

- 1→ Qual è la definizione di azione sinistra? → Dato un gruppo G e un insieme X definisco AZIONE DI X SU G un'applicazione $A : G \times X \rightarrow X$ che soddisfa:

1. $A(e, x) = x \ \forall x \in X$
2. $A(g, A(h, x)) = A(gh, x) \ \forall g, h \in G, \ \forall x \in X$

Dico che G AGISCE SU X , $G \curvearrowright X$

- 3→ Fornisci un esempio di azione su uno spazio vettoriale V → È sufficiente prendere $A : G \times V \rightarrow V : (g, v) \mapsto f(v)$
- 3.01→ Illustra come S_X agisce su X → L'azione è $g \cdot x := g(x)$
- 4→ Enuncia il lemma di caratterizzazione delle azioni di gruppo come morfismi nel gruppo simmetrico → Data un'azione $A : G \times X \rightarrow X : (g, x) \mapsto g \cdot x$, posso definire un morfismo $\alpha : G \rightarrow S_X$ ponendo $\alpha(g)$ la funzione $X \rightarrow X : x \mapsto A(g, x)$. (Cioè quindi $\alpha(g)(x) := A(g, x)$) (da dimostrare che α è ben definita).
Viceversa, dato $\alpha : G \rightarrow S_X$ morfismo, posso definire un'azione A come segue: $A(g, x) := \alpha(g)(x)$ (da dimostrare che è un'azione)
- 5→ Qual è la definizione di insieme G -invariante? → Se $G \curvearrowright X$, un sottoinsieme $Y \subseteq X$ è INVARIANTE quando $g \cdot y = y \ \forall y \in Y$
- 6→ Quali invarianti puoi trovare per $SO(3) \curvearrowright \mathbb{R}^3$? → Le sfere sono G -invarianti
- 7→ Come si comportano i sottogruppi di un gruppo che agisce su un insieme? → Agiscono anche loro sullo stesso insieme con la restrizione dell'azione
- 8→ Qual è la definizione di G -ORBITA di $x \in X$? → È $Gx = \{g \cdot x \mid g \in G\}$
- 9→ La collezione delle orbite di un'azione come si rapporta all'insieme su cui agisce l'azione? → Data $G \curvearrowright X$, le sue orbite formano una partizione di X
- 10→ Essere in nella stessa orbita è c1:: una relazione d'equivalenza → clz
- 11→ Qual è la definizione di X/G ? → $X/G := X/\sim$, con \sim relazione di equivalenza su X di appartenenza alla stessa orbita.
- 12→ Qual è la definizione di STABILIZZATORE di $x \in X$? → È $G_x := \{g \in G \mid g \cdot x = x\}$
- 13→ Come sono in relazione gli stabilizzatori di due elementi sulla stessa orbita? → Se x e y sono sulla stessa orbita, allora G_x e G_y sono coniugati.
- 14→ Qual è la definizione di azione transitiva? → $G \curvearrowright X$ è TRANSITIVA quando $\forall x, y \in X \ \exists g \in G : g \cdot x = y$ (cioè ho un'unica orbita, $Gx = X$)
- 15→ $SO(3) \curvearrowright S^2$ è c1::transitiva → clz
- 16→ Qual è la definizione di spazio omogeneo? → Data $G \curvearrowright X$ azione, se è transitiva dico che X è uno SPAZIO OMOGENEO per G
- 17→ Esibisci un'azione di un gruppo sul quoziente per un sottogruppo → In generale: se $H \leq G$, $X := G/H$ ho che $G \curvearrowright G/H : g \cdot aH := gaH$
- 18→ Qual è la definizione di un G -INSIEME? → è un insieme X su cui agisce G
- 19→ G/H è sempre c1:: omogeneo → clz
- 20→ Chi è lo stabilizzatore di un $x \in G/H$? → È in generale un coniugato di H
- 21→ Qual è la definizione di funzione equivariante? → È una $f : X \rightarrow Y$ due G -insiemi t.c. $f(g \cdot x) = g \cdot f(x)$

- 22 → Quando due insiemi sono ISOMORFI come G -insiemi? → Quando esiste una funzione biunivoca ed equivariante tra loro
- 23 → Enuncia il lemma di caratterizzazione degli spazi omogenei → $G \curvearrowright X$ transitiva, preso $x_0 \in X$ e posto $H := G_{x_0}$ allora $X \cong G/H$ come G -insieme
- 24 → La classe dei G -insiemi è una → Categoria, G -**insiemi** con $\text{Obj}(G\text{-ins.}) = \{X \text{ insiemi con una fissata } G\text{-azione}\}$ e $\forall X, Y \text{ } G\text{-ins.}: \text{Mor}(X, Y) = \{f : X \rightarrow Y \text{ equivarianti}\}$
- 25 → Enuncia che relazione collega lo stabilizzatore di un elemento con la sua orbita → $Gx \cong G/G_x$ come G -ins.
- 26 → Qual è la definizione di punto fisso di un'azione? → se $G \curvearrowright X$, un PUNTO FISSO dell'azione è un $x \in X$ t.c. $g \cdot x = x \forall g \in G$
- 27 → x è un punto fisso $\Leftrightarrow \text{cl}::G_x = G \rightarrow \text{clz}$
- 28 → Qual è la definizione di azione fedele? → Posto $\alpha : G \rightarrow S_X$ il morfismo associato a $G \curvearrowright X$, dico che l'azione è FEDELE quando α è iniettivo
- 29 → Data un'azione $\alpha : G \rightarrow S_X$ generica, costruisci un'azione fedele. → Dato che α è un morfismo, $\exists! \beta : G/\text{Ker}(\alpha) \rightarrow S_X$ iniettivo, che induce quindi un'azione fedele.
- 30 → Enuncia una caratterizzazione di azione fedele → $G \curvearrowright X$ è fedele $\Leftrightarrow \forall g \in G \setminus e \exists x \in X : g \cdot x \neq x$
- 31 → È $GL(V) \curvearrowright \mathbb{P}(V)$ effettiva? → No perché $f := x \rightarrow \lambda x$ è t.c. $f \neq id_V$ e $\alpha(f) = id_V$
- 32 → Se $G \curvearrowright X$ qual è la definizione di punto fisso di un $g \in G$? → $G \curvearrowright X$, dico che $x \in X$ è PUNTO FISSO di $g \in G$ quando $g \cdot x = x$.
- 33 → Qual è la definizione di azione libera? → $G \curvearrowright X$ è LIBERA quando $\forall g \in G, g \neq e$ vale che g non ha punti fissi
- 34 → Enuncia una caratterizzazione di azione fedele → $G \curvearrowright X$ è LIBERA $\Leftrightarrow \forall g \in G \setminus e, \forall x \in X : g \cdot x \neq x$
- 35 → Qual è la definizione di sistema di rappresentanti? → X insieme, \sim relazione di equivalenza su X , dico SISTEMA DI RAPPRESENTANTI un insieme $S \subseteq X$ t.c. $\pi|_S : S \rightarrow X/\sim$ (proiezione canonica) è biettiva.
- 36 → Enuncia l'equazione delle orbite → X, G finiti, $G \curvearrowright X$, sia $S = x_1, \dots, x_k$ un sistema di rappresentanti per la relazione "essere nella stessa orbita", allora $\#X = \sum_{i=1}^k \#G/\#G_{x_i}$
- 37 → Enuncia cosa è l'azione per traslazione → È l'azione $G \curvearrowright G : g \cdot x := gx$
- 38 → Enuncia qual è l'azione per moltiplicazione a destra. → È l'azione $G \curvearrowright G : g \cdot x := xg^{-1}$
- 39 → Qual è la definizione di azione destra? → È una funzione $X \times G \rightarrow X : (x, g) \mapsto x \cdot g$ che verifica $x \cdot e = x$; $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 g_2)$
- 40 → Come posso passare da un'azione destra ad un'azione sinistra (o viceversa?) → Se $B : X \times G \rightarrow X$ è un'azione destra, allora $A : G \times X \rightarrow X : A(g, x) := B(x, g^{-1})$ è un'azione sinistra
- 41 → Enuncia qual è l'azione di $G \curvearrowright G$ per coniugio → È l'azione $G \curvearrowright G : g \cdot x := gxg^{-1}$

- 42→ Qual è la definizione di automorfismo interno? → È un morfismo della forma: dato $\text{inn}_g : G \rightarrow G : x \mapsto gxg^{-1}$ per un certo $g \in G$
- 43→ Qual è il morfismo associato all'azione $G \curvearrowright G$ per coniugio? → È $\alpha : G \rightarrow S_G : \alpha(g) = \text{inn}_g$
- 44→ È l'azione per coniugio $G \curvearrowright G$ libera? → No: $\text{inn}_g(e) = e \forall g$, e è un punto fisso dell'azione
- 45→ Qual è la definizione di X^G se $G \curvearrowright X$? → $X^G := \text{Fix}_G(X) := \{x \in X \mid \forall g : g \cdot x = x\}$
- 46→ Se $G \curvearrowright G$ per coniugio, chi è $\text{Fix}_G(G)$? → $\text{Fix}_G(G) = Z(G)$ il centro di G
- 47→ Se $G \curvearrowright G$ per coniugio, chi è G_x ? → $G_x = Z_G(x)$ il centralizzante di x
- 48→ Enuncia l'EQUAZIONE DELLE CLASSI → È $|G| = |Z(G)| + \sum_{i=1}^m [G : Z_G(x_i)]$ se x_1, \dots, x_k è un sistema di rappresentanti della relazione delle orbite, con $x_1, \dots, x_m \notin Z(G)$
- 49→ Qual è la definizione di p -gruppo? → È un gruppo G con $o(G) = p^\alpha$, p primo e $\alpha \in \mathbb{N}^{>0}$
- 50→ Com'è il centralizzante di un p gruppo? → È banale, $Z(G) = \{1\}$
- 51→ Puoi estendere un'azione su un insieme al suo insieme delle parti? → Sì, è facile vedere che se $G \curvearrowright X$, allora si ha anche che $G \curvearrowright \mathcal{P}(X) : g \cdot E := \{g \cdot x \mid x \in E\} (= \alpha(g)(E))$
- 52→ Come puoi far agire un gruppo G sull'insieme dei suoi sottogruppi? → Sapendo che $G \curvearrowright \mathcal{P}(G)$ per coniugio, ho che $\mathcal{S}(G) := \{\text{sottogruppi di } G\}$ è un insieme invariante. Allora posso restringere l'azione sopra $g \cdot H := gHg^{-1}$
- 53→ Presa l'azione $G \curvearrowright S(G)$ per coniugio, e $H \in S(G)$, chi è G_H ? → È il NORMALIZZANTE di H in G
- 54→ Presa l'azione $G \curvearrowright S(G)$ per coniugio dai una caratterizzazione dell'orbita di $H < G$ → $GH = \{\text{coniugati di } H\}$, $|GH| = |G|/|G_H| = \#\text{CONIUGATI DI } H = |G|/N_G(H)$
- 55→ che relazione c'è tra un sottogruppo $H < G$ e il suo normalizzante? → $H \triangleleft N_G(H)$ e $H \triangleleft G \Leftrightarrow N_G(H) = G$
- 56→ Come puoi descrivere euristicamente il normalizzante di un sottogruppo $H < G$? → È il "più grande sottogruppo di G in cui H è normale", cioè se $H' < G$, $H \subseteq H'$, $H \triangleleft H' \Rightarrow H' \subseteq N_G(H)$
- 57→ Che rapporto c'è tra il centro di un elemento $x \in G$ ed il normalizzante del suo gruppo generato? → Vale in generale $Z_G(x) \subseteq N_G(\langle x \rangle)$, non vale in generale l'uguaglianza
- 58→ Enuncia il teorema di Cayley nel contesto delle azioni → Ogni gruppo ha un'azione fedele su un qualche insieme
- 59→ Esibisci un Gruppo che non possiede sottogruppi di un determinato ordine che divide l'ordine del gruppo → $G = A_4$ non possiede sottogruppi di ordine 6
- 60→ Qual è l'ordine di un generico elemento di un gruppo ciclico? → Se $G = \langle g \rangle$, $o(G) = n$, allora $o(g^s) = \frac{n}{(n,s)}$

- 61 → Quanti generatori ha un gruppo ciclico $G = \langle g \rangle$ $o(G) = n$? → Sono tanti quanto i naturali $\leq n$ che non dividono n , cioè $\varphi(n)$
- 62 → Caratterizza i sottogruppi di ordine $d|n$ di un gruppo ciclico G → Sono gli $H < G$ t.c. $H = \langle g^{n/d} \rangle$, questo esiste ed unico $\Leftrightarrow d|n$
- 63 → Enuncia la FORMULA DI GAUSS → $\sum_{d:d|n} \varphi(d) = n$
- 64 → Dai una condizione sui sottogruppi di un gruppo G sufficiente affinché esso sia ciclico → G gruppo, $o(G) = n$, se $\forall d|n$ esiste al più un sottogruppo di ordine d , allora G è ciclico
- 65 → Dai la definizione di G^d e una condizione su di esso affinché il gruppo G sia ciclico → $G^d = \{x \in G \mid x^d = 1\}$. Se $\forall d|n : |G^d| \leq d \Rightarrow G$ è ciclico.
- 66 → Dai delle condizioni sufficienti per trovare dei sottogruppi di un gruppo abeliano → G gruppo abeliano, $o(G) = n$, $d|n \Rightarrow \exists H \leq G : o(H) = d$
- 67 → Cosa puoi dire dei sottogruppi di gruppi ciclici e abeliani? →
 1. G abeliano $\Rightarrow \forall d|n \exists$ un sottogruppo di G di ordine n
 2. G ciclico $\Rightarrow \forall d|n \exists$ un sottogruppo di G di ordine n
- 68 → Enuncia il teorema di Sylow → Dato un gruppo finito G , posto $o(G) = p^\alpha m$, p primo, $p \nmid m$, allora
 1. \exists un p -syLOW in G
 2. se $H \leq G$ è un p -sottogruppo $\Rightarrow H$ è contenuto in un p -syLOW
 3. tutti i p -syLOW sono coniugati
 4. Detto $n_p = \#\{p\text{-syLOW}\} \Rightarrow n_p = [G : N_G(P)]$, con P un p -syLOW.
 5. $n_p \equiv 1 \pmod{p}$ e $n_p | n$
- 69 → Enuncia il lemma che ti permette di trovare dei p -syLOW di un sottogruppo → G gruppo finito, H sottogruppo e P p -syLOW $\Rightarrow \exists x \in G : xPx^{-1} \cap H$ è un p -syLOW di H
- 70 → Dati $P, H < G$, come può agire $P \times H$ su G ? Di' chi è lo stabilizzatore di un elemento → $P \times H \curvearrowright G : (a, h) \cdot x = axh^{-1}$, e inoltre $(P \times H)_x \cong (x^{-1}Px) \cap H$ tramite $f : f(a, h) = h$ e $f^{-1}(h) = (x^{-1}Px, h)$
- 71 → Enunciai il corollario del lemma sui p -syLOW dei sottogruppi → $H \leq G$, G ha un p -syLOW \Rightarrow anche H ha un p -syLOW
- 72 → Dai un'idea di quale sia la strategia per dimostrare il teorema di Sylow → Esegui due passi:
 1. trovo una classe di gruppi con un p -syLOW banale, cioè $GL(n, F_p)$, p primo e $F_p = \mathbb{Z}/p$
 2. esibisco un morfismo iniettivo in $GL(n, F_p)$ per un qualsiasi gruppo finito
- 73 → Qual è la cardinalità di $GL(n, F_p)$ con p primo e $F_p = \mathbb{Z}/p$? → È $\prod_{i=0}^{n-1} (p^n - p^i)$
- 74 → Enuncia una caratterizzazione dei gruppi di ordine un quadrato di un primo → G gruppo, $Z(G) \neq \{1\}$, $\#G = p^2$, p primo $\Rightarrow G \cong C_{p^2}$ oppure $G \cong C_p \times C_p$

- 75 → Enuncia una condizione sufficiente su un gruppo affinché esso sia abeliano che va a guardare $G/Z(G) \rightarrow G$ finit. $G/Z(G)$ ciclico $\Rightarrow G$ abeliano
- 76 → Esibisci il morfismo iniettivo da $S_n \hookrightarrow GL(n, F_p) \rightarrow$ È il morfismo che manda $\sigma \mapsto \varphi(\sigma) := (e_{\sigma(1)} | \dots | e_{\sigma(n)})$ cioè che manda un morfismo nella matrice identità con le colonne permutate.
- 77 → Descrivi il funtore dalla categoria degli insiemi alla categoria degli spazi vettoriali su un campo fissato \rightarrow È una mappa della forma $\mathbf{Set} \xrightarrow{\alpha} \mathbf{Vec}(F) : \text{Mor}_{\mathbf{Set}}(X, Y) = \{f : X \rightarrow Y\} \xrightarrow{\alpha} \{f^* : F^Y \rightarrow F^X\} = \text{Mor}_{\mathbf{Set}}(\alpha(X), \alpha(Y)) : f \mapsto f^*, \text{ con } f^* : F^Y \rightarrow F^X : u \mapsto u \circ f$ È un funtore controvariante
- 78 → Descrivi il processo di linearizzazione di un'azione $\rightarrow ???$
- 79 → Qual è la definizione di F -ALGEBRA ? \rightarrow È un anello A che è anche un F -spazio vettoriale, con la stessa struttura additiva e t.c. $\forall a, b \in A \forall \lambda \in F : \lambda(ab) = a(\lambda b) = (\lambda a)b$
- 80 → Esibisci una F -algebra facile \rightarrow Dati X insieme e F campo, F^X è un' F -algebra commutativa con unità $1 : X \rightarrow F : x \mapsto 1 \in F$
- 81 → Dato un p -gruppo, esibisci dei suoi sottogruppi $\rightarrow \#G = p^\alpha, p$ primo $\Rightarrow \forall i = 0, \dots, \alpha \exists H < G : \#H = p^i$
- 82 → Enuncia il lemma che caratterizza il prodotto NH di due sottogruppi $N, H < G$, data la funzione $f : N \times H \rightarrow G, f(n, h) := nh \rightarrow$
 1. $\text{Im}(f) = NH$
 2. $nh \in \text{Im}(f)$ e $f^{-1}(nh) = \{(nx, x^{-1}h) \mid x \in N \cap H\}$
 3. $|NH| = |N||H|/|N \cap H|$
 4. $N \triangleleft G \Rightarrow NH < G$
 5. $N, H \triangleleft G \Rightarrow NH \triangleleft G$
 6. Se $N, H \triangleleft G \Rightarrow [N, H] \subseteq N \cap H$
 7. Se $H, N \triangleleft G, N \cap H = \{1\} \Rightarrow NG \cong N \times H$
- 83 → Enuncia la proposizione sull'equivalenza tra il prodotto diretto interno ed esterno $\rightarrow H, G \triangleleft G, N \cap H = \{1\}, NH = G \Rightarrow N \cong N \times H$.
D'altro lato, se pongo $N \times H =: K$ ho: $\bar{N} := N \times \{1\} \triangleleft K, \bar{H} := \{1\} \times H \triangleleft K$ sono tali che $\bar{N} \cap \bar{H} = \{(1, 1)\} e K = \bar{N} \bar{H}$
- 84 → Enuncia il lemma di caratterizzazione del prodotto di un numero finito arbitrario di gruppi $\rightarrow G$ gruppo, $N_1, \dots, N_k \triangleleft G$ tali che $N_i \cap (N_1 \cdot \dots \cdot \hat{N}_i \cdot \dots \cdot N_k) = \{1\} \Rightarrow f : N_i \times \dots \times N_k \rightarrow N_1 \cdot \dots \cdot N_k : (n_1, \dots, n_k) \rightarrow n_1 \cdot \dots \cdot n_k$ è un isomorfismo
- 85 → Enuncia il teorema di Cauchy per gruppi $\rightarrow G$ gruppo finito, p primo t.c. $p | o(G) \Rightarrow G$ contiene un elemento di ordine p
- 86 → Enuncia il teorema di caratterizzazione dei gruppi con p -syLOW unici $\rightarrow G$ gruppo finito, $o(G) = p_1^{\alpha_1} \dots p_k^{\alpha_k}, p_i$ primi, se tutti i p -syLOW sono unici \Rightarrow posti P_1, \dots, P_k gli unici p -syLOW ho che $G \cong P_1 \times \dots \times P_k$
- 87 → Cosa puoi dire su n_p se il p -syLOW è normale? \rightarrow Ho che $P \triangleleft G \Leftrightarrow n_p = 1$
- 88 → Enuncia la proposizione di caratterizzazione dei gruppi con ordine un prodotto di

- primi $\rightarrow G$ gruppo con $o(G) = pq$, p, q primi, $p < q$ e $p \nmid q-1 \Rightarrow G \cong C_p \times C_q (\cong C_{pq})$
- 89 \rightarrow Illustra la costruzione del prodotto semidiretto interno di gruppi \rightarrow Dati un gruppo G , $N \triangleleft H$ ed un sottogruppo H di G , tali che $G = NH$, $N \cap H = \{e\}$ ho che $f : N \times H \rightarrow G$ è biunivoca. Se $h \in H$ allora inn_h è un automorfismo che preserva N , dunque è anche un automorfismo di N , che indico con $\varepsilon_h : N \rightarrow N$, $\varepsilon_h(n) = hnh^{-1}$. Otengo dunque che $f(n_1, h_1) \cdot f(n_2, h_2) = f(n_1 \varepsilon_{h_1}(n_2), h_1 h_2)$. Questo significa che dato un il morfismo ϵ è possibile calcolare il prodotto di G e ricostruire questo gruppo a partire da N ed H . (very bad flashcard)
 - 90 \rightarrow Enuncia il teorema sul prodotto semidiretto esterno \rightarrow Dati N ed H gruppi e $\theta : H \rightarrow \text{Aut } N : h \rightarrow \theta_h$ un morfismo. Definiamo su $N \times H$ il prodotto \bullet_θ mediante la formula

$$(n_1, h_1) \bullet_\theta (n_2, h_2) := (n_1 \theta_{h_1}(n_2), h_1 h_2)$$

. Vale quindi che

1. $G := (N \times H, \bullet_\theta)$ è un gruppo, indicato con $N \rtimes_\theta H$, chiamato **PRODOTTO SEMIDIRETTO** di N ed H
2. Le mappe

$$\alpha : N \rightarrow G, \alpha(n) = (n, e), \quad \beta : H \rightarrow G, \beta(h) = (e, h)$$

sono morfismi iniettivi di gruppi.

3. $\bar{N} := \alpha(N) = N \times \{e\}$ è un sottogruppo normale di G , mentre $\bar{H} := \{e\} \times H$ è un sottogruppo di G
4. $G = \bar{N}\bar{H}$. Infine il morfismo ε coincide con θ a meno di α e β , ossia se $n \in N$ e $h \in H$, $\bar{n} := \alpha(n)$, $\bar{h} := \beta(h)$ allora

$$\varepsilon_{\bar{h}}(\bar{n}) = \bar{h} \bullet_\theta \bar{n} \bullet_\theta h^{-1} = \alpha \circ \theta_h(n)$$

(very very bad flashcard)

- 91 \rightarrow Enuncia la proposizione sul rapporto tra il prodotto interno ed il prodotto semidiretto di gruppi \rightarrow Dato un gruppo G , $H \leq G$, $N \triangleleft G$, definito $\epsilon : H \rightarrow \text{Aut } N : h \mapsto (\epsilon_h : N \rightarrow N : n \mapsto \epsilon_h(n) = hnh^{-1})$, se $G = NH$ e $H \cap N = \{e\}$ allora $G \cong N \rtimes_\epsilon H$
- 92 \rightarrow Se in un prodotto semidiretto ho due morfismi coniugati cosa succede? \rightarrow Dati N ed H gruppi, $\theta, \theta' : H \rightarrow \text{Aut } N$ morfismi. Se esiste $\alpha \in \text{Aut } N$ tale che

$$\theta'_h = \alpha \circ \theta_h \circ \alpha^{-1}$$

allora l'applicazione

$$F : N \rtimes_\theta H \rightarrow N \rtimes_{\theta'} H, F(n, h) := (\alpha(n), h)$$

è un isomorfismo $N \rtimes_\theta H \cong N \rtimes_{\theta'} H$

- 93 → Qual è la definizione di sottogruppo caratteristico? → È un sottogruppo tale che per ogni $\alpha \in \text{Aut } G$ vale $\alpha(H) = H$
- 94 → Esibisci due sottogruppi caratteristici sempre presenti in un gruppo → Il centro $Z(G)$ ed il sottogruppo dei commutatori, $[G, G]$
- 95 → Un p -sylo di G è normale se e solo se c1::è unico se e solo se c1::è caratteristico → clz
- 96 → Enuncia la proposizione che caratterizza i quozienti abeliani → Dato G gruppo, il sottogruppo dei commutatori $[G, G]$ è caratteristico. Inoltre se $N \triangleleft G$ allora G/N è abeliano se e solo se $[G, G] \subseteq N$
- 97 → Qual è la definizione di CATENA NORMALE in un gruppo G ? Cosa sono i fattori della catena? → È una successione di sottogruppi

$$G = G_0 \supset G_1 \supset \dots \supset G_i \supset G_{i+1} \supset \dots$$

tale che $g_{i+1} \triangleleft G_i$ per ogni i e $G_n = \{1\}$ per qualche n . I fattori della catena sono G_i/G_{i+1}

- 98 → Qual è la definizione di catena dei derivati? → È la catena $D^0G := G$, $D^{i+1}G := [D^iG, D^iG]$, tale che $G = D^0G \supset D^1G \supset \dots \supset D^iG \supset D^{i+1}G \supset \dots$
- 99 → Un gruppo abeliano finito è semplice se e solo se → è ciclico di ordine finito
- 99.1 → Un gruppo G è risolubile se e solo se → esiste un numero n tale che $D^nG = \{e\}$
- 99.2 → Dato un gruppo finito G , allora sono equivalenti le condizioni:

1. c1::G è risolubile

2. c2::Esiste una catena normale con fattori ciclici di ordine primo

- 100 → Cos'è la caratteristica di un anello? → Preso un anello A esiste sempre un morfismo $\phi : \mathbb{Z} \rightarrow A : n \mapsto \phi(n) = n \cdot 1_A$. Essendo \mathbb{Z} un PID, il nucleo di ϕ sarà principale, cioè esiste un n t.c. $\ker \phi = (n)$. Questo n è la CARATTERISTICA dell'anello A .
- 101 → Come si comporta il prodotto in un campo di caratteristica n ? → preso $m \in \mathbb{Z}$ e $x \in K^*$, $m \cdot x = 0$ sse $n|m$ con $n = \text{car } K$
- 102 → Qual è la definizione di campo primo? → È il campo generato dall'immagine di $\phi : n \mapsto n \cdot 1_A$
- 103 → Qual è la definizione di estensione di campi? → È un morfismo di anelli $i : F \rightarrow E$ dove E, F sono campi. Si verifica che è automaticamente iniettiva.
- 104 → Se E/F è un'estensione di campi, E è c1:: uno spazio vettoriale su F → clz
- 105 → Dato un campo F , cos'è una F -algebra? → È un anello A con una "moltiplicazione per scalare" $F \times A \rightarrow A$ che rende A uno spazio vettoriale su F ; inoltre deve valere che

$$\lambda(ab) = a(\lambda b) = (\lambda a)b$$

- 106 → Qual è la definizione di grado di un'estensione E/F ? → È il numero $[E : F] = \dim_F E$, dimensione come spazio vettoriale.

- 107→ Qual è la definizione di estensione finita? → È un'estensione E/F per la quale $[E : F] < \infty$
- 108→ Quando la mappa che manda un polinomio nella funzione indotta dal polinomio è iniettiva? → Quando il campo è infinito
- 109→ Data un'estensione di campi E/F , qual è la definizione di campo intermedio? → È un campo K tale che $F \subseteq K \subseteq E$
- 110→ Qual è la definizione di campo generato da $S \subseteq E$? → È l'intersezione di tutti i campi intermedi che contengono S
- 111→ Qual è la definizione di sistema di generatori di un'estensione E/F ? È un insieme $S \subseteq E$ tale che $E = F(S)$
- 112→ Qual è la definizione di estensione finitamente generata? → È un'estensione E/F per cui esiste un insieme finito S tale che $E = F(S)$
- 113→ Qual è la definizione di estensione semplice? → È un'estensione generata da un solo elemento
- 114→ Se E/F e F/K sono estensioni finite, allora $[E : K] = ? \rightarrow = [E : F] \cdot [F : K]$
- 115→ Come costruisco un'estensione che contenga una radice di un polinomio irriducibile? → F campo, f irriducibile, allora la composizione $F \hookrightarrow F[X] \rightarrow K := F[X]/(f)$ è un'estensione di grado $[K : F] = \deg f$. Se π è la proiezione canonica, allora $\gamma := \pi(X) \in K$ è una radice di f , e $K = F(\gamma)$
- 116→ Enuncia il procedimento di Kronecker → Sia F un campo e f un polinomio di grado $d \geq 1$. Allora c'è un'estensione finita di F in cui f possiede una radice. (Si prende la proposizione che richiede che f sia un polinomio irriducibile e la si applica ad un fattore irriducibile di f)
- 117→ Qual è la definizione di numero algebrico di un'estensione? → Data E/F dico che $\alpha \in E$ è ALGEBRICO su F se esiste un polinomio $p(X) \in F[X]$ tale che $p(x) \neq 0, p(\alpha) = 0$. Un elemento non algebrico è TRASCENDENTE
- 118→ Data E/F estensione, qual è la definizione di polinomio minimo di $\alpha \in E$? → È il "generatore monico dell'ideale $\ker v_\alpha$ ", cioè un polinomio monico che divide ogni polinomio che ha soluzione α . Si indica con $m_{\alpha, F, 0}$ m_α
- 119→ Enuncia la proposizione sulla relazione tra $F[x]/(f)$ e $F(\alpha)$ dove E/F estensione $f = m_\alpha$ e α algebrico → Data E/F un'estensione, α algebrico e $f = m_\alpha$ polinomio minimo. Allora la valutazione induce un isomorfismo

$$\varphi_\alpha : F[X]/(f) \xrightarrow{\cong} F(\alpha) \quad \varphi_\alpha(g + (f)) = g(\alpha).$$

Inoltre $[F(\alpha) : F] = \deg f =: d$ e $\{1, \alpha, \dots, \alpha^{d-1}\}$ è una base di $F(\alpha)$ su F

- 120→ Per descrivere $F(\alpha)$ bisogna per forza utilizzare le funzioni razionali? → No è sufficiente valutare i polinomi in quanto $F(\alpha) = \text{im } \varphi_\alpha = v_\alpha(F[X])$
- 121→ Data un'estensione E/F , e $\alpha \in E$, allora α è algebrico se e solo se → $[F(\alpha) : F] < \infty$
- 122→ Qual è la definizione di estensione algebrica → è un'estensione in cui ogni elemento è algebrico

- 123→ Come vengono caratterizzate le estensioni finite? → Le estensioni finite sono quelle algebriche e finitamente generate o equivalentemente quelle generate da un numero finito di elementi algebrici
 - 124→ Qual è la definizione di campo algebricamente chiuso? → è un campo per cui ogni polinomio non costante su di esso ammette una radice
 - 125→ Qual è la definizione di chiusura algebrica di un campo K ? → è un'estensione algebrica L/K con L algebricamente chiuso
 - 126→ Enuncia il teorema di Steinitz→ Ogni campo ammette una chiusura algebrica
 - 127→ Enuncia il lemma sugli elementi algebrici di una chiusura algebrica → K campo, L/K estensione con L algebricamente chiuso, allora $\overline{K}^L = \{\alpha \in L : \alpha \text{ è algebrico su } K\}$ è un campo intermedio algebricamente chiuso, inoltre \overline{K}^L/K è algebrica.
 - 128→ Dato un morfismo di campi $\sigma : K \rightarrow L$, e un polinomio $f = \sum a_i x^i$, cosa indica f^σ ? → $f^\sigma = \sum \sigma(a_i) x^i$
 - 129→ Dato $\sigma : K \rightarrow L$ un morfismo di campi, presi $K' = K(\alpha)$ un'estensione semplice algebrica, e f il polinomio minimo di α , allora:
 1. c1::se $\sigma' : K' \rightarrow L$ è un morfismo che estende σ , allora $\sigma'(\alpha)$ è una radice di f^σ
 2. c2::se $\beta \in L$ è una radice di f^σ , allora esiste uno ed un solo morfismo $\sigma' : K \rightarrow L$ che estende σ e tale che $\sigma'(\alpha) = \beta$
 3. c3::Le possibili estensioni di σ a K' sono al più $\deg f = [K' : K]$
- clz
- 130→ Enuncia il teorema sulla caratterizzazione delle estensioni algebricamente chiuse → Sia K'/K un'estensione algebrica e sia L un campo algebricamente chiuso. Sia $\sigma : K \rightarrow L$ un morfismo. Allora esiste sempre un morfismo $\sigma' : K' \rightarrow L$ che estende σ . Se K' è algebricamente chiuso e $L/\sigma(K)$ è algebrica, allora ogni estensione è un isomorfismo $K' \cong L$
 - 131→ Un'estensione algebrica di un campo **finito o numerabile** → è ancora **numerabile**
 - 132→ Qual è la definizione di numeri algebrici e trascendenti? → I NUMERI ALGEBRICI sono gli elementi della chiusura algebrica di \mathbb{Q} , cioè $\overline{\mathbb{Q}}^{\mathbb{C}}$. I NUMERI TRASCENDENTI sono gli elementi di $\mathbb{C} \setminus \overline{\mathbb{Q}}^{\mathbb{C}}$
 - 133→ Data un'estensione E/F e due campi intermedi, K ed L , qual è la definizione del campo composto? → È il campo $KL := \bigcap_{\substack{M \subseteq L \text{ sottocampo} \\ K \cup L \subseteq M}} M$. È il più piccolo sottocampo di E che contiene L e K .
 - 134→ Cosa vuol dire che un polinomio $f \in F[X]$ si SPEZZA su un'estensione E/F ? → Che è possibile scriverlo come prodotto di fattori lineari:

$$f(X) = c \cdot (X - \alpha_1) \dots (X - \alpha_n) \quad \alpha_i \in E$$

- 135→ Qual è la definizione di campo di spezzamento di un polinomio→ Un'estensione E/F è un CAMPO DI SPEZZAMENTO di f su F se f si spezza su E e se f non si spezza su nessun campo intermedio.
- 136→ Come si caratterizzano i campi di spezzamento? → E è di spezzamento di f se e solo se f si spezza su E ed E è generato dalle radici di f : $E = F(\alpha_1, \dots, \alpha_n)$
- 137→ Esiste sempre il campo di spezzamento di un polinomio non costante? → Sì, dato $f \in F[X]$, $\deg f =: d$, esiste E/F di spezzamento per f , con $[E : F] \leq d!$. Se f è irriducibile, allora $d \mid [E : F]$
- 138→ Cosa succede se ho due campi di spezzamento dello stesso polinomio $f \in F[X]$ → Se ho due campi di spezzamento $E/F, E'/F$, allora per ogni morfismo F -lineare $\eta : E \rightarrow \bar{E}'$ si ha $\eta(E) = E'$. Da questo scende che il campo di spezzamento di un polinomio è unico a meno di isomorfismo
- 139→ Qual è la definizione di estensione NORMALE? → È un'estensione algebrica E/F per cui ogni polinomio irriducibile a coefficienti in F che ha una radice in E si spezza su E .
- 140→ Un'estensione algebrica E/F è normale sse per ogni $\alpha \in E$ → il polinomio minimo $m_{\alpha, F}$ si spezza su E .
- 141→ Enuncia il teorema di caratterizzazione delle estensioni finite normali → Data un'estensione E/F finita, le seguenti condizioni sono equivalenti:
 1. Ogni morfismo F -lineare $\eta : E \rightarrow \bar{E}$ ha immagine contenuta in E
 2. L'estensione E/F è normale
 3. E/F è il campo di spezzamento di un polinomio $f \in F[X]$.
- 142→ Se ho una catena di campi $K \subseteq L \subseteq M$, come si comporta la normalità? → Se M/K è normale, allora anche M/L lo è
- 143→ Qual è la definizione di polinomio SEPARABILE? → Un polinomio a coefficienti in un campo F è separabile se non ha radici multiple in nessuna estensione di F
- 144→ Qual è la definizione di ELEMENTO SEPARABILE? → Data un'estensione algebrica E/F e $\alpha \in E$, diciamo che α è un elemento separabile su F se $m_{\alpha, F}$ è un polinomio separabile
- 145→ Qual è la definizione di ESTENSIONE SEPARABILE? → È un'estensione E/F in cui ogni elemento di E è separabile
- 146→ Se $f \in F[X]$ è irriducibile e non separabile, allora → $f' \equiv 0$
- 147→ Qual è la definizione di CAMPO PERFETTO?→ È un campo per cui le tutte le sue estensioni algebriche sono separabili
- 148→ Cosa succede ai polinomi sui campi di caratteristica zero? → Se F è un campo, ogni polinomio irriducibile in $F[X]$ è separabile, quindi ogni estensione algebrica di F è separabile. Dunque ogni campo di caratteristica zero è perfetto
- 149→ Enuncia il teorema sui campi finiti
 1. c1::Un campo finito di caratteristica p ha ordine p^n

2. c2::Per ogni n esiste un campo di ordine p^n
3. c3::Ogni campo di ordine $q = p^n$ è un campo di spezzamento del polinomio $X^q - X$ sul campo primo
4. c4::Per il punto precedente, per ogni n esiste uno ed un solo campo di ordine p^n a meno di isomorfismo
5. c5::I campi finiti sono perfetti

→ clz

- 150→ Enuncia il teorema dell'elemento primitivo → Un'estensione E/F finita e separabile è semplice, cioè esiste un elemento $\alpha \in E$, l'elemento primitivo, tale che $E = F(\alpha)$
- 151→ L campo, $f, g \in L[X]$, se $f|g$ e g è separabile allora → anche f lo è
- 152→ Data una catena di campi $K \subseteq L \subseteq M$, se M/K è separabile, allora → anche M/L e L/K lo sono
- 153→ Enuncia il teorema sui morfismi lineari su una chiusura algebrica. → E/F estensione finita e separabile, \bar{F} una chiusura algebrica di F . Allora esistono esattamente $[E : F]$ morfismi F -lineari da E a \bar{F}
- 154→ Qual è la definizione di GRUPPO DI GALOIS di un'estensione E/F ? → È l'insieme $\text{Gal}(E/F)$ degli automorfismi di campo F -lineari di E , che è un gruppo rispetto alla composizione.
- 155→ Qual è la definizione di estensione DI GALOIS? → È un'estensione finita E/F normale e separabile
- 156→ Se E/F è finita e normale, allora $\text{Gal}(E/F)$ coincide con → l'insieme dei morfismi F -lineari $E \rightarrow \bar{E}$
- 157→ Se E/F è di Galois, allora $|\text{Gal}(E/F)| = [E : F]$
- 158→ Qual è la definizione di gruppo di Galois di un polinomio f ? → È il gruppo di Galois del campo di spezzamento di f
- 159→ Se $E = F(\alpha_1, \dots, \alpha_n)$ e $d_i = \deg m_{\alpha_i}$, allora $|\text{Gal}(E/F)| \leq d_1 \dots d_n$
- 160→ Come si comporta il gruppo di Galois rispetto all'insieme delle radici di un polinomio? → Presi E/F estensione, $f \in F[X]$ e posto R l'insieme delle radici di f in E si ha che R è invariante per l'azione di $\text{Gal}(E/F)$. Cioè se $\alpha \in R$ e $\sigma \in \text{Gal}(E/F)$ si ha $\sigma(\alpha) \in R$. Possiamo quindi dire che $\text{Gal}(E/F) \curvearrowright R$
- 161→ Preso $f \in F[X]$ e posto E il campo di spezzamento di f . Se l'insieme delle radici di f in E è $R := \{\alpha_1, \dots, \alpha_n\}$, allora:

1. c1::l'azione di $\text{Gal}(E/F)$ è fedele

2. c2::se f è irriducibile, allora $\text{Gal}(E/F)$ agisce transitivamente sulle radici di f

→ clz

- 162→ Se $E = F(\alpha)/F$ è un'estensione semplice, allora

 1. l'azione di $\text{Gal}(E/F)$ sull'insieme R delle radici di $m_{\alpha, F}$ è libera e transitiva

2. l'ordine del gruppo di Galois, $|\text{Gal}(E/F)|$ coincide con il numero delle radici di $m_{\alpha,F}$ in E

→

- 163→ Qual è la definizione di CAMPO FISSATO da un sottogruppo di $\text{Gal}(E/F)$? → è un $E^G := \{\alpha \in E : \gamma(\alpha) = \alpha \ \forall \gamma \in G\}$ con $G \leq \text{Gal}(E/F)$
- 164→ Enuncia il lemma di Artin → Data un'estensione finita E/F , allora per ogni sottogruppo $G \leq \text{Gal}(E/F)$ l'estensione E/E^G è di Galois, $\text{Gal}(E/E^G) = G$ e $[E : E^G] = |G|$
- 165→ Enuncia il teorema di caratterizzazione delle estensioni di Galois → Se E/F è un'estensione finita, allora le seguenti condizioni sono equivalenti:
 1. E/F è di Galois
 2. $|\text{Gal}(E/F)| = [E : F]$
 3. $E^{\text{Gal}(E/F)} = F$
- 166→ Se $K \subseteq L \subseteq M$ sono estensioni finite e M/K è di Galois, allora → anche M/L è di Galois
- 167→ Se E/F è di Galois, $\alpha \in E$ e $\text{Gal}(E/F) \cdot \alpha = \alpha_1 = \alpha, \dots, \alpha_r$, allora $m_{\alpha,F}(X) = (X - \alpha_1) \dots (X - \alpha_r)$
- 168→ Cos'è la CORRISPONDENZA DI GALOIS? → Posti $\mathcal{K} := \{\text{campi } K \text{ tali che } F \subseteq K \subseteq E\}$ e $\mathcal{S} := \{G \leq \text{Gal}(E/F)\}$, è la coppia di funzioni

$$\begin{aligned}\sigma : \mathcal{K} &\rightarrow \mathcal{S} & \sigma(K) &:= \text{Gal}(E/K) \\ \tau : \mathcal{S} &\rightarrow \mathcal{K} & \tau(G) &:= E^G\end{aligned}$$

- 169→ Cosa vale sempre per le composizioni $\tau\sigma$ e $\sigma\tau$ della corrispondenza di Galois? →
 1. Per ogni $K \in \mathcal{K}$ si ha che $K \subseteq \tau\sigma(K) = E^{\text{Gal}(E/K)}$
 2. Per ogni $G \in \mathcal{S}$ si ha $G = \sigma\tau(G) (= \text{Gal}(E/E^G))$
- 170→ Enuncia il teorema fondamentale della teoria di Galois, I parte → Sia E/F un'estensione finita. Allora la corrispondenza di Galois è biunivoca (cioè σ e τ sono una l'inversa dell'altra) se e solo se E/F è di Galois
- 171→ Enuncia il teorema fondamentale della teoria di Galois, II parte → Sia E/F un'estensione di Galois, e sia $K \in \mathcal{K}$. Allora K/F è di Galois se e solo se $\text{Gal}(E/K) \triangleleft \text{Gal}(E/F)$. In tal caso

$$\text{Gal}(K/F) \cong \frac{\text{Gal}(E/F)}{\text{Gal}(E/K)}$$

- 172→ Qual è la definizione di ESTENSIONE RADICALE? → È un'estensione finita per cui esiste una catena

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \dots \subseteq F(\alpha_1, \dots, \alpha_r) = E'$$

tale che per ogni i esiste $0 < m_i \in \mathbb{Z}$ tale che $\alpha_i^{m_i} \in F(\alpha_1, \dots, \alpha_{i-1})$

- 173 → Quando un'equazione polinomiale $f(X) = 0$, $f \in F[X]$ è risolubile per radicali?
→ Quando il campo di spezzamento di $f(X)$ su F è contenuto in E' , dove E'/F è un'estensione radicale.
- 174 → Qual è la definizione di gruppo di Galois di un'equazione polinomiale $f(X) = 0$?
→ È il gruppo di Galois di f
- 175 → In caratteristica 0 ogni estensione radicale è contenuta in un'estensione → radicale e di Galois
- 176 → In caratteristica 0 un'estensione di Galois, E/F , è contenuta in un'estensione radicale e di Galois se e solo se → $\text{Gal}(E/F)$ è un gruppo risolubile
- 177 → Enuncia il teorema di Galois → Siano F un campo di caratteristica 0, $f \in F[X]$. Allora l'equazione $f(X) = 0$ si può risolvere per radicali se e solo se il suo gruppo di Galois è un gruppo risolubile.
- 178 → Data una catena di campi $K \subseteq L \subseteq M$ una catena di campi, se M/L e L/K sono radicali, allora → anche M/K lo è.
- 179 → Se K'/K è radicale e v è un elemento di una delle estensioni che portano a K' , allora → anche $K'(v)/K(v)$ è radicale
- 180 → Se K'/K è radicale, v_1, \dots, v_n sono elementi di un'estensione di K' , allora → anche l'estensione $K'(v_1, \dots, v_n)/K(v_1, \dots, v_n)$ è radicale
- 181 → Siano E/F un'estensione, K, L campi intermedi e KL il campo composto. Se le estensioni K/F e L/F sono radicali, → anche KL/F lo è
- 182 → Com'è l'estensione $F(\mu_n)/F$ con μ_n insieme delle radici di $X^n - 1$? → $F(\mu_n)/F$ è di Galois e $\text{Gal}(F(\mu_n)/F)$ è un gruppo abeliano
- 183 → Enuncia il lemma sulle estensioni dei campi di caratteristica nulla che contengono n radici n -esime dell'unità. → Siano $n \in \mathbb{Z}^{>0}$, K un campo di caratteristica nulla che contiene n radici n -esime dell'unità, K'/K un'estensione finita. Supposto che $K' = K(v)$ con $v \in K' \setminus K$ e che $v^n \in K$, allora:
 1. K'/K è di Galois
 2. $\text{Gal}(K'/K)$ è ciclico
- 184 → Come si comporta la risolubilità rispetto alle operazioni sui gruppi? → I sottogruppi di gruppi risolubili sono risolubili e le immagini di gruppi risolubili mediante morfismi di gruppi sono risolubili
- 185 → Enuncia il lemma sui generatori di S_n → Le permutazioni (12) e $(12\dots n)$ generano S_n . Inoltre se p è primo, un p -ciclo qualsiasi ed una trasposizione qualsiasi generano S_p
- 186 → Enuncia il lemma sui sottogruppi transitivi di S_p con p primo → Preso un sottogruppo transitivo $G \leq S_p$, cioè che agisce transitivamente su $\{1, \dots, p\}$, G contiene un p -ciclo
- 187 → Enuncia il teorema della condizione sufficiente per la non solubilità per radicali → preso $f \in \mathbb{Q}[X]$ un polinomio irriducibile di grado $p \geq 5$, p primo. Se f ha esattamente $p - 2$ radici reali allora $\text{Gal}(f) = S_p$ ed f non è risolubile per radicali

- 188 → Enuncia il teorema sulle estensioni di campi finiti → Sia p un primo e siano n, m naturali. Allora
 1. Se E/F è un'estensione con $|F| = p^n$ e $|E| = p^m$, allora $n|m$
 2. Se $n|m$, allora esiste un'estensione $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$, unica a meno di isomorfismo.
- 189 → Ogni estensione di campi finiti è → di Galois
- 190 → Se E/F è un'estensione con $|E| = p^m$ e $|F| = p^n$, p primo, e $m = nr$, allora $\text{Gal}(E/F) \rightarrow$ è un gruppo ciclico di ordine r generato da ϕ^n dove ϕ è il morfismo di Frobenius