENZA:
sia X insieme, una relazione $\sim$ su $X \times X$ si dice di equivalenza se $\forall x, y, z \in X$
i) $x \sim x$ (riflessiva)
ii) $x \sim y \Rightarrow y \sim x$ (simmetrica)
iii) $x \sim y, y \sim z \Rightarrow x \sim z$ (transitiva)
se $(G, \cdot)$ è un gruppo, una rel. di eq. si dice compatibile se dati $a \sim b$ e $c \sim d \Rightarrow a \cdot c \sim b \cdot d$

P-GRUPPO:
sia p primo e $\alpha \in \mathbb{N}$, un gruppo finito di ordine p^α si dice p-gruppo

P-SOTTOGRUPPO DI SYLOW:
sia G un gruppo finito di ordine n, sia p primo e $\alpha \in \mathbb{N}$ t.c. $p^\alpha \mid n$ e $p^{\alpha+1} \nmid n$, un p-sottogruppo di G di ordine p^α si dice p-sottogruppo di Sylow

OMOMORFISMO DI VALUTAZIONE:
sia A anello, $A[x]$ e $a \in A$ fissato, l'omomorfismo $v_a: A[x] \to A$ definito da $(a_0 + a_1x + \ldots + a_nx^n) \to (a_0 + a_1a + \ldots + a_na^n)$ si dice omomorfismo di valutazione

CONGRUENZA MODULO f:
siano $f, g, h \in K_{[x]}$ tre polinomi.
Si dice che g è congruo ad h modulo f
$g \equiv h \mod f$ se $\exists a \in K_{[x]}$ t.c. $a = f \mid (g - h)$

COPRIMI:
due polinomi $f, g \in K_{[x]}$ t.c. $deg(MCD(f, g)) = 0$ si dicono coprimi

GRADO RELATIVO ALLA VARIABILE:
sia $f \in A[x_1, \ldots, x_n]$ un polinomio in n variabili si definisce grado relativo alla variabile x_i di f il grado di $f \in (A[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n])[x_i]$

GRADO GLOBALE:
sia $f \in A[x_1, \ldots, x_n]$ un polinomio in n variabili si definisce grado globale di f la somma di tutti i gradi relativi di x_i, $i = \{1 \ldots n\}$

CAMPO DI SPEZZAMENTO:
sia K campo e $K[x] \ni f$ un polinomio l'estensione $L:K$ t.c. f si spezza in fattori lineari si dice campo di spezzamento per f o campo di riducibilità completa

CLASSI DI EQUIVALENZA e QUOZIENTE:
sia X insieme e $\sim$ una relazione d'equivalenza su X, si dicono classi di equivalenza gli insiemi $[a]_\sim = \{x \in X \mid x \sim a\}$.
L'insieme $X/_\sim = \{[a]_\sim \mid a \in X\}$ si dice quoziente di X

PRODOTTO DI CAUCHY:
sia A anello commutativo unitario, $B := \{(a_n)_n \mid a_n \in A$ e $\exists \bar{n} \in \mathbb{N}$ t.c. $a_n = 0$ $\forall n > \bar{n}\}$
si definisce in B un prodotto $\cdot$ t.c. $(a_n)_n \cdot (b_n)_n = (c_n)_n$ dove, $\forall i$ $c_i = \sum_{j=0}^{i} a_j b_{i-j}$,
tale prodotto si definisce prodotto di Cauchy

ANELLO DEI POLINOMI:
sia A anello commutativo unitario, $B = \{(a_n)_n \mid a_n \in \mathbb{N} \wedge \exists \bar{n} \in \mathbb{N}$ t.c. $a_n = 0$ $\forall n > \bar{n}\}$,
definendo $1 = x^0 = (1, 0, 0, \ldots)$, $x = (0, 1, 0, \ldots)$, $x^2 = (0, 0, 1, 0, \ldots)$ ecc, in cui x^n indica un 1 in posizione $(n+1)$esima, allora ogni elemento $(a_n)_n \in B$ riscritto in forma esplicita $(a_0, a_1, a_2, \ldots, a_n, 0, \ldots)$ si può scrivere come
$(a_0, 0, \ldots) \cdot (1, 0, \ldots) = (a_0, 0, \ldots)$
$(a_1, 0, \ldots) \cdot (0, 1, 0, \ldots) = (0, a_1, 0 \ldots)$
$(a_2, 0, 0) \cdot (0, 0, 1, 0, \ldots) = (0, 0, a_2, 0 \ldots)$
$\vdots$
$(a_n, 0, \ldots) \cdot (0, \ldots, 1, 0) = (0, \ldots a_n, 0 \ldots)$ dove 1 e a_n stanno in posizione $(n+1)$esima
da cui è naturale identificare $(a_0, a_1, \ldots, a_n, 0, \ldots) = a_0 + a_1x + \ldots + a_nx^n$
tale identificazione dà origine all'anello dei polinomi a coefficienti in A con variabile x, ossia $A[x]$

DOMINIO A FATTORIZZAZIONE UNICA (UFD)
sia A dominio d'integrità, se $\forall a \in A$ t.c. $0 \neq a$ e a non è unitario a si può scrivere come prodotto di irriducibili in modo unico a meno di permutazioni e associati allora A si dice dominio a fattorizzazione unica.
Se $a = f_1 \cdots f_n = g_1 \cdots g_m \Rightarrow m = n$ e $\exists \sigma$ permutazione t.c. f_i è associato a $g_{\sigma(i)}$

ANELLO DEI POLINOMI IN DUE VARIABILI:
sia A un anello e $A' = A_{[x]}$ un anello dei polinomi nella variabile x.
L'anello dei polinomi $A'_{[y]}$ ha elementi $b_0 + b_1y + \ldots + b_ny^n$ dove
$b_0 = a_{00} + a_{10}x + \ldots$
$\vdots$
$b_n = a_{0n} + a_{1n}x + \ldots$
quindi un generico polinomio $f \in A'_{[y]}$ è nella forma $f = (a_{00} + a_{10}x + \ldots) + (a_{01} + a_{11}x + a_{21}x^2 + \ldots)y + \ldots + (a_{0n} + a_{1n}x + \ldots)y^n = \sum_{i,j \in I} a_{ij}x^iy^j$ dove $0 \leq j \leq n$
l'anello così costruito si denota $A[x, y]$ e si chiama anello dei polinomi in due variabili

CAMPO DI GALOIS:
l'unico (a meno di isomorfismi) campo finito di p^n elementi si dice campo di Galois di p^n elementi e si scrive $GF(p, n)$