

**Corso di Laurea in Matematica**  
**Programma di Algebra n.1 – a.a. 2021/2022**  
**Prof.ssa Margherita Barile**

**Insiemi e relazioni:**

Relazioni, relazioni funzionali, applicazioni iniettive, surgettive, bigettive. Composizione di applicazioni, applicazioni invertibili. Relazioni di equivalenza, classi di equivalenza, insieme quoziente, sistema completo di rappresentanti. Relazioni d'ordine.

**Gli insiemi numerici:**

Una presentazione di  $\mathbb{N}$ , il principio di induzione, le dimostrazioni per induzione. Il principio del minimo. La relazione di divisibilità in  $\mathbb{N}$ , i numeri primi. L'algoritmo di divisione euclidea in  $\mathbb{Z}$ . La relazione di divisibilità in  $\mathbb{Z}$ . Il M.C.D. e l'identità di Bézout, l'algoritmo delle divisioni successive. Il teorema fondamentale dell'aritmetica. Il teorema di Euclide sull'infinità dei numeri primi. I numeri complessi come coppie ordinate di numeri reali, operazioni in  $\mathbb{C}$ , forma algebrica e forma trigonometrica, le radici  $n$ -esime di un numero complesso, l'enunciato del teorema fondamentale dell'algebra.

**Strutture algebriche ed omomorfismi:**

Gruppi e loro proprietà elementari, gruppi abeliani, sottogruppi, gruppi ciclici e loro generatori, periodo di un elemento, il teorema di Lagrange sul periodo degli elementi di un gruppo abeliano finito. Anelli e loro proprietà elementari, anelli commutativi, anelli unitari, elementi invertibili, domini di integrità, campi, sottoanelli, sottocampi. Anelli di matrici. Prodotto diretto di gruppi e di anelli. Omomorfismi, monomorfismi, epimorfismi, isomorfismi, nucleo di un omomorfismo.

**L'anello dei polinomi:**

Polinomi, grado di un polinomio. Operazioni tra polinomi. Polinomi a coefficienti in un dominio, la formula del grado. L'algoritmo della divisione euclidea tra polinomi in  $K[x]$ . Il M.C.D. e l'identità di Bézout, l'algoritmo delle divisioni successive. Radici di un polinomio, il criterio di Ruffini. Polinomi irriducibili e fattorizzazione, polinomi associati, polinomi monici. Campi algebricamente chiusi e polinomi irriducibili. L'enunciato del teorema di Gauss e la fattorizzazione in  $\mathbb{Q}[x]$ . La riduzione modulo  $p$ , il criterio di Eisenstein. Polinomi irriducibili in  $\mathbb{C}[x]$  e in  $\mathbb{R}[x]$ .

**Strutture quozienti:**

La congruenza modulo  $n$  in  $\mathbb{Z}$ . L'anello delle classi di resto  $\mathbb{Z}_n$ . La congruenza lineare in  $\mathbb{Z}$  e l'equazione di I grado in  $\mathbb{Z}_n$ . Il gruppo degli elementi invertibili in  $\mathbb{Z}_n$ . I campi  $\mathbb{Z}_p$ . La funzione di Eulero. Il teorema cinese del resto. Il piccolo teorema di Fermat, il teorema di Eulero. La congruenza modulo  $f$  in  $K[x]$ . L'anello delle classi resto modulo  $f$ , il sistema di rappresentanti canonici. Elementi invertibili in  $K[x]/(f)$ ; il caso dei polinomi irriducibili.

**Il gruppo simmetrico:**

L'azione naturale di  $S_n$  su  $X = \{1, \dots, n\}$ . Orbite e cicli associati ad una permutazione. Decomposizione in cicli disgiunti. Parità e segno di una permutazione, il gruppo alterno  $A_n$ .