- 1→ Qual è la definizione di azione sinistra? → Dato un gruppo G e un insieme X definisco AZIONE DI X SU G un'applicazione $A : G \times X \to X$ 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 $A : G \times V \to V : (f, v) \mapsto f(v)$
- 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 $A : G \times X \to X : (g, x) \mapsto g \cdot x$, posso definire un morfismo $\alpha : G \to S_X$ ponendo $\alpha(g)$ la funzione $X \to X : x \mapsto A(g, x)$. (Cioè quindi $\alpha(g)(x) := A(g, x)$) (da dimostrare che αè ben definita).
  Viceversa, dato $\alpha : G \to S_X$ 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 $\mathrm{SO}(3) \curvearrowright \mathbb{R}^3$? → Le sfere sono G-invarianti
- 7→ Come si comportano i sottogruppi di un gruppo che agisce su un insieme? → Agiscono anche loro sullo stesso inseme con la restrizione dell'azione
- 8→ Qual è la definizione di G-ORBITA di $x \in X$? → È $Gx = \{g \cdot x \forall g \in G\}$
- 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 sessa 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 $f : X \to Y$ due G-insiemi t.c. $f(g \cdot x) = g \cdot f(x)$

- 22$\rightarrow$ Quando due insiemi sono ISOMORFI come G-insiemi? $\rightarrow$ Quando esiste una funzione biunivoca ed equivariante tra loro
- 23$\rightarrow$ Enuncia il lemma di caratterizzazione degli spazi omogenei $\rightarrow$ $G \curvearrowright X$ transitiva, preso $x_0 \in X$ e posto $H := G_{x_0}$ allora $X \cong G/H$ come G-insieme
- 24$\rightarrow$ La classe dei G-insiemi è una $\rightarrow$ Categoria, G–**insiemi** con
  Obj(G $-ins.$) $= \{X$ insiemi con una fissata G-azione$\}$ e
  $\forall X, Y$ G-ins.: $\mathrm{Mor}(X,Y) = \{f : X \to Y$ equivarianti$\}$
- 25$\rightarrow$ Enuncia che relazione collega lo stabilizzatore di un elemento con la sua orbita $\rightarrow$ $Gx \cong G/G_x$ come G-ins.
- 26$\rightarrow$ Qual è la definizione di punto fisso di un'azione? $\rightarrow$ 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$\rightarrow$ x è un punto fisso $\Leftrightarrow$ c1::$G_x = G$ $\rightarrow$ clz
- 28$\rightarrow$ Qual è la definizione di azione fedele? $\rightarrow$ Posto $\alpha : G \to S_X$ il morfismo associato a $G \curvearrowright X$, dico che l'azione è FEDELE quando α è iniettivo
- 29$\rightarrow$ Data un'azione $\alpha : G \to S_X$ generica, costruisci un'azione fedele. $\rightarrow$ Dato che α è un morfismo, $\exists! \beta : G/\operatorname{Ker}(\alpha) \to S_X$ iniettivo, che induce quindi un'azione fedele.
- 30$\rightarrow$ Enuncia una caratterizzazione di azione fedele $\rightarrow$ $G \curvearrowright X$ è fedele $\Leftrightarrow$ $\forall g \in G \setminus e$ $\exists x \in X : g \cdot x \neq x$
- 31$\rightarrow$ È $GL(V) \curvearrowright \mathbb{P}(V)$ effettiva? $\rightarrow$ No perché $f := x \to \lambda x$ è t.c. $f \neq id_V$ e $\alpha(f) = id_V$
- 32$\rightarrow$ Se $G \curvearrowright X$ qual è la definizione di punto io di un $g \in G$? $\rightarrow$ $G \curvearrowright X$, dico che $x \in X$ è PUNTO FISSO di $g \in G$ quando $g \cdot x = x$.
- 33$\rightarrow$ Qual è la definizione di azione libera? $\rightarrow$ $G \curvearrowright X$ è LIBERA quando $\forall g \in G, g \neq e$ vale che g non ha punti fissi
- 34$\rightarrow$ Enuncia una caratterizzazione di azione fedele $\rightarrow$ $G \curvearrowright X$ è LIBERA $\Leftrightarrow$ $\forall g \in G \setminus e, \forall x \in X : g \cdot x \neq x$
- 35$\rightarrow$ Qual è la definizione di sistema di rappresentanti? $\rightarrow$ X insieme, $\sim$ relazione di equivalenza su X, dico SISTEMA DI RAPPRESENTANTI un insieme $S \subseteq X$ t.c. $\pi_{|_S} : S \to X/\sim$ (proiezione canonica) è biettiva.
- 36$\rightarrow$ Enuncia l'equazione delle orbite $\rightarrow$ X, G finiti, $G \curvearrowright X$, sia $S = x_1, ..., x_k$ un sistema di rappresentanti per la relazione "essere nella stessa orbita", allora $\#X = \sum_{i=1}^{k} \#G/\#G_{x_i}$
- 37$\rightarrow$ Enuncia cosa è l'azione per traslazione $\rightarrow$ È l'azione $G \curvearrowright G :$ $g \cdot x := gx$
- 38$\rightarrow$ Enuncia qual è l'azione per moltiplicazione a destra. $\rightarrow$ È l'azione $G \curvearrowright G : g \cdot x := xg^{-1}$
- 39$\rightarrow$ Qual è la definizione di azione destra? $\rightarrow$ È una funzione $X \times G \to X : (x, g) \mapsto x \cdot g$ che verifica $x \cdot e = x;$ $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 g_2)$
- 40$\rightarrow$ Come posso passare da un'azione destra ad un'azione sinistra (o viceversa?) $\rightarrow$ Se $B : X \times G \to X$ è un'azione destra, allora $A : G \times X \to X : A(g,x) := B(x, g^{-1})$ è un'azione sinistra
- 41$\rightarrow$ Enuncia qual è l'azione di $G \curvearrowright G$ per coniugio $\rightarrow$ È l'azione $G \curvearrowright G :$ $g \cdot x := gxg^{-1}$

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

- 61$\rightarrow$ Quanti generatori ha un gruppo ciclico $G =< g > \quad o(G) = n$? $\rightarrow$ Sono tanti quanto i naturali $\leq n$ che non dividono n, cioè $\varphi(n)$
- 62$\rightarrow$ Caratterizza i sottogruppi di ordine $d|n$ di un gruppo ciclico G $\rightarrow$ Sono gli $H < G$ t.c. $H =< g^{n/d} >$, questo esiste ed unico $\Leftrightarrow d|n$
- 63$\rightarrow$ Enuncia la FORMULA DI GAUSS $\rightarrow \sum\limits_{d:d|n} \varphi(d) = n$
- 64$\rightarrow$ Dai una condizione sui sottogruppi di un gruppo G sufficiente affinché esso sia ciclico $\rightarrow$ G gruppo, $o(G) = n$, se $\forall d|n$ esiste al più un sottogruppo di ordine d, allora G è ciclico
- 65$\rightarrow$ Dai la definizione di G^d e una condizione su di ess affinché il gruppo G sia ciclico $\rightarrow G^d = \{x \in G \mid x^d = 1\}$. Se $\forall d \mid n: \ |G^d| \leq d \Rightarrow \ G$ è ciclico.
- 66$\rightarrow$ Dai delle condizioni sufficienti per trovare dei sottogruppi di un gruppo abeliano $\rightarrow$ G gruppo *abeliano*, $o(G) = n, \ d|n \Rightarrow \ \exists H \leq G: \ o(H) = d$
- 67$\rightarrow$ Cosa puoi dire dei sottogruppi di gruppi ciclici e abeliani? $\rightarrow$
  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$\rightarrow$ Enuncia il teorema di Sylow$\rightarrow$ 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. $n_p \equiv 1 \mod p$ e $n_p \mid n$
- 69$\rightarrow$ Enuncia il lemma che ti permette di trovare dei p-sylow di un sottogruppo $\rightarrow$ G gruppo finito, H sottogruppo e Pp-sylow $\Rightarrow \ \exists x \in G: \ xPx^{-1} \cap H$ è un p-sylow di H
- 70$\rightarrow$ Dati $P, H < G$, come può agire $P \times H$ su G ? Di' chi è lo stabilizzatore di un elemento$\rightarrow$ $P \times H \curvearrowright G: \ (a, h) \cdot x = axh^-1$, 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$\rightarrow$ Enunciai il corollario del lemma sui p-sylow dei sottogruppi $\rightarrow$ $H \leq G$, G ha un p-sylow $\Rightarrow$ anche H ha un p-sylow
- 72$\rightarrow$ Dai un'idea di quale sia la strategia per dimostrare il teorema di Sylow $\rightarrow$ Eseguo 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$\rightarrow$ Qual è la cardinalità di $GL(n, F_p)$ con p primo e $F_p = \mathbb{Z}/p$? $\rightarrow$ È $\prod_{i=0}^{n-1}(p^n - p^i)$
- 74$\rightarrow$ Enuncia una caratterizzazione dei gruppi di ordine un quadrato di un primo $\rightarrow$ 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$\rightarrow$ 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$\rightarrow$ Esibisci il morfismo iniettivo da $S_n \hookrightarrow GL(n, F_p)$ $\rightarrow$ È il morfismo che manda $\sigma \mapsto \varphi(\sigma) := (e_{\sigma(1)}|...|e_{\sigma(n)})$ cioè che manda un morfismo nella matrice identità con le colonne permutate.
- 77$\rightarrow$ Descrivi il funtore dalla categoria degli insiemi alla categoria degli spazi vettoriali su un campo fissato $\rightarrow$ È una mappa della forma $\mathbf{Set} \overset{\alpha}{\rightarrow} \mathbf{Vec}(F) : \mathrm{Mor}_{\mathbf{Set}}(X,Y) = \{f : X \rightarrow Y\} \overset{\alpha}{\rightarrow} \{f^* : F^Y \rightarrow F^X\} = \mathrm{Mor}_{\mathbf{Set}}(\alpha(X), \alpha(Y)) : f \mapsto f^*$, con $f^* : F^Y \rightarrow F^X : u \mapsto u \circ f$ È un funtore controvariante
- 78$\rightarrow$ Descrivi il processo di linearizzazione di un'azione $\rightarrow$???
- 79$\rightarrow$ 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$\rightarrow$ 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$\rightarrow$ Dato un p-gruppo, esibisci dei suoi sottogruppi $\rightarrow$ $\#G = p^\alpha,\ p$ primo $\Rightarrow\ \forall i = 0, ..., \alpha\ \exists H < G :\ \#H = p^i$
- 82$\rightarrow$ Enuncia il lemma che caratterizza il prodottoNH di due sottogruppi $N, H < G$, data la funzione $f : N \times H \rightarrow G,\ f(n,h) := nh$ $\rightarrow$
  1. $\mathrm{Im}(f) = NH$
  2. $nh \in \mathrm{Im}(f)$ e $f^{-1}(nh) = \{(nx, x^{-1}h) \mid x \in N \cap H\}$
  3. $|NH| = |N||H|/|N \cap H|$
  4. $N \lhd G \Rightarrow\ NH < G$
  5. $N, H \lhd G \Rightarrow\ NH \lhd G$
  6. Se $N, H \lhd G \Rightarrow\ [N, H] \subseteq N \cap H$
  7. Se $H, N \lhd G, N \cap H = \{1\}\ \Rightarrow\ NG \cong N \times H$
- 83$\rightarrow$ Enuncia la proposizione sull'equivalenza tra il prodotto diretto interno ed esterno $\rightarrow H, G \lhd G, N \cap H = \{1\}, NH = G \Rightarrow\ N \cong N \times H$.
  D'altro lato, se pongo $N \times H =: K$ ho: $\bar{N} := N \times \{1\} \lhd K,\ \bar{H} := \{1\} \times H \lhd K$ sono tali che $\bar{N} \cap \bar{H} = \{(1,1)\} e K = \bar{N}\bar{H}$
- 84$\rightarrow$ Enuncia il lemma di caratterizzazione del prodotto di un numero finito arbitrario di gruppi $\rightarrow G$ gruppo, $N_1, ..., N_k \lhd G$ tali che $N_i \cap (N_1 \cdot ... \cdot \hat{N_i} \cdot ... \cdot N_k) = \{1\}\ \Rightarrow\ f : N_i \times ... \times N_k \rightarrow N_1 \cdot ... \cdot N_k : (n_1, ..., n_k) \rightarrow n_1 \cdot ... \cdot n_k$ è un isomorfismo
- 85$\rightarrow$ 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$\rightarrow$ Enuncia il teorema di caratterizzazione dei gruppi con p-sylow unici $\rightarrow G$ gruppo finito, $o(G) = p_1^{\alpha_1}...p_k^{\alpha_k},\ \ p_i$ primi, se tutti i p-sylow sono unici $\Rightarrow$ posti $P_1, ..., P_k$ gli unici p-sylow ho che $G \cong P_1 \times ... \times P_k$
- 87$\rightarrow$ Cosa puoi dire su n_p se il p-sylow è normale? $\rightarrow$ Ho che $P \lhd G\ \Leftrightarrow\ n_p = 1$
- 88$\rightarrow$ Enuncia la proposizione di caratterizzazione dei gruppi con ordine un prodotto di

primi $\to$ 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$\to$ Illustra la ostruzione del prodotto semidiretto interno di gruppi $\to$ Dati un gruppo G, $N \lhd H$ ed un sottogruppo H di G, tali che $G = NH$, $N \cap H = \{e\}$ ho che $f : N \times H \to G$ 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 $\varepsilon_h : N \to N$, $\varepsilon_h(n) = hnh^{-1}$. 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$\to$ Enuncia il teorema sul prodotto semidiretto esterno $\to$ Dati N ed H gruppi e $\theta : H \to \operatorname{Aut} N : h \to \theta_h$ un morfismo. Definiamo su $N \times H$ il prodotto $\bullet_\theta$ 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

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

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

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

allora l'applicazione

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

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 $\alpha \in \operatorname{Aut} G$ 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-sylow 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 $N \lhd G$ 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

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

tale che $g_{i+1} \lhd G_i$ 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 $D^0 G := G,\ D^{i+1} G := [D^i G, D^i G]$, tale che $G = D^0 G \supset D^1 G \supset ... \supset D^i G \supset D^{i+1} G \supset ...$
- 99→ Un gruppo abeliano finito è semplice se e solo se → È ciclico di ordine finito. ciao
- 99.1→ Un gruppo G è risolubile se e solo se → esiste un numero n tale che $D^n G = \{e\}$.
- 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

  →clz
- 100→ Cos'è la caratteristica di un anello? → Preso un anello A esiste sempre un morfismo $\phi : \mathbb{Z} \to A : n \mapsto \phi(n) = n \cdot 1_A$. 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 $n = \operatorname{car} K$
- 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 $i : F \to E$ 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" $F \times A \to A$ 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 $[E : K] = ?$ → $= [E : F] \cdot [F : K]$
- 115→ Come costruisco un'estensione che contenga una radice di un polinomio irriducibile? → F campo, f irriducibile, allora la composizione $F \hookrightarrow F[X] \to K := F[X]/(f)$ 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 $p(x) \not\equiv 0, p(\alpha) = 0$. 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 $m_{\alpha,F}$,o 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 $\{1, \alpha, ..., \alpha^{d-1}\}$ 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 $F(\alpha) = \operatorname{im} \varphi_\alpha = v_\alpha(F[X])$
- 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 $\sigma : K \to L$, e un polinomio $f = \sum a_i x^i$, cosa indica f^σ?→ $f^\sigma = \sum \sigma(a_i)x^i$
- 129→ Dato $\sigma : K \to L$ un morfismo di campi, presi $K' = K(\alpha)$ un'estensione semplice algebrica, e f il polinomio minimo di α, allora:

  1. c1::se $\sigma' : K' \to L$ 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 $\sigma' : K \to L$ 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 $\sigma : K \to L$ un morfismo. Allora esiste sempre un morfismo $\sigma' : K' \to L$ 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:

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

- 135$\to$ Qual è la definizione di campo di spezzamento di un polinomio$\to$ 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$\to$ Come si caratterizzano i campi di spezzamento? $\to$ E è di spezzamento di f se e solo se f si spezza su E ed E è generato dalle radici di f : $E = F(\alpha_1, ..., \alpha_n)$
- 137$\to$ Esiste sempre il campo di spezzamento di un polinomio non costante? $\to$ 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 $d|[E : F]$
- 138$\to$ Cosa succede se ho due campi di spezzamento dello stesso polinomio $f \in F[X]$$\to$ Se ho due campi di spezzamento $E/F, E'/F$, allora per ogni morfismo F-lineare $\eta : E \to \bar{E}'$ si ha $\eta(E) = E'$. Da questo scende che il campo di spezzamento di un polinomio è unico a meno di isomorfismo
- 139$\to$ Qual è la definizione di estensione NORMALE? $\to$ 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$\to$ Un'estensione algebrica E/F è normale sse per ogni $\alpha \in E$ $\to$ il polinomio minimo $m_{\alpha,F}$ si spezza su E.
- 141$\to$ Enuncia il teorema di caratterizzazione delle estensioni finite normali $\to$ Data un'estensione E/F finita, le seguenti condizioni sono equivalenti:

  1. Ogni morfismo F-lineare $\eta : E \to \bar{E}$ 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$\to$ Se ho una catena di campi $K \subseteq L \subseteq M$, come si comporta la normalità? $\to$ Se M/K è normale, allora anche M/L lo è
- 143$\to$ Qual è la definizione di polinomio SEPARABILE? $\to$ Un polinomio a coefficienti in un campo F è separabile se non ha radici multiple in nessuna estensione di F
- 144$\to$ Qual è la definizione di ELEMENTO SEPARABILE? $\to$ 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$\to$ Qual è la definizione di ESTENSIONE SEPARABILE? $\to$ È un'estensione E/F in cui ogni elemento di E è separabile
- 146$\to$ Se $f \in F[X]$ è irriducibile e non separabile, allora $\to$ $f' \equiv 0$
- 147$\to$ Qual è la definizione di CAMPO PERFETTO?$\to$ È un campo per cui le tutte le sue estensioni algebriche sono separabili
- 148$\to$ Cosa succede ai polinomi sui campi di caratteristica zero? $\to$ 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$\to$ 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

$\to$ clz

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

1. c1::l'azione di $\mathrm{Gal}(E/F)$ è fedele
2. c2::se f è irriducibile, allora $\mathrm{Gal}(E/F)$ agisce transitivamente sulle radici di f

$\to$ clz

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

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

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

$\to$

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

$$\begin{aligned} \sigma : \mathscr{K} \to \mathscr{S} \quad & \sigma(K) := \operatorname{Gal}(E/K) \\ \tau : \mathscr{S} \to \mathscr{K} \quad & \tau(G) := E^G \end{aligned}$$

- 169$\to$ Cosa vale sempre per le composizioni $\tau\sigma$ e $\sigma\tau$ della corrispondenza di Galois? $\to$
  1. Per ogni $K \in \mathscr{K}$ si ha che $K \subseteq \tau\sigma(K) = E^{\operatorname{Gal}(E/K)}$
  2. Per ogni $G \in \mathscr{S}$ si ha $G = \sigma\tau(G)(= \operatorname{Gal}(E/E^G))$
- 170$\to$ Enuncia il teorema fondamentale della teoria di Galois, I parte$\to$ 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$\to$ Enuncia il teorema fondamentale della teoria di Galois, II parte$\to$ Sia E/F un'estensione di Galois, e sia $K \in \mathscr{K}$. Allora K/F è di Galois se e solo se $\operatorname{Gal}(E/K) \lhd \operatorname{Gal}(E/F)$. In al caso

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

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

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

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

- 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 → $\mathrm{Gal}(E/F)$ 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, $v_1, ..., v_n$ sono elementi di un'estensione di K', allora → anche l'estensione $K'(v_1, ..., v_n)/K(v_1, ..., v_n)$ è radicale
- 181→ Siano E/F un'estensione, K, L campi intermedi eKL 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 $\mathrm{Gal}(F(\mu_n)/F)$ 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. $\mathrm{Gal}(K'/K)$ 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 $(12...n)$ 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 $\{1, ..., p\}$, 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 $\mathrm{Gal}(f) = S_p$ ed f non è risolubile per radicali

- 188$\rightarrow$ Enuncia il teorema sulle estensioni di campi finiti $\rightarrow$ 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$\rightarrow$ Ogni estensione di campi finiti è $\rightarrow$ di Galois
- 190$\rightarrow$ Se E/F è un'estensione con $|E| = p^m$ e $|F| = p^n$, p primo, e $m = nr$, allora $\mathrm{Gal}(E/F) \rightarrow$ è un gruppo ciclico di ordine r generato da ϕ^n dove ϕ è il morfismo di Frobenius