1. Diario approssimativo delle lezioni

Lezione 1; lun. 3/10; 2 ore.
Presentazione del programma.
Richiami sui polinomi: distribuzione esercizi sui polinomi, correzione esercizi 9 e 18 e osservazioni sulla riduzione modulo p.
Serie formali: definizione delle serie formali e delle serie formali di Laurent e loro proprietà elementari, distribuzione esercizi sulle serie formali.

Lezione 2; mer. 5/10; 2 ore.
Correzione 19, 20, 21.
Invertibilità di una serie formale e esercizi sulle serie formali.
Polinomi simmetrici: definizione, funzioni simmetriche elementari e polinomi di Newton, risolvente $R(f, x)$.

Lezione 3; gio. 6/10; 1 ora.
Teorema fondamentale sui polinomi simmetrici: $A[x_1, \dots, x_n]^{\mathsf{S}_n} = A[e_1, \dots, e_n]$.
Discriminante.
Matrice di Vandermonde: definizione e calcolo del determinante della matrice di Vandermonde.

Lezione 4; lun. 10/10; 1 ora.
Correzione esercizi 31, 32, 35, 38, 39

Lezione 5; mer. 12/10; 1 ora.
Correzione esercizi 44, 45, 46, 36, 37.

Lezione 6; gio. 13/10; 1 ora.
Richiami da Algebra 2. Elementi algebrici e trascendenti, polinomio minimo, estensioni finite e estensioni algebriche, grado, morfismi di campi. Correzione esercizio 65

Lezione 7; lun. 17/10; 2 ore.
Richiami dalla lezione 6: morfismi di campi e gruppo di Galois. Correzione esercizio 76.
Discriminante di $x^3 + px + q$ (esercizio 41). Definizione di $R(F, f)$.
Campi di spezzamento.
Campi algebricamente chiusi, chiusure algebriche.

Lezione 8; lezione mer. 19/10; 2 ore.
estensioni separabili: elementi separabili, polinomi separabili, grado di separabilità.
$[F : E]_s \leqslant [F : E]$ e vale $=$ se e solo l'estensione è separabile

La lezione di gio. 20/10 che doveva svolgersi in Piazza della chiesa nuova è saltata causa pioggia.

Lezione 9; lun. 24/10; 2 ore.
Assioma della scelta e Lemma di Zorn.
Chiusura algebrica e estensioni di morfismi.
Estensioni normali e estensioni di Galois.
$card\,\mathrm{Gal} \leqslant grado$ e vale $=$ se e solo l'estensione è di Galois.

Lezione 10; mer. 26/10; 2 ore.
correzione esercizio 102.
separabilità di un suo polinomio e derivata; correzione esercizio 101.
campi perfetti in car. p e morfismo di Frobenius, correzione esercizi 106 e 107 .
estensioni normali e campi di spezzamento.
$F^{\mathrm{Gal}(F:E} = E$ se l'estensione è di Galois.

Lezione 11; gio. 27/10; 2 ore.
Correzione esercizio 109, 115 e 116.
Lemma di Artin.
Teorema fondamentale della teoria di Galois

Lezione 12; lun. 31/10; 2 ore.
Correzione esercizio 119.
Estensioni risolubili per radicali: enunciazione del problema
Estensioni cicliche

Lezione 13; mer. 2/11; 2 ore.
Correzione esercizio (chiusura normale)
Risoluzione effettiva nel caso ciclico
gruppi risolubili
Equivalenza tra risolubilità del gruppo di Galois risolubile e risolubilità per radicali del polinomio (in car. 0 e con radici di 1).

Lezione 14; gio. 3/11; 1 ora.
Gruppo di Galois del polinomio generico
Esempi di polinomi con gruppo di Galois S_p su $\mathbb{Q}$

Lezione 15; lun. 7/11; 2 ore.
Esr. 117, 118
Sottogruppi finiti di $\Bbbk^*$, esr. 127
Estensioni primitive Esr. 123, 124, 125
Estensioni ciclotomiche per $n = p$ primo, esr. 128
Gruppo di Galois di un prodotto

Lezione 16; mer. 9/11; 2 ore.
Esr. 129
Come si calcola il gruppo di Galois quando non si sanno calcolare le radici
Il discriminante
quando un polinomio di quarto grado ha gruppo di Galois D_4

Lezione 17; gio. 10/11; 1 ora.
risolventi (richiami dalle prime lezioni) applicazione a polinomi di quarto grado

Lezione 18; lun. 21/11; 2 ore.
correzione esr. 131
Risolventi con radici distinte.

Lezione 19; mer. 23/11; 2 ore.
correzione esercizi 135, 136, 137, 138.
irriducibilita' del polinomio ciclotomico φ_n, n qualsiasi. Calcolo del gruppo di Galois dell'estensione ciclotomica.

Lezione 20; gio. 24/11; 1 ora.
Infinitezza dei primi congrui a 1 modulo n.
Descrizione di $(\mathbb{Z}/n)^*$.

Lezione 21; lun. 28/11; 2 ore.
Correzione esercizi 132 e 142.
Estensioni di grado 2 di $\mathbb{Q}$ contenute in $\mathbb{Q}(\zeta_p)$.
Simbolo di Legendre e reciprocità quadratica.

Lezione 22; mer. 30/11; 2 ore.
reciprocità quadratica e fattorizzazione dei primi in $A = \mathbb{Z}[\sqrt{n}]$, primi della forma $x^2 - n\,y^2$ (discussione assumendo l'ipotesi quasi mai verificata A euclideo).
Traccia, norma, e polinomio caratteristico.

Lezione 23; gio. 1/12; 1 ora.
Hilbert 90 e altre osservazioni su traccia e norma.

Lezione 24; lun. 5/12; 2 ore.
Correzione esercizi 144, 148
moduli su anello, $\mathbb{Z}$-moduli e gruppi abeliani, sottomoduli, quozienti, orfismi di moduli, moduli ciclici, moduli finitamente generati,

Lezione 25; mer. 7/12; 2 ore.
Correzione esercizio 147
moduli e anelli noetheriani, teorema della base di Hilbert

Lezione 26; lun. 12/12; 2 ore.
Correzione esercizi 149, 150, 153
Torsione e p-torsione.
morfismi tra moduli liberi e finitamente generati su anelli ad ideali principali.

Lezione 27; mer. 14/12; 2 ore.
moduli finitamente generati su anelli ad ideali principali.

Lezione 28; gio. 15/12; 1 ora.
unicità della decomposizione in moduli.
Endomorfismi di uno spazio vettoriale e $\Bbbk[t]$-moduli.

Lezione 29; lun. 19/12; 2 ore.
polinomio minimo, forma canonica razionale e forma di Jordan;
endomorfismi che commutano.

Lezione 30; mer. 21/12; 2 ore.
estensioni di Kummer.

Lezione 31; lun. 9/1; 2 ore.
prima forma del teorema degli zeri di Hilbert.

Lezione 32; mer. 11/1; 2 ore.
varietà algebriche affini.

Lezione 33; gio. 12/1; 1 ora.
forma forte del teorema degli zeri di Hilbert.

Lezione 34; lun. 16/1; 2 ore.
correzione esercizi 154, 156, 157

Lezione 35; mer. 18/1; 2 ore.
correzione esercizi 159, 160, 161, 163

2. Programma

Per chi deve preparare l'esame il modo migliore per farsi un'idea degli argomenti affrontati nel corso e del tipo di compito che può trovarsi di fronte è quello di guardare la lista degli esercizi dati durante l'anno.

Prima parte.

- criterio di Eisenstein;
- serie formali e serie di Laurent;
- invertibilità di una serie formale;
- polinomi simmetrici;
- risolvente $R(F, x)$ e $R(F, f)$;
- funzioni simmetriche elementari;
- polinomi di Newton;
- $A[x_1, \dots, x_n]^{\mathsf{S}_n} = A[e_1, \dots, e_n]$;
- discriminante e sua radice quadrata;
- matrice di Vandermonde e suo determinante;
- espressione esplicita del discriminante in funzione dei polinomi di Newton;
- gruppo di Galois;
- elementi di Liouville;
- campi algebricamente chiusi e chiusura algebrica di un campo;
- assioma della scelta, lemma di Zorn ed esistenza della chiusura algebrica;
- estensioni di morfismi tra estensioni algebriche;
- estensioni separabili, elementi separabili, polinomi separabili;
- grado di separabilità e confronto con il grado usuale;
- polinomi separabili e derivate;
- campi perfetti in car. p e morfismo di Frobenius;
- estensioni normali e estensioni di Galois, chiusura normale;
- estensioni normali e campi di spezzamento;
- estensioni di Galois e cardinalità del gruppo di Galois;
- $F^{\mathrm{Gal}(F:E)} = E$ se l'estensione è di Galois;
- lemma di Artin;
- calcolo di gruppi di Galois;
- corrispondenza campi intermedi sottogruppi;
- estensioni cicliche;
- estensioni risolubili per radicali e estensioni risolubili (in car. 0 e con radici di 1);
- gruppo di Galois del polinomio generico;
- esempi di polinomi con gruppo di Galois S_p su $\mathbb{Q}$;
- sottogruppi ciclici di $\Bbbk^*$;
- estensioni primitive;
- gruppo di Galois di un prodotto;
- osservazioni su polinomi di terzo e quarto grado (quando un polinomio di quarto grado ha gruppo di Galois contenuto in D_4);
- il caso di risolventi con radici distinte;
- estensioni ciclotomiche e polinomi ciclotomici φ_n, n qualsiasi;
- traccia, norma e polinomio caratteristico di un elemento;
- Hilbert 90;

Per gli argomenti coperti in questa prima parte si può guardare il libro di Lang "Algebra" e le note "Polinomi simmetrici" che potete scaricare dalla mia homepage. Le parti del libro di Lang in questione sono: il capitolo "Algebraic extensions" tranne la parte sulle estensioni puramente inseparabili, e il capitolo "Galois theory" (i paragrafi 1, 2, 3, 4, 5, 6, 7). Molti altri libri di teoria di Galois coprono lo stesso materiale e quindi vanno bene, rispetto ad altri l'impostazione generale del Lang è più simile a quella che abbiamo seguito a lezione.

Seconda parte. La seconda parte del corso è stata dedicata a dei complementi. In parte si è trattato di piccole applicazioni della teoria di Galois alla teoria dei numeri e in parte di argomenti standard di algebra commutativa e algebra lineare collegati con la parte di teoria di Galois che stavamo sviluppando.

- descrizione di $(\mathbb{Z}/n)^*$;
- esistono infiniti primi congrui a 1 modulo n;
- estensioni di grado 2 di $\mathbb{Q}$ contenute in $\mathbb{Q}(\zeta_p)$;
- reciprocità quadratica;
- reciprocità quadratica e fattorizzazione di primi in estensioni quadratiche;
- moduli su anelli, modulo generato, moduli ciclici, moduli semplici, quozienti di moduli, morfismi di moduli;
- moduli noetheriani e anelli noetheriani;
- teorema della base di Hilbert;
- classificazione dei moduli su un anello ad ideali principali;

- forma canonica razionale e forma di Jordan di un endomorfismo lineare;
- polinomio minimo di un endomorfismo lineare e criteri di diagonalizzabilità;
- endomorfismi lineari che commutano;
- estensioni di Kummer;
- varietà algebriche affini;
- teorema degli zeri di Hilbert.

Per questa seconda parte la cosa migliore sarebbe avere gli appunti perché riguardano materiale un po' sparso in giro. Altrimenti queste sono alcuni possibili referenze: (il conto fondamentale sulla reciprocità quadratica lo trovate sul Lang al paragrafo sulle estensioni ciclotomiche), le estensioni di Kummer le trovate sono sempre un paragrafo del Lang (anche se la dimostrazione del Lang è un po' diversa), la parte sui moduli su un anello ad ideali principali sull'Artin (algebra) anche se forse fa solo il caso euclideo e anche sull'Hernstein (algebra) così come la sua applicazione alle applicazioni lineari. Lo stesso materiale si trova anche sul libro di Lang ma non nella parte sui campi ma su quella (nella mia edizione) sulle applicazioni lineari.

3. Esercizi corretti o svolti in qualche forma in classe

9, 18, 19, 20, 21,22, 23, 24, 25, 26, 27, 28, 29, 31, 32, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 53, 71, 76, 80, 82, 84, 91, 2, 93, 96, 97, 98, 99, 101, 102, 106, 107, 109, 110(3), 111, 112, 113, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 127, 128, 129, 131, 135, 136, 137, 138, 142, 144, 147, 148, 149, 150, 153, 154, 156, 157, 160, 161, 163

4. Esercizi e richiami sugli anelli

Il contenuto dei seguenti esercizi e delle seguenti definizioni dovrebbe essere (circa) noto.

Definizione. Sia A un anello, un elemento $a \in A$ si dice

i) invertibile se esiste $b \in A$ tale che $ba = 1$;
ii) irriducibile se non è invertibile e se $\forall\, b, c \in A$ se $bc = a$ allora b è invertibile o c è invertibile;
iii) primo se non è invertibile e se $\forall\, b, c \in A$ se a divide bc allora a divide b o a divide c;

Un anello A si dice un dominio se per ogni $a, b \in A$ $ab = 0$ implica $a = 0$ o $b = 0$.

Un dominio A si dice un anello fattoriale se ogni elemento a in A si può scrivere in modo "essenzialmente" unico come prodotto di irriducibili: più precisamente se

i) per ogni $a \in A$ non nullo e non invertibile esistono $p_1, \dots, p_n$ irriducibili tali che $a = p_1 p_2 \cdots p_n$;
ii) se $p_1, \dots, p_n, q_1, \dots, q_m$ sono irriducibili e $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ allora $n = m$ e esiste una permutazione σ di $\{1, \dots, n\}$ e $b_1, \dots, b_n$ invertibili tali che $p_i = b_i q_{\sigma(i)}$ per $i = 1, \dots, n$.

Esercizio 1. Far vedere che primo implica irriducibile ma che il viceversa non è sempre vero (si consideri $\mathbb{Q}[t^2, t^3]$).

Esercizio 2. Far vedere che in un anello fattoriale irriducibile implica primo.

Esercizio 3. Dimostrare che un dominio è fattoriale se e solo

i) per ogni $a \in A$ non nullo e non invertibile esistono $p_1, \dots, p_n$ irriducibili tali che $a = p_1 p_2 \cdots p_n$;
ii) $\forall\, p \in A$ p è primo se e solo se p è irriducibile

Definizione. Sia A un anello commutativo e unitario (questo spesso per noi sarà sottointeso). Un sottoinsieme I di A si dice un ideale se

i) $0 \in I$;
ii) $\forall\, a, b \in I$ $a + b \in I$ e $-a \in I$;
iii) $\forall\, a \in A$ e $\forall\, b \in I$ $ab \in I$.

In particolare I possiamo considerare il quoziente che si indica A/I di A rispetto alla relazione di equivalenza

$$a \equiv b \text{ se e solo se } a - b \in I.$$

Se a è un elemento di A indicheremo spesso la classe di equivalenza a cui appartiene con $\bar{a}$. È facile verificare che si può definire una somma ed un prodotto su A/I mediante

$$\bar{a} + \bar{b} = \overline{(a + b)} \quad \text{e} \quad \bar{a} \cdot \bar{b} = \overline{(a \cdot b)}$$

e che l'elemento neutro rispetto alla somma è $\bar{0}$ e rispetto al prodotto è $\bar{1}$.

Se I è un ideale di A diciamo inoltre che

i) I è un ideale proprio se $I \neq A$;
ii) I è un ideale primo se è un ideale proprio e se $\forall\, a, b \in A$ se $ab \in I$ allora $a \in I$ o $b \in I$;
iii) I è un ideale massimale se è un ideale proprio e se per ogni ideale J di A se $J \supset I$ allora $J = I$ o $J = A$;

L'insieme degli ideali primi di A si indica con $\operatorname{Spec} A$ e l'insieme degli ideali massimali con $\operatorname{Max} A$.

Se $a \in A$ l'insieme di tutti gli elementi della forma ba con $b \in A$ è un ideale che si indica con (a) o con Aa. Gli ideali di questo tipo si dicono ideali principali.

Esercizio 4. Dimostrare che l'intersezione di ideali è un ideali, se S è un sottoinsieme di A possiamo quindi considerare il minimo ideale che contiene S e lo indichiamo con (S). Dimostare che se $S = \{a\}$ allora $(S) = (a)$. Dimostrare inoltre che

(1) $(a) = A$ se e solo se a è invertibile;
(2) (a) è un ideale primo se e solo se a è un elemento primo.

Ricordo che un elemento $p \in A$ si dice primo se per ogni $a, b \in A$ se p divide ab allora p divide a o p divide b.

Esercizio 5. Sia I un ideale proprio di A dimostrare che

(1) I è un ideale primo se e solo se A/I è un dominio (Ricordo che un anello B si dice un dominio se non ha divisori dello zero);
(2) I è un ideale massimale se e solo se A/I è un campo

In particolare un anello A è un campo se e solo se l'unico ideale proprio è $\{0\}$.

Esercizio 6. Dimostrare che se in un dominio tutti gli ideali sono principali allora l'anello è fattoriale.

Definizione. Siano A, B due anelli. Un morfismo (o omomorfismo) di anelli (unitari) è una applicazione $\varphi : A \longrightarrow B$ tale che $\varphi(0) = 0$, $\varphi(1) = 1$, $\varphi(x + y) = \varphi(x) + \varphi(y)$ e $\varphi(xy) = \varphi(x)\varphi(y)$ per ogni x, y.

Esercizio 7 (Teorema di omomorfismo)**.** Sia $\varphi : A \longrightarrow B$ un morfismo di anelli e sia I un ideale di A. Dimostrare che se $\varphi(I) = 0$ allora esiste ed è un unico un morfismo di anelli $\psi : A/I \longrightarrow B$ tale che $\varphi(a) = \psi(\bar{a})$ per ogni a in A.

Esercizio 8 (Teorema di omomorfismo)**.** Sia $\varphi : A \longrightarrow B$ un morfismo di anelli e sia $I = \ker \varphi$. Dimostrare che I è un ideale di A. Per l'esercizio precedente esiste un morfismo di anelli $\psi : A/I \longrightarrow B$ tale che $\varphi(a) = \psi(\bar{a})$ per ogni a in A. Dimostrare che ψ è iniettivo. Dimostrare inoltre che se φ è surgettivo allora ψ è un isomorfismo.

5. Esercizi e richiami sui polinomi (3 ottobre)

Esercizio 9 (Proprietà universale dell'anello dei polinomi)**.** Sia A un anello commutativo e sia $S = A[x_1, \dots, x_n]$ l'anello dei polinomi a coefficienti in A nelle variabili $x_1, \dots, x_n$. Dimostrare che per ogni anello commutativo B, per ogni morfismo di anelli $\varphi : A \longrightarrow B$ e per ogni scelta di $b_1, \dots, b_n \in B$ esiste ed è unico un morfismo di anelli $\phi : S \longrightarrow B$ tale che $\phi\big|_A = \varphi$ e $\phi(x_i) = b_i$.

In particolare se $\varphi : A \longrightarrow A'$ è un morfismo di anelli possiamo considerare l'estensione di φ all'anello dei polinomi su A e A' definita nel modo seguente: nella costruzione precedente consideriamo $B = A'[x_1, \dots, x_n]$ e $\phi : S \longrightarrow B$ il morfismo che ristretto a A è uguale a φ e tale che $\phi(x_i) = x_i$. Nel seguito del corso useremo spesso questa costruzione e indicheremo ϕ con lo stesso simbolo φ. Se inoltre $A = \mathbb{Z}$ e $A' = \mathbb{Z}/p$ e φ è il morfismo di anelli (unitari) da $\mathbb{Z}$ a $\mathbb{Z}/p$ allora chiameremo la mappa ϕ così costruita la riduzione di un polinomio modulo p e scriveremo $f \mod p$ o spesso semlicemente $\bar{f}$.

Esercizio 10. Sia A un anello comm. unit. e $S = A[x_1, \dots, x_n]$. Sia $a = (a_1, \dots, a_n) \in A^n$ e sia $v_a : S \longrightarrow A$ il morfismo di anelli che è l'identità su A e che manda x_i in a_i. Dimostrare che $v_a(f) = f(a)$ la valutazione di f in a.

Esercizio 11. Sia A un anello comm. unit. e $S = A[x_1, \dots, x_n]$. Sia $a = (a_1, \dots, a_n) \in A^n$ e sia $I = \{f \in S : f(a) = 0\}$. Dimostrare che I è l'ideale generato da $(x_1 - a_1, \dots, x_n - a_n)$. Dimostrare inoltre che I è un ideale primo se e solo se A è un dominio e che I è un ideale massimale se e solo A è un campo.

Esercizio 12. Se A è un dominio allora l'anello dei polinomi a coefficienti in A è un dominio.

Esercizio 13. Sia $\Bbbk$ un campo. Dimostrare che tutti gli ideali in $\Bbbk[t]$ sono principali. (Questo fatto segue dal fatto che tra polinomi si può definire la divisione con resto).

Esercizio 14 (Lemma di Gauss 1)**.** Se $f \in \mathbb{Z}[t]$ e $f = a_n t^n + \cdots + a_0$ definiamo il contenuto di f che indichiamo con $c(f)$ come il massimo comune divisore di $a_0, \dots, a_n$. Un polinomio si dice primitivo se $c(f) = 1$. Se $f, g \in \mathbb{Z}[t]$ dimostrare

1) f, g primitivi implica fg primitivo;
2) $c(fg) = c(f)c(g)$.

Esercizio 15 (Lemma di Gauss 2)**.** Sia $f \in \mathbb{Z}[t]$ dimostrare che se $f = gh$ con $g, h \in \mathbb{Q}[t]$ allora esiste $a \in \mathbb{Q} \smallsetminus \{0\}$ tale che $ag, a^{-1}h \in \mathbb{Z}[t]$.

Esercizio 16 (Lemma di Gauss 3)**.** Dimostrare che un polinomio $f \in \mathbb{Z}[t] \smallsetminus \{\pm 1\}$ è irriducibile se e solo se $c(f) = 1$ e f è irriducibile in $\mathbb{Q}[t]$.

Esercizio 17 (Lemma di Gauss 4)**.** $\mathbb{Z}[t]$ è un anello fattoriale.

Gli esercizi sul lemma di Gauss valgono senza cambiamenti per un qualsiasi anello fattoriale.

Esercizio 18 (Criterio di Eisenstein)**.** Sia $f \in \mathbb{Z}[t]$ un polinomio di grado n e sia p un numero primo. Sia $f = a_n t^n + \cdots + a_0$. Supponiamo che p divide $a_0, \dots, a_{n-1}$, che p non divide a_n e che p^2 non divide a_0. Dimostrare che f è un polinomio irriducibile.

Esercizio 19. Quali dei seguenti polinomi sono irriducibili su $\mathbb{Q}$?

a) $2x^5 + 15x^4 + 9x^3 + 3$;
b) $x^3 + 5x^2 + 3$;
c) $x^4 + 15x^3 + 15$;

[Quando è possibile provare ad applicare il criterio di Eisenstein]

Esercizio 20. Scrivere tutti i polinomi irriducibili di grado 2, 3 e 4 su $\mathbb{F}_2$ e tutti i polinomi irriducibili di grado 2 su $\mathbb{F}_3$.

Esercizio 21. $a_1, \dots, a_n$ interi distinti. Dimostrare che $(x - a_1) \cdots (x - a_n) - 1$ è irriducibile in $\mathbb{Z}[x]$.

6. Serie formali (3 ottobre)

Sia A un anello commutativo e unitario. Come insieme, l'anello delle serie formali di Laurent a coefficienti in A nella variabile t, è l'insieme $A((t))$ delle espressioni $\sum_{n=-k}^{\infty} a_n t^n$ con k un qualsiasi numero intero e $a_n \in A$. Equivalentemente è l'insieme delle espressioni $\sum_{n=-\infty}^{\infty} a_n t^n$ in cui $a_n = 0$ per n minore di un qualche intero n_0 (questo fatto si indica spesso scrivendo $a_n = 0$ per $n << 0$). Su $A((t))$ si possono definire le seguenti operazioni di somma e prodotto:

$$\Big(\sum_{n=-\infty}^{\infty} a_n t^n\Big) + \Big(\sum_{n=-\infty}^{\infty} b_n t^n\Big) = \sum_{n=-\infty}^{\infty} (a_n + b_n)\, t^n;$$

$$\Big(\sum_{n=-\infty}^{\infty} a_n t^n\Big) \cdot \Big(\sum_{n=-\infty}^{\infty} b_n t^n\Big) = \sum_{n=-\infty}^{\infty} \Big(\sum_{i,j\,:\,i+j=n} a_i\, b_j\Big)\, t^n.$$

dove $a_n = 0$ e $b_n = 0$ per $n << 0$.

Esercizio 22. Nella definizione di prodotto il coefficiente di t^n è scritto come una somma infinita, verificare che in questa somma in realtà solo un numero finito di termini è non nullo e che quindi la definizione di prodotto è ben data.

Esercizio 23. Verificare che $A((t))$ è un anello commutativo unitario con unità data da $1 = t^0$.

Se $f = \sum_{n=-k}^{\infty} a_n t^n$ non è uguale a zero il suo grado è definito come il minimo intero n per cui $a_n \neq 0$.

Esercizio 24. Sia A un dominio. Dimostrare che $A((t))$ è un dominio e che se $f, g \in A((t))$ non nulli allora $grado(f \cdot g) = grado(f) + grado(g)$.

L'anello delle serie formali a coefficienti in A nella variabile t, che si indica con $A[[t]]$, è il sottoanello di $A((t))$ delle espressioni $\sum_{n=0}^{\infty} a_n t^n$.

Esercizio 25. Verificare che $A[[t]]$ è un sottoanello di $A((t))$.

Nel caso in cui $A = \mathbb{R}$ avete probabilmente già incontrato le serie di potenze convergenti che sono un sottoinsieme di $\mathbb{R}[[t]]$ e potete riconoscere nel prodotto e nella somma definiti sopra l'usuale prodotto e somma tra funzioni. In generale ovviamente una serie formale non individua una funzione a valori in A ma è definito in ogni caso il suo valore in 0: se $f = \sum_{n=0}^{\infty} a_n t^n$ definiamo $f(0)$ come a_0.

Esercizio 26. L'applicazione $f \mapsto f(0)$ da $A[[t]]$ ad A è un omomorfismo di anelli.

Esercizio 27. Sia $f \in A[[t]]$. Dimostrare che f ammette un inverso in $A[[t]]$ se e solo se $f(0)$ è invertibile in A.

Esercizio 28. Calcolare l'inverso di $1 - t$.

Assumiamo da ora in poi che $A = \Bbbk$ sia un campo.

Esercizio 29. Dimostrare che $\Bbbk((t))$ è un campo e che è il campo dei quozienti di $\Bbbk[[t]]$.

Esercizio 30. Dimostrare che $\Bbbk[[t]]$ è un anello ad ideali principali e descrivere tutti gli ideali di $\Bbbk[[t]]$.

7. Operazioni sulle serie formali

Le serie formali hanno molte delle proprietà delle serie usuali, possiamo definire esponenziale e logaritmo o la derivata di una serie formale.

Esponenziale e logaritmo. Sia $A = \Bbbk$ una campo di caratteristica 0. Se $f = \sum_{n=0}^{\infty} a_n t^n \in \Bbbk[[t]]$ è una serie formale osserviamo che non è detto che l'espressione $\sum_{n=0}^{\infty} \frac{f^n}{n!}$ sia ben definita. Se però il grado di f è maggiore o uguale a uno l'espressione è sicuramante ben definita. Sia quindi $\mathfrak{p} = t\,\Bbbk[[t]]$ l'ideale generato da t in $\Bbbk[[t]]$ e U l'insieme degli elementi della forma $1 + f$ con $f \in \mathfrak{p}$. Possiamo definire $\exp : \mathfrak{p} \longrightarrow U$ e $\log : U \longrightarrow \mathfrak{p}$ mediante

$$\exp(f) = \sum_{n=0}^{\infty} \frac{f^n}{n!} \quad \text{e} \quad \log(1+f) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{f^n}{n}$$

Esercizio 31. Verificare che exp e log sono ben definite e che sono una l'inversa dell'altra.

Esercizio 32. Verificare che $\exp(f + g) = \exp(f) \cdot \exp(g)$.

Più in generale se $g \in A[[t]]$ (con A qualsiasi) e $g(0) = 0$ possiamo definire $g(f)$ per ogni $f \in \mathfrak{p}$.

Derivate. Se $f = \sum_{n=-k}^{\infty} a_n t^n \in A((t))$ possiamo definire la derivata $f' = \sum_{n=-k}^{\infty} n a_n t^{n-1}$. La derivata si indica anche con d/dt e la derivata n-esima con $f^{(n)}$ o con d^n/dt^n.

Esercizio 33. Dimostrare che $f \mapsto f'$ è A-lineare e che verifica la formula di Leibniz: $(fg)' = f\,g' + f'\,g$.

Esercizio 34. Se $A = \Bbbk$ è un campo di caratteristica 0 verificare che se $f \in \Bbbk[[t]]$ allora $f' \in \Bbbk[[t]]$ e

$$f = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!}\, t^n.$$

8. Esercizi sulle serie formali (5 ottobre)

Esercizio 35. Trovare una serie formale f tale che $t^2 f + tf = f - t$.

9. Esercizi sui polinomi simmetrici (6 ottobre)

Esercizio 36. Calcolare la somma dei quadrati delle radici di $x^4 - 2x^3 + x^2 - 3x + 1$. [Non c'è bisogno di calcolare le radici]

Esercizio 37. Sia $F \in B[x_1, x_2, x_3]$. Esprimere i coefficienti del polinomio risolvente $R(x_1^2, x)$ per mezzo delle funzioni simmetriche elementari.

Ricordiamo che il k-esimo polinomio di Newton nelle variabili $x_1, \dots, x_n$ è definito come

$$p_k = x_1^k + \cdots + x_n^k$$

Esercizio 38. Sia $A = \Bbbk$ un campo di caratteristica 0. Dimostrare che

$$1 - e_1 t + e_2 t^2 \cdots \pm e_n t^n = \prod_{i=1}^{n} (1 - t x_i) = e^{-\sum_k \frac{p_k}{k} t^k}$$

[dove e_i sono le funzioni simmetriche elementari nelle variabili x_i]

Questo esercizio fornisce induttivamente una formula per i polinomi di Newton p_k in funzione delle funzioni simmetriche elementari $e_1, \dots, e_n$. Altre formule apparentemente più esplicite si possono ottenere in modo analogo.

Il discriminante. Sia E un campo e sia $f \in E[t]$ un polinomio di grado n. Siano $\alpha_1, \dots, \alpha_n$ le radici di f in una estensione F di E considerate con la loro molteplicità. Definiamo il discriminante di f mediante la formula

$$\Delta(f) = \prod_{i>j} (\alpha_i - \alpha_j)^2.$$

Esercizio 39. Dimostrare che $\Delta(f) \in E$.

Esercizio 40. Nel caso di un polinomio di grado 2: $f = x^2 + bx + c$, esprimere $\Delta(f)$ in funzione dei coefficienti b e c?

Esercizio* 41. Sia $f = x^3 + px + q$. Esprimere $\Delta(f)$ in funzione di p e q.

10. La matrice di Vandermonde (6 ottobre)

La matrice di Vandermonde è la seguente matrice:

$$\mathsf{V} = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ & & \cdots & \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix}$$

Esercizio 42. Calcolare il determinante della matrice di Vandermonde nel caso $n = 2$ e $n = 3$.

Esercizio 43. Dimostrare che

$$\det \mathsf{V} = \prod_{i>j} (x_i - x_j).$$

Esercizio 44. Esistono dei numeri complessi $x_1, \dots, x_n$ non tutti nulli tali che

$$x_1 + x_2 2^m + \cdots + x_n n^m = 0 \quad \text{per } m = 0, \dots, n-1?$$

Esercizio 45. Dimostrare che se p_i sono i polinomi di Newton nelle variabili $x_1, \dots, x_n$ allora

$$\Delta(x) = \det \begin{pmatrix} n & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ p_2 & p_3 & p_4 & \cdots & p_{n+1} \\ & & \cdots & & \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{pmatrix}$$

Esercizio* 46. Calcolare l'inversa della matrice di Vandermonde.

11. Polinomi semisimmetrici

Sia $\Bbbk$ un campo di caratteristica diversa da due e sia $B = \Bbbk[x_1, \dots, x_n]$. Sia $\mathsf{A}_n \subset \mathsf{S}_n$ il sottogruppo alterno, ovvero il sottogruppo delle permutazioni pari. Diciamo che un polinomio $f \in B$ è semisimmetrico se è invariante per il gruppo A_n. Sia

$$\delta(x) = \prod_{i>j} (x_i - x_j).$$

Esercizio 47. δ è un polinomio semisimmetrico e $\sigma\delta = \varepsilon(\sigma)\delta$ per ogni $\sigma \in \mathsf{S}_n$.

Esercizio* 48. Sia $f \in B$ tale che $\sigma f = \varepsilon(\sigma) f$ per ogni $\sigma \in \mathsf{S}_n$. Allora δ divide f.

Esercizio* 49. Ogni polinomio semisimmetrico si scrive in modo unico nella forma $f + g\delta$ con f, g simmetrici.

12. Altri esercizi sui polinomi simmetrici

Esercizio 50. Siano $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ le radici del polinomio $f(x) = x^4 + 2x^3 - 4x^2 - 2x + 5$. Calcolare $\sum_i \alpha_i^3$.

Esercizio 51. Esprimere e_4 come polinomio a coefficienti razionali nei polinomi di Newton.

Esercizio* 52. Sia A una matrice a coefficienti razionali $n \times n$. Dimostrare che se $\mathrm{Tr}(A) = \mathrm{Tr}(A^2) = \cdots = \mathrm{Tr}(A^n) = 0$ allora $A^n = 0$. [Se non si riesce a fare questo esercizio in generale supporre che A sia diagonalizzabile]

Esercizio 53. Sia f un polinomio a coefficienti in un campo E con radici distinte $\alpha_1, \dots, \alpha_n$ in un campo F contenente E. Sia $g \in E[x_1, \dots, x_n]$ un polinomio simmetrico in $x_1, \dots, x_n$. Dimostrare che $g(\alpha_1, \dots, \alpha_n) \in E$.

Esercizio 54. Dimostrare che $\mathbb{Q}[p_1, \dots, p_n] = \mathbb{Q}[x_1, \dots, x_n]^{\mathsf{S}_n}$. È vero lo stesso enunciato se al posto di $\mathbb{Q}$ si mette $\mathbb{Z}$?

13. Risultante e discriminante

Abbiamo definito il discriminante $\Delta(f)$ di un polinomio f di grado n di radici $\alpha_1, \dots, \alpha_n$ mediante

$$\Delta(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Per quanto fatto vedere sui polinomi simmetrici sappiamo che $\Delta(f)$ si può esprimere in modo polinomiale nei coefficienti $a_1, \dots, a_n$ di f. Vogliamo fornire una ulteriore formula esplicita per queste espressioni polinomiali.

Risultante. Sia A un anello e siano $f, g \in A[t]$ due polinomi a coefficienti in A di gradi m e n strettamente positivi:

$$f = a_m t^m + \cdots + a_0;$$
$$g = b_n t^n + \cdots + b_0.$$

Definiamo il risultante $R(f, g)$ come il determinante della seguente matrice R

$$\mathsf{R} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{m-1} & a_m & & & \\ & a_0 & a_1 & \cdots & a_{m-1} & a_m & & \\ & & & & \cdots & & & \\ & & & a_0 & a_1 & \cdots & a_{m-1} & a_m \\ b_0 & b_1 & \cdots & b_{n-1} & b_n & & & \\ & b_0 & b_1 & \cdots & b_{n-1} & b_n & & \\ & & & & \cdots & & & \\ & & & b_0 & b_1 & \cdots & b_{n-1} & b_n \end{pmatrix}$$

di forma $(n+m) \times (n+m)$, dove nelle prime n righe compaiono i coefficienti di f, nelle ultime m i coefficienti di g e gli spazi bianchi sono completati aggiungendo 0.

Esercizio 55. Sia $f = x^3 + px + q$ allora $R(f, f') = 27q^2 + 4p^3 = -\Delta(f)$.

Più in generale abbiamo la seguente proposizione:

Proposizione. *Sia f monico di grado m positivo allora*

$$R(f, f') = (-1)^{\frac{m(m-1)}{2}} \Delta(f).$$

Chi vuole può dimostrare questa proposizione seguendo i seguenti esercizi:

Esercizio 56. Siano f, g due polinomi di grado positivo allora f e g hanno un divisore in comune se e solo se esistono due polinomi non nulli φ e ψ con $\mathit{grado}\,\varphi < \mathit{grado}\, f$ e $\mathit{grado}\,\psi < \mathit{grado}\, g$ tali che $f\psi = g\varphi$.

Esercizio 57. Dimostrare che l'esistenza dei polinomi φ e ψ dell'esercizio precedente è equivalente alla esistenza di soluzioni non nulle del sistema $\mathsf{R}\mathsf{v} = 0$.

Esercizio 58. Dimostrare che f e g hanno dei fattori in comune se e solo se $R(f, g) = 0$.

Esercizio 59. Sia $\mathsf{M} = (m_i j)$ una matrice $(n+m) \times (n+m)$ con $m_i j$ un elemento omogeneo e

$$\mathit{grado}\, m_{ij} = \begin{cases} m + i - j & \text{se } i \leqslant n; \\ i - j & \text{se } i > n \end{cases}$$

allora $\det \mathsf{M}$ è omogeneo di grado nm.

Sia ora

$$f = \prod_{i=1}^{m} (t - x_i).$$

e consideriamo $\Delta(f)$ e $R(f, f')$ come polinomi F e G nelle variabili $x_1, \dots, x_m$.

Esercizio 60. Dimostrare che F e G sono polinomi omogenei e simmetrici nelle variabili $x_1, \dots, x_m$ di grado $m(m-1)$.

Esercizio 61. Dimostrare che se $(x_i - x_j)$ divide G allora $(x_i - x_j)^2$ divide G sfruttando la simmetria di G.

Esercizio 62. Dimostrare che $(x_i - x_j)^2$ divide G per $i \neq j$.

Esercizio 63. Dimostrare che $G = \lambda F$ con λ una costante indipendente da f.

Esercizio 64. Calcolare la costante λ considerando un polinomio opportuno.

14. Richiami e notazioni su estensioni algebriche, estensioni finite e polinomio minimo

Richiamiamo qualche risultato che avete visto ad Algebra 2 introducendo qualche convenzione e qualche definizione.

Definizione. Siano E, F due campi. Una applicazione $\varphi : E \longrightarrow F$ che conserva la somma e il prodotto si dice un morfismo di campi, o una estensione di campi, se $\varphi(1) = 1$. L'insieme dei morfismi di campi da E a F si indica con $\mathrm{Mor}_c(E, F)$ o con $\mathrm{Mor}(E, F)$.

In particolare si osservi che ogni morfismo di campi è iniettivo e che il campo E si identifica con un sottocampo di F. Di fatto molto spesso, per evitare di appesantire la notazione, utilizzeremo la parola "estensione" come sinonimo di inclusione $E \subset F$ e enunceremo molti risultati in questa generalità.

In altre occasioni sarà invece utile distinguere tra una inclusione insiemistica e un morfismo di campi qualsiasi.

Definizione (Gruppo di Galois)**.** Siano $E \subset F$ e $E \subset K$ due estensioni di campi. Un morfismo da F a K su E è un morfismo di campi $\varphi : F \longrightarrow K$ tale che $\varphi\big|_E = \mathrm{id}$. L'insieme dei morfismi da F a K si indica con $\mathrm{Mor}_E(F, K)$.

La composizione di due morfismi su E è ancora un morfismo su E e se φ è un morfismo di campi su E bigettivo la sua inversa è ancora un morfismo di campi su E.

Possiamo quindi definire il gruppo di Galois di F su E come l'insieme

$$\mathrm{Gal}(F : E) = \{\varphi \in \mathrm{Mor}_E(F, F) \,:\, \varphi \text{ bigettiva}\}$$

con l'operazione di gruppo data dalla composizione.

Osservazione. Più in generale se $\alpha : E \longrightarrow F$ e $\beta : E \longrightarrow K$ sono due estensioni di campi avremmo potuto definire un morfismo di campi da F a K su E (o forse sarebbe meglio dire su α, β) come un morfismo di campi $\varphi : F \longrightarrow K$ tale che $\varphi \circ \alpha = \beta$. E analogamente per il gruppo di Galois.

Esercizio 65. Calcolare $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}\,], \mathbb{Q})$.

Le definizioni di elemento algebrico, elemento trascendente, estensione algebrica di campi, estensione finita sono quelle date ad Algebra 2. In particolare, se $E \subset F$ è una estensione di campi, il grado dell'estensione, che si indica con $[F : E]$, è la dimensione di F come E spazio vettoriale ovvero la cardinalità di una base dell'E spazio vettoriale F. Se $E \subset F \subset K$ ricordo che abbiamo

$$[K : E] = [K : F][F : E].$$

Se $E \subset F$ è una estensione di campi e se $E \subset F_i \subset K$ sono dei sottocampi di K la loro intersezione $\bigcap F_i$ è un campo contenente E. Analogamente se $A \subset C$ è una estensione di anelli e se $A \subset B_i \subset C$ sono dei sottoanelli di C la loro intersezione $\bigcap B_i$ è un anello. Ha quindi senso dare le seguenti definizioni.

Definizione. Sia $A \subset C$ una estensione di anelli e S un sottoinsieme di C (o per abuso di notazione anche un elemento di C o una lista di elementi di C), allora $A[S]$ è il minimo anello contente A e S.

Sia $E \subset K$ una estensione di anelli e S un sottoinsieme di K (o per abuso di notazione anche un elemento di K o una lista di elementi di K), allora $E(S)$ è il minimo campo contente E e S. In particolare se $S = F$ è un sottocampo di C il campo prodotto EF di E e F è il campo $E(F) = F(E)$.

Esercizio 66. Siano A, B due sottoanelli di C allora

$$A[B] = B[A] = \left\{ \sum_i a_i\, b_i \,:\, a_i \in A, b_i \in B \right\}$$

Esercizio 67. Siano E, F due sottocampi di K allora

$$EF = \left\{ \frac{\sum_i a_i\, b_i}{\sum_i a'_i\, b'_i} \,:\, a_i, a'_i \in E, b_i, b'_i \in F \text{ e } \sum_i a'_i\, b'_i \neq 0 \right\}$$

Ricordiamo che se $E \subset F$ è una estensione di campi e $\alpha \in F$ allora α è algebrico su E se e solo se $E[\alpha] = E(\alpha)$ e che il grado dell'estensione $E \subset E[\alpha]$ è pari al grado del polinomio minimo di α su E. Più precisamente se $f \in E[t]$ è il polinomio minimo e d è il suo grado abbiamo che $E[\alpha] \simeq E[t]/(f)$ e che $1, \alpha, \ldots, \alpha^{d-1}$ è una base di F su E.

Ricordiamo inoltre che se $f \in E[t]$ e $E \subset F$ è una estensione di campi allora F si dice un campo di spezzamento per f su E se f si scrive come prodotto di fattori lineari su E e che se $\alpha_1, \ldots, \alpha_d \in F$ sono le radici di f, F è generato da queste radici come estensione di E ovvero $F = E[\alpha_1, \ldots, \alpha_d]$ o equivalentemente, essendo estensioni finite, $F = E(\alpha_1, \ldots, \alpha_d)$. Più in generale se $\mathcal{F}$ è un insieme di polinomi di $E[t]$ di grado maggiore o uguala a 1 un campo F si dice un campo di spezzamento per $\mathcal{F}$ se ogni poinomio di $\mathcal{F}$ si scrive come prodotto di fattori lineari in $F[t]$ e se F è generato da E e dalle radici dei polinomi in $\mathcal{F}$.

Infine riassumiamo alcune proprietà che avete visto ad Algebra 2 delle estensioni algebriche e finite introducendo la seguente definizione.

Definizione. Sia $\mathcal{C}$ una classe di estensioni di campi [1]. Diciamo che $\mathcal{C}$ è una classe distinta se ha le seguenti proprietà ($E \subset F$, $F \subset K$, etc. sono tutte estensioni di campi):

1) $E \subset F$ e $F \subset K$ appartengono a $\mathcal{C}$ se e solo se $E \subset K$ appartiene a $\mathcal{C}$;
2) Se $E \subset F$ appartiene a $\mathcal{C}$ e $E \subset K$ qualsiasi e $F, K \subset L$ allora $K \subset FK$ appartiene a $\mathcal{C}$.

Esercizio 68. Se $\mathcal{C}$ è una classe distinta e se $E \subset F$ e $E \subset K$ sono elementi di $\mathcal{C}$ e $F, K \subset L$ allora $E \subset FK$ appartiene a $\mathcal{C}$.

Esercizio 69. Dimostrare che la classe delle estensioni finite sono una classe distinta.

Esercizio 70. Dimostrare che la classe delle estensioni algebriche sono una classe distinta.

15. Esercizi su estensioni e polinomio minimo

Esercizio 71. Calcolare il polinomio minimo di $1 + \sqrt{2}$ su $\mathbb{Q}$.
Calcolare il polinomio minimo di $1 + \sqrt{2}$ su $\mathbb{Q}[\sqrt{2}]$.

Esercizio 72. Siano $f = x^3 + x^2 + 1$ e $g = x^3 + x + 1$ in $\mathbb{F}_2[x]$. Verificare che sono due polinomi irriducibili e descrivere un isomorfismo esplicito tra $\mathbb{F}_2[x]/(f)$ e $\mathbb{F}_2[x]/(g)$. [osservare che questo quoziente è il campo $\mathbb{F}_8$, esprimere quindi una radice di g in funzione di una radice di f, o viceversa]

Esercizio 73. Siano $\alpha, \beta, \gamma \in \mathbb{C}$. Siano $a = \alpha + \beta + \gamma$, $b = \alpha\beta + \alpha\gamma + \beta\gamma$ e $c = \alpha\beta\gamma$ algebrici su $\mathbb{Q}$. Dimostrare che α, β, γ sono algebrici su $\mathbb{Q}(a, b, c)$. È sempre vero che α, β, γ sono algebrici su $\mathbb{Q}$?

Esercizio 74. Sia α una radice del polinomio $f(x) = x^4 + 3x + 3$ e sia $\beta = \alpha^2$.

(1) Dimostrare che $\mathbb{Q}[\beta] = \mathbb{Q}[\alpha]$;
(2) Calcolare il polinomio minimo di β su $\mathbb{Q}$.

Esercizio 75. Sia F il campo di spezzamento del polinomio $x^3 - 2$ su $\mathbb{Q}$. Calcolare $[F : \mathbb{Q}]$.

Esercizio 76. Calcolare $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}\,] : \mathbb{Q})$.

Esercizio* 77. Sia $\alpha = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$. Dimostrare che α non è algebrico su $\mathbb{Q}$.

16. Assioma della scelta e lemma di Zorn

L'assioma della scelta dice che se uno ha una famiglia di insiemi non vuoti allora può scegliere un elemento da ogni insieme. Se X è un insieme ricordiamo che l'insieme delle parti di X, che indichiamo con $\mathcal{P}(X)$, è l'insieme i cui elementi sono tutti i sottoinsiemi di X.

Assioma della scelta: Se X è un insieme non vuoto allora esiste una funzione $f : \mathcal{P}(X) \longrightarrow X$ tale che $f(Y) \in Y$ per ogni $Y \subset X$ e $Y \neq \varnothing$. (una f con queste proprietà si dice una funzione di scelta).

Enunciamo ora il Lemma di Zorn che malgrado sia equivalente all'assioma della scelta è molto meno intuitivo. In compenso la formulazione del lemma di Zorn è molto astuta ed in molte situazioni si presta ad essere applicata in modo semplice. Se $(X, \leqslant)$ è un insieme con una relazione d'ordine (per noi una relazione d'ordine senza ulteriori specificazioni sarà sempre una relazione d'ordine parziale) ricordiamo che una *catena* di X è un sottoinsieme C di X tale che l'ordine di X induca un ordine totale su C, ovvero: per ogni $x, y \in C$ si ha $x \leqslant y$ o $y \leqslant x$.

Lemma di Zorn: Sia X un insieme non vuoto con una relazione d'ordine $\leqslant$. Supponiamo che per ogni catena C di X esista $x \in X$ tale che $c \leqslant x$ per ogni $c \in C$. Allora in X esiste un elemento massimale ovvero un elemento $m \in X$ tale che per ogni $y \in X$ $m \leqslant y$ implica $m = y$.

Esercizio 78. Usando il lemma di Zorn dimostrare che ogni anello ha un ideale massimale.

Esercizio 79. Usando il lemma di Zorn dimostrare che ogni spazio vettoriale ha una base.

Per dimostrare che l'assioma della scelta implica il lemma di Zorn è utile introdurre una forma debole del Lemma di Zorn nel quale la relazione d'ordine dell'enunciato precedente è sostituita con l'inclusione tra insiemi e in cui l'esistenza di un generico maggiorante è sostituita con l'unione di tutti gli elementi della catena.

[1] Se la parola classe non vi è chiara pensate ad insieme, in realtà la distinzione tra classe ed insieme è un modo per evitare paradossi tipo quello di Russell

Forma debole del lemma di Zorn. Sia X un insieme e sia $\mathcal{F}$ una famiglia non vuota di sottoinsiemi di X che consideriamo ordinata con la relazione d'ordine data dall'inclusione insiemistica: se $Y, Z \in \mathcal{F}$ diciamo che $Y \leqslant Z$ se e solo se $Y \subset Z$. Supponiamo inoltre che $\mathcal{F}$ abbia le seguenti due proprietà:

i) Se $Y \in \mathcal{F}$ e $Z \subset Y$ allora $Z \in \mathcal{F}$;
ii) Se $\mathcal{C} \subset \mathcal{F}$ è una catena in $\mathcal{F}$ allora $\bigcup \mathcal{C} := \bigcup_{Y \in \mathcal{C}} Y$ è un elemento di $\mathcal{F}$.

Allora esiste un elemento di $\mathcal{F}$ massimale.

Esercizio 80. Dimostrare che il lemma di Zorn implica l'assioma della scelta.

Esercizio 81. Dimostrare che la forma debole del lemma di Zorn implica il lemma di Zorn.

La dimostrazione che l'assioma della scelta implica la forma debole del lemma di Zorn è più complicata (questa sotto ne è una traccia):
Primo Si consideri una funzione di scelta $f : \mathcal{P}(X) \longrightarrow X$;
Secondo Per ogni $Y \in \mathcal{F}$ sia $Y' = \{x \in X \,:\, Y \cup \{x\} \in \mathcal{F}\}$ e si definisca $g : \mathcal{F} \longrightarrow \mathcal{F}$ mediante $g(Y) = Y$ se $Y' = Y$ e $g(Y) = Y \cup g(Y' \smallsetminus Y)$ se $Y' \neq Y$. Si osservi che Y è massimale se e solo se $g(Y) = Y$.
Terzo Un sottoinsieme $\mathcal{T}$ di $\mathcal{F}$ si dice una torre se

i) $\varnothing \in \mathcal{T}$;
ii) se $Y \in \mathcal{T}$ allora $g(Y) \in \mathcal{T}$;
iii) se $\mathcal{C} \subset \mathcal{T}$ è una catena in $\mathcal{T}$ allora $\bigcup \mathcal{C} \in \mathcal{T}$.

dimostrare che l'intersezione di torri è una torre. Quindi esiste una torre minima $\mathcal{T}_0$.
Quarto Dimostrare che $\mathcal{T}_0$ è una catena.
Quinto Dimostrare l'esistenza di un elemento massimale.

17. La chiusura algebrica di un campo

Un campo E si dice algebricamente chiuso se ogni polinomio in $E[t]$ non costante ha una radice in E.

Esercizio 82. Sia E un campo. Le seguenti affermazioni sono equivalenti:

a) E è algebricamente chiuso;
b) se $f \in E[t]$ è un polinomio non costante allora f si scrive come prodotto di fattori lineari in $E[t]$;
c) se $E \subset F$ è una estensione algebrica di E allora $E = F$;
d) se $E \subset F$ è una estensione finita di E allora $E = F$.

Ad Algebra 2 avete visto che dato un campo E ed un polinomio f non costante esiste sempre una estensione F di E che contiene una radice di f. La chiusura algebrica di un campo è un campo che contiene tutte le radici di tutti polinomi non costanti a coefficenti in E.

Definizione. Sia $E \subset F$ una estensione di campi, allora F si dice una chiusura algebrica di E se F è algebricamente chiuso e se F è una estensione algebrica di E.

Il campo dei numeri complessi $\mathbb{C}$ è algebricamente chiuso. La dimostrazione di questo fatto che si chiama "Teorema fondamentale dell'algebra" risiede (sempre) nelle proprietà di completezza dei numeri reali. Nel prossimo esercizio trovate dei suggerimenti per una dimostrazione che si basa sul Teorema di Weierstrasse sull'esistenza di minimi per funzioni reali continue definite su insiemi compatti (più avanti vedremo una dimostrazione che invece utilizza il teorema di Bolzano-Weierstrasse e un po' di teoria di Galois).

Esercizio* 83 (Teorema fondamentale dell'algebra)**.** Sia f un polinomio a coefficienti complessi non costante. Dimostrare che f ha una radice complessa seguendo queste indicazioni:

i) Dimostrare che il modulo di f è una funzione da $\mathbb{C}$ in $\mathbb{R}$ che ammette minimo;
ii) Osservare che il minimo del modulo di f è zero se e solo se f ha una radice complessa;
iii) Se α è un punto in cui il modulo di f assume il valore minimo dimostrare che tale valore è zero considerando l'andamento di f in un intorno di α [può aiutare la comprensione studiare prima il caso in cui α sia uguale a 0].

Abbiamo già visto che $\mathbb{C}$ non è algebrico su $\mathbb{Q}$ ma l'esercizio 84 ci assicura che $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \,:\, \alpha \text{ è algebrico su } \mathbb{Q}\}$ è una chiusura algebrica di $\mathbb{Q}$.

Esercizio 84. Sia $E \subset K$ una estensione di campi e sia K algebricamente chiuso. Consideriamo $F = \{\alpha \in K \,:\, \alpha \text{ è algebrico su } E\}$. Allora F è un campo ed è una chiusura algebrica di E.

In particolare abbiamo così dimostrato l'esistenza di una chiusura algebrica di $\mathbb{Q}$. Per un campo generale per dimostrare l'esistenza della chiusura algebrica è invece necessario l'assioma della scelta.

Teorema. *Ogni campo ha una chiusura algebrica. Inoltre se $E \subset F$ è una estensione algebrica e se $E \subset \Bbbk$ è una estensione di campi con $\Bbbk$ algebricamente chiuso allora esiste $\varphi : F \longrightarrow \overline{\Bbbk}$ tale che $\varphi\big|_E = \mathrm{id}_E$.*

18. Altri esercizi sui campi algebricamente chiusi e sulla chiusura algebrica

Esercizio 85. Sia $E \subset F$ una estensione algebrica di campi e sia $\mathcal{P}$ l'insieme di tutti i polinomi a coefficienti in E. Dimostrare che $card\, F \leqslant card(\mathcal{P} \times \mathbb{N})$.

Esercizio 86. Sia $E \subset F$ una estensione algebrica di campi. Dimostrare che $card\, F \leqslant \max(card(E), card(\mathbb{N}))$.

Esercizio* 87. Sia $\mathbb{C} \subset K$ una estensione di $\mathbb{C}$ tale che $[K : \mathbb{C}] \leqslant card(\mathbb{N})$. Dimostrare che $K = \mathbb{C}$.

Esercizio* 88. Sia E un campo algebricamente chiuso e sia $E \subset D$ un corpo su E, ovvero sia D un corpo e $E \subset Z(D)$. Dimostrare che se se la dimensione di D come E spazio vettoriale è finita allora $D = E$.

Esercizio 89. Sia $\mathcal{F} \subset E[t]$ un insieme di polinomi non costanti. Dimostrare che esiste un campo di spezzamento per $\mathcal{F}$ su E.

Esercizio 90. Sia $\mathcal{F} \subset E[t]$ un insieme di polinomi non costanti. Siano $E \subset F$ e $E \subset K$ due campi di spezzamento su E. Dimostrare che esiste un isomorfismo di campi su E da F a K.

19. Esercizi sui morfismi di campi (II-III settimana)

Esercizio 91. Sia $A \subset B$ una estensione di anelli e sia $b \in B$, allora $A[b] = \{f(b) \,:\, f \in A[t]\}$.

Esercizio 92. Sia $E \subset F$ una estensione di campi e sia $\alpha \in F$, allora $E(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \,:\, f, g \in E[t] \text{ e } g(\alpha) \neq 0\}$.

Esercizio 93. Sia $E \subset F$ una estensione di campi e sia $\alpha \in F$, allora i seguenti fatti sono equivalenti

i) α è algebrico su E;
ii) $E(\alpha) = E[\alpha]$;
iii) $E(\alpha) \supset E$ è una estensione finita.

Esercizio 94. Determinare il gruppo degli automorfismi di $\mathbb{Q}$ e di $\mathbb{F}_p$.

Esercizio 95. Determinare $\mathrm{Gal}(\mathbb{C}, \mathbb{R})$.

Esercizio* 96. Determinare il gruppo degli automorfismi di $\mathbb{R}$.

Esercizio 97. Determinare $\mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)$.

Esercizio* 98. Sia $E \subset F$ una estensione algebrica e sia $\varphi : F \longrightarrow F$ un morfismo di campi su E. Dimostrare che φ è bigettiva.

Esercizio 99. Far vedere con un esempio che l'ipotesi che l'estensione sia algebrica nell'esercizio precedente non non si può eliminare.

Esercizio 100. Sia F il campo di spezzamento del polinomio $x^3 - 2$ su $\mathbb{Q}$. Calcolare $\mathrm{Gal}(F, \mathbb{Q})$.

20. Esercizi sulle estensioni separabili (III settimana)

Esercizio 101. Sia $f \in E[t]$

i) se f non è separabile allora $\mathrm{MCD}(f, f') \neq 1$;
ii) se f è irriducibile e non è separabile allora $f' = 0$.

Esercizio 102. Siano $E \subset F \subset K$ estensioni di campi e sia $\alpha \in K$. Se α è separabile su E allora α è separabile su F.

Esercizio 103. Sia $E \subset F \subset K$ allora $E \subset K$ è una estensione separabile se e solo se $E \subset F$ e $F \subset K$ sono estensioni separabili.

Esercizio 104. Siano $E \subset F \subset L$ e $E \subset K \subset L$ estensioni di campi. Se $E \subset F$ è separabile allora $K \subset KF$ è separabile.

Esercizio 105. Sia $E \subset F$ una estensione si campi. Allora $\{\alpha \in F \,:\, \alpha \text{ è separabile su } E\}$ è un sottocampo di F.

Un campo si dice *perfetto* se ogni sua estensione algebrica è separabile.

Esercizio 106. Dimostrare che ogni campo di caratteristica 0 è perfetto.

Esercizio 107. Sia E un campo di caratteristica p e sia $\varphi : E \longrightarrow E$ il morfismo di Frobenius definito da $\varphi(x) = x^p$ per ogni $x \in E$. Dimostrare che E è perfetto se e solo se φ è surgettiva. In particolare dimostrare che ogni campo finito è perfetto.

Esercizio* 108. Sia $E \subset F$ una estensione finita di campi di *car* $p > 0$. Sia $K = \{\alpha \in F \,:\, \alpha \text{ è separabile su } E\}$. Dimostrare che per ogni $\beta \in F$ esiste n tale che $\beta^{p^n} \in K$.

21. Esercizi lunedì 24 ottobre

Esercizio 109. Sia $E \subset F$ una estensione normale e sia $f \in E[t]$ un polinomio irriducibile non nullo. Dimostrare che se f ha una radice in F allora si scrive come prodotto di fattori lineari in $F[t]$.

Esercizio 110. Siano $E \subset F \subset K$ estensioni algebriche di campi.

1) $E \subset K$ è una estensione normale, implica che $F \subset K$ è una estensione normale;
2) In generale non è vero che $E \subset K$ estensione normale implica $E \subset F$ normale, fornire un esempio;
3) In generale non è vero che se $E \subset F$ e $F \subset K$ normali allora $E \subset K$ è normale, fornire un esempio.

Esercizio 111. Siano $E \subset F \subset L$ e $E \subset K \subset L$ estensioni di campi. Dimostrare che se $E \subset F$ è normale allora $K \subset KF$ è normale.

Esercizio 112. Dimostrare che l'intersezione di estensioni normali è una estensione normale.

In particolare data una estensione algebrica di campi $E \subset F \subset \overline{E}$ con allora esiste una minima estensione normale $E \subset L$ con $F \subset L$. L viene chiamata a volte la *chiusura normale* di F.

Esercizio 113. Sia $E \subset F \subset \overline{E}$ e sia L la chiusura normale di F Dimostrare che L è generata dalle estensioni $E \subset \varphi(F)$ con $\varphi : F \longrightarrow \overline{E}$ morfismo su E.

Esercizio 114. Sia L una estensione di Galois di $\mathbb{Q}$ della forma $\mathbb{Q}[\sqrt[3]{d}]$ con $d \in \mathbb{Z}$. Dimostrare che d è un cubo perfetto.

[se $x \in \mathbb{R}$ con $\sqrt[3]{x}$ indico la radice cubica reale di x]

Esercizio 115. Sia $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Calcolare il polinomio minimo di $\sqrt{2} + \sqrt{3}$ e dimostrare che $E = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

Esercizio* 116. Siano $p_1, \ldots, p_n$ numeri primi distinti e sia $E = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$. Calcolare $[E : \mathbb{Q}]$ e $\mathrm{Gal}(E : \mathbb{Q})$. Dimostrare che $E = \mathbb{Q}[\sqrt{p_1} + \cdots + \sqrt{p_n}]$

22. Esercizi giovedì 27 ottobre

Esercizio 117. Sia F un campo. È possibile trovare un sottogruppo finito di $\mathrm{Aut}(F)$ tale che $\mathrm{Gal}(F : F^G) \neq G$?

Esercizio 118. Sia $E \subset F$ una estensione di Galois. Sia $\mathrm{Gal}(F : E) = \mathbb{Z}/15$. Quanti sono i sottocampi di F contenenti E?

Esercizio 119. Descrivere il gruppo di Galois e le estensioni intermedie del campo di spezzamento su $\mathbb{Q}$ del polinomio $x^4 - 2$.

Esercizio 120. Descrivere il gruppo di Galois del campo di spezzamento su $\mathbb{Q}$ del polinomio $x^3 - 3x - 6$.

Esercizio 121. Sia $E = \mathbb{C}((t))$ e sia $f(x) = x^n - t$. Descrivere il campo di spezzamento di f su E e il suo gruppo di Galois. Quanti soo i suoi sottocampi intermedi e quanti i suoi sottocampi intermedi che sono estensioni normali di E.

Esercizio 122. Sia E un campo di caratteristica diversa da 2, f un polinomio irriducibile e separabile di grado 3 a coefficienti in E e sia G il gruppo di Galois di f (ovvero il gruppo di Galois del campo di spezzamento del polinomio f sul campo E). Dimostrare che

a) $\Delta(f)$ è un quadrato in E implica $G \simeq \mathbb{Z}/3$;
b) $\Delta(f)$ non è un quadrato in E implica $G \simeq \mathsf{S}_3$.

23. Estensioni primitive (27 ottobre)

Esercizio* 123. Sia $E \subset F$ una estensione finita di campi. Dimostrare che se esiste solo un numero finito di campi compresi tra E e F allora esiste $\alpha \in F$ tale che $F = E[\alpha]$. [potrebbe essere utile separare il caso in cui i campi sono infiniti da quello in cui sono finiti e per i quali potete prendere il risultato per buono].

Le estensioni algebriche della forma $E[\alpha]$ si chiamano *estensioni primitive o semplici* e α si chiama elemento primitivo. Ovviamente ogni estensione di questo tipo è finita. Per le estensioni separabili è vero anche il viceversa ma in generale è falso.

Esercizio 124. Sia $E \subset F$ una estensione separabile finita. Dimostrare che esiste α tale che $F = E[\alpha]$. [utilizzare il risultato dell'esercizio precedente, se si trovasse qualche difficoltà a fare questo esercizio fare il caso in cui l'estensione sia di Galois].

Esercizio 125 (Lang)**.** Sia $F = \mathbb{F}_p(s, t)$ ovvero il campo dei quozienti dell'anello dei polinomi in due variabili s, t a coefficienti in $\mathbb{F}_p$. Sia $E = \mathbb{F}_p(s^p, t^p)$ il sottocampo generato da s^p e t^p. Dimostrare che $[F : E] = p^2$ e che F non è una estensione primitiva di E.

24. Esercizi lunedì 31 ottobre

Esercizio 126. Sia $E = \mathbb{Q}[\zeta]$ con $\zeta = e^{\frac{2\pi i}{n}}$. Siano $a, b \in E$ e sia F il campo di spezzamento su E di $(x^n - a)(x^n - b)$. Dimostrare che $\mathrm{Gal}(F : E)$ è abeliano e che $\sigma^n = \mathrm{id}$ per ogni $\sigma \in \mathrm{Gal}(F : E)$.

Esercizio 127. Sia K un campo e Γ un sottogruppo finito di $\mathbb{K}^*$. Dimostrare che Γ è ciclico.

Esercizio 128. Sia p un numero primo, f il polinomio $x^{p-1} + x^{p-2} + \cdots + 1$ e $\zeta = e^{\frac{2\pi i}{p}}$.

a) descrivere le radici di f;
b) dimostrare che f è irriducibile [Sugg. provare ad utilizzare il cambiamento di variabile $x = y + 1$];
c) calcolare $[\mathbb{Q}(\zeta) : \mathbb{Q}]$;
d) descrivere il gruppo di Galois $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$.

Esercizio 129. Sia F il campo di spezzamento di $x^3 - 15$ su $\mathbb{Q}$:

a) Calcolare il gruppo di Galois di F su $\mathbb{Q}$;
b) Descrivere tutti i sottocampi di F che sono estensioni di grado 2 di $\mathbb{Q}$;
c) Calcolare $F \cap \mathbb{Q}(\sqrt{-p})$ al variare del primo p.

Esercizio 130 (Milne esr. 15)**.** Sia $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ e $F = \mathbb{Q}[\alpha]$. Dimostrare che $F \supset \mathbb{Q}$ è di Galois e che $\mathrm{Gal}(F : \mathbb{Q})$ è isomorfo al gruppo delle unità dei quaternioni $\{\pm 1, \pm i, \pm j, \pm k\}$.

25. Esercizi lunedì 7 novembre

Esercizio 131. Sia E il campo di spezzamento di $(x^3 - 2)(x^3 - 5x + 1)$ su $\mathbb{Q}$. Calcolare il gruppo di Galois di E su $\mathbb{Q}$.

Esercizio 132. Sia G un gruppo finito. Dimostrare che esistono due estensioni algebriche E ed F di $\mathbb{Q}$ con $E \subset F$ estensione di Galois e $\mathrm{Gal}(F : E)$ isomorfo a G.

Esercizio 133 (Teorema di Lagrange)**.** Su $F = \Bbbk(x_1, \ldots, x_n)$ si consideri l'usuale azione di S_n e sia $E = F^{\mathsf{S}_n}$ il campo delle funzioni razionali simmetriche.

Siano $\varphi, \psi \in F$. Dimostrare che $\varphi \in E[\psi]$ se e solo se per ogni $\sigma \in \mathsf{S}_n$ $\sigma\psi = \psi$ implica $\sigma\varphi = \varphi$.

Esercizio 134. Si calcoli il discriminante del polinomio $x^n + ax + b$.

26. Esercizi giovedì 10 novembre (esercizi per casa da consegnare entro mercoledì 23 novembre)

Esercizio 135. Sia f un polinomio irriducibile di grado n su un campo E di car. 0 e sia F il suo campo di spezzamento. Dimostrare che se $[F : E] > n$ il gruppo di Galois non è abeliano.

Esercizio 136. Sia f un polinomio irriducibile di quarto grado, G il suo gruppo di Galois, Δ il suo discriminante e $R = R(x_1 + x_2, f)$. Supponiamo che R abbia tutte le radici distinte, allora

1) se Δ non è un quadrato e R è irriducibile $G \simeq \mathsf{S}_4$;
2) se Δ non è un quadrato e R è riducibile $G \simeq \mathsf{D}_4$;
3) se Δ è un quadrato e R è irriducibile $G \simeq \mathsf{A}_4$;
4) se Δ è un quadrato e R è il prodotto di tre polinomi irriducibili di grado 2 $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$;
5) Se Δ è un quadrato e R è il prodotto di due polinomi irriducibili $G \simeq \mathbb{Z}/4$.

[Questo esercizio è sbagliato 2 e 5 vanno sostituiti con se Δ non è un quadrato e R è riducibile allora $G \simeq \mathsf{D}_4$ o $G \simeq \mathbb{Z}/4$]

Esercizio 137. Si considerino i polinomi $e = x^4 - 3$, $f = x^3 - 2$ e $\ell = ef$. Siano F e L i campi di spezzamento di f e ℓ su $\mathbb{Q}$.

1) Descrivere il gruppo di Galois $\mathrm{Gal}(F, \mathbb{Q})$;
2) Calcolare $[L : \mathbb{Q}]$.

Esercizio 138. Sia $\alpha \in \overline{\mathbb{Q}}$ e sia E un campo massimale tra i campi contenuti in $\overline{\mathbb{Q}}$ e non contenenti α. Dimostrare che ogni estensione finita di E è ciclica.

27. Esercizi giovedì 24 novembre

Esercizio 139. Sia f un polinomio separabile un campo E e sia F un suo campo di spezzamento. Dimostrare che f è irriducibile se e solo se $\mathrm{Gal}(F, E)$ agisce transitivamente sulle radici di f.

Esercizio 140. Dimostrare che esistono infiniti numeri primi congrui a -1 modulo 6.

Esercizio 141. Sia $P = x_1 - x_2$ e sia f un polinomio di quarto grado separabile e irriducibile. Sia $R = R(P, f)$ e supponiamo che abbia le radici distinte. Cosa si può dedurre sulla fattorizzazione di R se $\mathrm{Gal}(f) = \mathsf{D}_4$? e se $\mathrm{Gal}(f) = \mathbb{Z}/4$?

Esercizio 142. Costruire una estensione di Galois di $\mathbb{Q}$ con gruppo di Galois $\mathbb{Z}/5$.

Esercizio 143. Dimostrare che se p è un numero primo dispari allora $(\mathbb{Z}/p^n)^*$ è ciclico.

28. Traccia, norma e polinomio caratteristico

Sia $E \subset F$ una estensione finita di campi separabile. Scegliamo una chiusura algebrica di F e quindi di E e indichiamola con $\overline{E}$: abbiamo $E \subset F \subset \overline{E}$. Sia $\Phi(F,E) = \{\varphi : F \longrightarrow \overline{E} \,:\, \varphi|_E = \mathrm{id}_E\}$. Ricordiamo che questo insieme ha $[F:E]$ elementi. Per $x \in F$ definiamo:

$$Traccia_E^F(x) = \mathrm{Tr}_E^F(x) = \sum_{\varphi \in \Phi(F,E)} \varphi(x) \in E$$

$$Norma_E^F(x) = \mathrm{N}_E^F(x) = \prod_{\varphi \in \Phi(F,E)} \varphi(x) \in E$$

$$polinomio\ caratteristico_{E,x}^F(t) = c_{E,x}^F(t) = \prod_{\varphi \in \Phi(F,E)} (t - \varphi(x)) \in E[t]$$

I risultati degli esercizi seguenti valgono per una estensione $F \supset E$ finita separabile qualsiasi. Chi vuole però può assumere quando gli torna comodo che si tratti di estensioni di Galois (il che non cambia la sostanza ma alleggerisce qualche argomento). Osserviamo che nel caso in cui $F \supset E$ sia di Galois $\Phi(F,E) = \mathrm{Gal}(F:E)$.

Esempio. Sia $E = \mathbb{Q}$ e $F = \mathbb{Q}(\sqrt{d})$ con d diverso da 1 e libero da quadrati. Sia $\alpha = a + b\sqrt{d}$ con $a, b \in \mathbb{Q}$. Allora $\mathrm{Tr}(\alpha) = 2a$, $\mathrm{N}(\alpha) = a^2 - db^2$ e che $c_\alpha = t^2 - 2at + a^2 - db^2$.

Esempio. Sia p primo e sia $F = \mathbb{Q}[\zeta_p]$. Allora $\mathrm{Tr}(\zeta_p) = 0$.

Esempio. La funzione traccia $\mathrm{Tr} : F \longrightarrow E$ è surgettiva.

Lemma. $\mathrm{Tr}_E^F(x), \mathrm{N}_E^F(x) \in E$ *e* $c_{E,x}^F(t) \in F[t]$.

Lemma. *Sia* $F = E[\alpha]$ *e sia* $f = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$ *il polinomio minimo di* α. *Dimostrare che* $\mathrm{Tr}(\alpha) = a_1$, $\mathrm{N}(\alpha) = a_n$ *e che* $f = c_\alpha$.

Proposizione. *Siano* $E \subset F \subset L$ *estensioni separabili finite e sia* $n = [L:F]$. *Allora*

$$\mathrm{Tr}_E^L = \mathrm{Tr}_E^F \circ \mathrm{Tr}_F^L \qquad e \qquad \mathrm{N}_E^L = \mathrm{N}_E^F \circ \mathrm{N}_F^L.$$

Inoltre se $\alpha \in F$ *allora* $c_{E,\alpha}^L(t) = (c_{E,\alpha}^F(t))^n$.

Proposizione. *Sia* $\alpha \in F$ *e sia* $\phi : F \longrightarrow F$ *la funzione E-lineare (è anche F lineare ma a noi interessa come applicazione E-lineare) definita da* $\phi(x) = \alpha x$. *Allora* $\mathrm{Tr}(\phi) = \mathrm{Tr}_E^F(\alpha)$, $\det(\phi) = \mathrm{N}_E^F(\alpha)$ *e il polinomio caratteristico di* ϕ *è uguale a* $(c_{E,\alpha}^F)^n$.

29. Esercizi giovedì 1 dicembre

Esercizio 144. Sia $\zeta_8 = e^{\frac{2\pi \mathrm{i}}{8}}$.

1) calcolare il polinomio minimo di ζ_8 su $\mathbb{Q}$.
2) quanti sono i sottocampi di $\mathbb{Q}[\zeta_8]$?
3) quali sono?

Esercizio 145. Calcolare $\left(\frac{719}{2351}\right)$.

Esercizio 146. Per quali primi p l'equazione $x^2 - 3\,x + 1 = 0$ ha soluzione in $\mathbb{F}_p$?

Esercizio 147. Sia $A = \mathbb{Z}/m$ un gruppo ciclico. Dimostrare che esiste una estensione E di Galois di $\mathbb{Q}$ con gruppo di Galois uguale ad A.

Sia $A = \mathbb{Z}_{/m_1} \times \cdots \times \mathbb{Z}_{/m_r}$. Dimostrare che esiste una estensione E di Galois di $\mathbb{Q}$ con gruppo di Galois uguale ad A.

Esercizio 148. Descrivere tutte le soluzioni di $a^2 - 2\,b^2 = 1$ con a, b numeri razionali.

30. Esercizi mercoledì 7 dicembre

Esercizio 149. Sia $\mathbb{F}$ un campo finito di car. p dispari e f un polinomio irriducibile di grado n. Dimostrare che $\Delta(f)$ (il discriminante di f) è un quadrato in $\mathbb{F}$ se e solo se n è dispari.

Esercizio 150. Sia $\mathbb{F}$ un campo finito. Dimostrare che ogni elemento di $\mathbb{F}$ si può scrivere come somma di due quadrati.

Esercizio 151. Sia $f = x^5 - 2$, $g = x^2 + x - 1$ e $h = fg$. Siano L, M e N i campi di spezzamento su $\mathbb{Q}$ rispettivamente di f, g e h. Si calcoli:

i) il grado di L su $\mathbb{Q}$;
ii) il grado di N su $\mathbb{Q}$;
iii) il gruppo di Galois di N su M;
iv) quanti e quali sono i sottocampi di L che sono estensioni di grado 2 o 4 di $\mathbb{Q}$;
v) quanti e quali sono i sottocampi di L.

Esercizio 152. Quanti sono i gruppi abeliani di ordine 36 a meno di isomorfismo?

Esercizio 153. Sia A un anello ad ideali principali. Se M un A modulo e $a \in A$ l'a-torsione di M è il sottomodulo

$$M[a] := \{m \in M \,:\, \exists\, n > 0 \text{ tale che } a^n\, m = 0\}.$$

Dimostrare che $M[a]$ è un sottomodulo di M e che se a e b sono primi tra loro allora $M[ab] = M[a] \oplus M[b]$.

31. Esercizi mercoledì 21 dicembre

Esercizio 154. Dire quante radici hanno i seguenti polinomi in $\mathbb{Z}/16$, $x^3 - 1$, $x^4 - 13$, $x^{15} - 1$, $x^{17} - 7$ e $x^7 - 8$.

Esercizio 155. Per quali primi p il polinomio $x^3 + 1$ si spezza in fattori lineari su $\mathbb{F}_p$?

Esercizio 156. Sia $\mathbb{F}$ un campo finito e $f \in \mathbb{F}[t]$. Sia g il prodotto di tutti i polinomi non nulli di grado minore del grado di f. Allora f è irriducibile se e solo se esiste $q \in \mathbb{F}[t]$ tale che $g = fq - 1$.

Esercizio 157. Sia $f(x) = x^6 - 2$, $g_p(x) = x^2 + p$, e $h_p(x) = f(x)\, g_p(x)$. Siano K e L_p i campi di spezzamento su $\mathbb{Q}$ rispettivamente di f e h_p.

1) Calcolare $[K : \mathbb{Q}]$;
2) Calcolare il gruppo di Galois dell'estensione $K \supset \mathbb{Q}$;
3) Calcolare $[L_p : \mathbb{Q}]$ al variare del primo p.

Esercizio 158. Sia $f(x) = x^4 + ax^2 + b$ un polinomio irriducibile a coefficienti in $\mathbb{Q}$ e sia G il suo gruppo di Galois.

1) se b è un quadrato $\in \mathbb{Q}$ allora $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$;
2) se $b(a^2 - 4b)$ è un quadrato in $\mathbb{Q}$ allora $G \simeq \mathbb{Z}/4$;
3) $G \simeq \mathsf{D}_4$ altrimenti.

Esercizio 159. Sia $E \subset F$ una estensione finita di Galois. Sia $\sigma \in \mathrm{Gal}(F : E)$ tale che $E = \{x \in F \,:\, \sigma(x) = x\}$. Dimostrare che σ genera il gruppo di Galois $\mathrm{Gal}(F : E)$.

Esercizio 160. Sia $E \subset F$ una estensione separabile finita. Sull'E spazio vettoriale F possiamo definire la forma E-bilineare simmetrica (detta a volte forma traccia) $(x : y) = \mathrm{Tr}_E^F(xy)$. Dimostrare che è una forma non degenere.

Esercizio 161. Sia $\phi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^3$ il morfismo di $\mathbb{Z}$ moduli associato alla matrice

$$\begin{pmatrix} 4 & 8 \\ 12 & 6 \\ 6 & 8 \end{pmatrix}.$$

Descrivere lo $\mathbb{Z}$-modulo $\mathbb{Z}^3/\operatorname{Im}\phi$ come somma diretta di moduli ciclici.

Esercizio 162. Sia $\Bbbk$ algebricamente chiuso, V uno spazio vettoriale di dimensione finita su $\Bbbk$ e $T, S : V \longrightarrow V$ due applicazioni lineari. Dimostrare che T è coniugata ad S se e solo se $\dim \ker(T - \lambda)^i = \dim \ker(S - \lambda)^i$ per ogni $\lambda \in \Bbbk$ e per ogni $i = 1, \ldots, n$.

Esercizio 163. Sia V uno spazio vettoriale di dimensione finita su un campo $\Bbbk$ e sia $T : V \longrightarrow V$ una applicazione lineare. Un sottospazio W di V si dice T stabile se $T(W) \subset W$. T si dice semisemplice se per ogni $W \subset V$ sottospazio T stabile esiste un sottospazio T stabile U tale che $V = U \oplus W$.

Dimostrare che T è semisemplice se e solo se μ_T non ha fattori multipli.

Di seguito trovate i testi e le tracce delle soluzioni di alcuni compiti dati in passato. Considerate però che il corso era diverso da quello fatto quest'anno e questo condiziona sia la scelta degli esercizi che le loro soluzioni, quindi sono sensibilmente diversi dal tipo di compito che vi troverete di fronte voi.

32. Compito 12 luglio 2004

Esercizio 164. Sia $L \supset \mathbb{Q}$ una estensione di grado 2 dimostrare che esiste d in $\mathbb{Z}$ tale che $L = \mathbb{Q}[\sqrt{d}]$.

Esercizio 165. Sia L una estensione di Galois di $\mathbb{Q}$ della forma $\mathbb{Q}[\sqrt[3]{d}]$ con $d \in \mathbb{Z}$. Dimostrare che d è un cubo perfetto.

[se $x \in \mathbb{R}$ con $\sqrt[3]{x}$ indico la radice cubica reale di x]

Esercizio 166. Sia $f \in \mathbb{Z}(x)$ un polinomio monico irriducibile di grado dispari con radici $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ e poniamo $g = (x - \alpha_1^2) \cdots (x - \alpha_n^2)$.

1) mostrare che g è un polinomio a coefficienti interi;
2) mostrare che g è un polinomio irriducibile in $\mathbb{Q}[x]$ (o $\mathbb{Z}[x]$).

Esercizio 167. Sia L il campo di spezzamento del polinomio $x^3 - 2$ su $\mathbb{Q}$ e sia K il campo di spezzamento di $(x^3 - 2)(x^3 - 5x + 1)$ su $\mathbb{Q}$.

1) Calcolare il gruppo di Galois di L su $\mathbb{Q}$;
2) Descrivere i sottocampi di L che sono estensioni normali di $\mathbb{Q}$;
3) Dimostrare che il gruppo di Galois di K su $\mathbb{Q}$ è $\mathsf{S}_3 \times \mathsf{S}_3$.

33. Tracce di soluzioni degli esercizi del compito del 12 luglio

Soluzione esercizio 164. Sia $\alpha \in L \smallsetminus \mathbb{Q}$. Allora $L = \mathbb{Q}[\alpha]$ e esistono $a, b, c \in \mathbb{Z}$ con $a \neq 0$ tali che $a\alpha^2 + b\alpha + c = 0$ e sia $\Delta = b^2 - 4\,a\,c$. Abbiamo $L = \mathbb{Q}[\sqrt{\Delta}]$.

Soluzione esercizio 165. Sia $\delta = \sqrt[3]{d}$, $\omega = e^{\frac{2\pi \mathrm{i}}{3}}$ e $f = x^3 - d = (x - \delta)(x - \omega\delta)(x - \omega^2\delta)$. Se f è irriducibile su $\mathbb{Q}$ allora è il polinomio minimo di δ su $\mathbb{Q}$ e quindi essendo l'estensione normale avremmo $\omega \in \mathbb{Q}[\delta] \subset \mathbb{R}$ che non è vero. Quindi f è riducibile e in particolare essendo un polinomio monico di grado 3 a coefficienti in $\mathbb{Z}$ ha una radice in $\mathbb{Z}$. Quindi d è un cubo perfetto.

Soluzione esercizio 166. Osserviamo che il gruppo di Galois permuta le radici $\alpha_1, \dots, \alpha_n$ e quindi g è lasciato invariato dall'azione del gruppo di Galois. Osserviamo inoltre che le radici sono interi algebrici quindi anche i coefficienti del polinomio sono interi algebrici. Quindi sono numeri interi.

Consideriamo la catena di estensioni $\mathbb{Q} \subset \mathbb{Q}(\alpha_1^2) \subset \mathbb{Q}(\alpha_1)$ e osserviamo che $\mathbb{Q} \subset \mathbb{Q}(\alpha_1)$ è una estensione di grado n mentre $\mathbb{Q}(\alpha_1^2) \subset \mathbb{Q}(\alpha_1)$ è una estensione di grado 1 o 2. Poiché n è dispari non può di essere di grado 2. Quindi $\mathbb{Q}(\alpha_1^2) = \mathbb{Q}(\alpha_1)$ e quindi il polinomio minimo di α_1^2 ha grado n, quindi è il polinomio g. In particolare g è irriducibile.

Soluzione esercizio 167. 1) S_3;

2) È il sottocampo corrispondente ad A_3 che è l'unico sottogruppo normale di S_3. Quindi è l'unico sottocampo di grado 2 su $\mathbb{Q}$ ovvero $L' = \mathbb{Q}[e^{\frac{2\pi \mathrm{i}}{3}}] = \mathbb{Q}[\sqrt{-3}]$.

3) Sia M il campo di spezzamento di $x^3 - 5x + 1$. Il discriminante del polinomio è $473 = 11 \cdot 43$, quindi il suo gruppo di Galois è S_3 e ha un unica sottoestensione normale $M' = \mathbb{Q}[\sqrt{473}]$. Ora $M \cap L = \mathbb{Q}$. Sia infatti $M \cap L = N$. Osserviamo che N è una estensione normale non banale di $\mathbb{Q}$ contenuta in L e M. Quindi per motivi di dimensione o $N = L = M$ o $N = L' = M'$ o $N = \mathbb{Q}$. Nei primi due casi ricaviamo $L' = M'$ che invece non è verificata visto che $M' \subset \mathbb{R}$ e L' invece no. Quindi $N = \mathbb{Q}$. Osserviamo infine che $K = LM$: la tesi segue quindi dalla descrizione del gruppo di Galois del prodotto di due estension normali.

34. Compito 23 luglio 2004

Esercizio 168. Sia $E = \mathbb{Q}[\sqrt{-3}, \sqrt{-5}]$ e $F = \mathbb{Q}[e^{\frac{2\pi \mathrm{i}}{5}}]$. Dire se i campi E ed F sono isomorfi.

Esercizio 169. Sia f un polinomio a coefficienti in un campo E con radici distinte $\alpha_1, \dots, \alpha_n$. Sia $g \in E[x_1, \dots, x_n]$ un polinomio simmetrico in $x_1, \dots, x_n$. Dimostrare che $g(\alpha_1, \dots, \alpha_n) \in E$.

Esercizio 170. Siano $E, F \subset \mathbb{C}$ due estensioni di Galois di $\mathbb{Q}$. Dimostrare che E è isomorfo a F (come campi) se e solo $E = F$. Se leviamo l'ipotesi E, F estensioni di Galois, l'affermazione rimane vera?

Esercizio 171. Sia f il polinomio $x^5 - 2$ e g il polinomio $(x^5 - 2)(x^5 - 3)$. Sia F il campo di spezzamento di f su $\mathbb{Q}$ e E il campo di spezzamento di g su $\mathbb{Q}$.

1) Calcolare $[F : \mathbb{Q}]$ e dimostrare che f è irriducibile su $\mathbb{Q}[e^{\frac{2\pi \mathrm{i}}{5}}]$;
2) Descrivere il gruppo di Galois di F su $\mathbb{Q}$ come gruppo di permutazioni delle radici di f o mediante generatori e relazioni;
3) Calcolare $[E : \mathbb{Q}]$.

35. Tracce di soluzioni degli esercizi del compito del 23 luglio

Soluzione esercizio 168. Ogni morfismo di campi è l'identità su $\mathbb{Q}$. Quindi se E e F fossero isomorfi anche i loro gruppi di Galois su $\mathbb{Q}$ lo sarebbero, ma $\mathrm{Gal}(E,\mathbb{Q}) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$ mentre $\mathrm{Gal}(F,\mathbb{Q}) = \mathbb{Z}/4$.

Soluzione esercizio 169. Basta dimostrare che $c = g(\alpha_1,\dots,\alpha_n)$ è fissato da ogni automorfismo di $\overline{\mathbb{Q}}$. Ma un tale automorfismo non fa che permutare le radici e quindi essendo g simmetrico fissa c.

Soluzione esercizio 170. Se $E = F$ chiaramente è anche $E \simeq F$. Viceversa sia $\varphi : E \longrightarrow F$ un isomorfismo. Osserviamo che $\varphi|_{\mathbb{Q}}$ è l'identità. Poiché E è una estensione normale di $\mathbb{Q}$ abbiamo $\varphi(E) \subset E$ e quindi $F \subset E$. Analogamente si dimostra $E \subset F$.

Soluzione esercizio 171. Sia $\alpha = \sqrt[5]{2}$, $\beta = \sqrt[5]{3}$ e $\omega = e^{\frac{2\pi \mathrm{i}}{5}}$. Osserviamo che $F = \mathbb{Q}[\alpha,\omega]$ e $E = \mathbb{Q}[\alpha,\beta,\omega]$.

1) Osserviamo che f è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein. Quindi $[\mathbb{Q}[\alpha],\mathbb{Q}] = 5$. Inoltre sappiamo che $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$ quindi $[F : \mathbb{Q}[\alpha]] \leqslant 4$. Quindi $[F : \mathbb{Q}] \leqslant 20$. Inoltre poichè $\mathbb{Q} \subset \mathbb{Q}[\omega] \subset F$ e $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset F$ Abbiamo che 5 e 4 dividono $[F : \mathbb{Q}]$ quindi $[E : \mathbb{Q}] = 20$

2) Osserviamo che $\sigma(\alpha)$ e $\sigma(\omega)$ determinano σ. Inoltre $\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha, \omega^3\alpha, \omega^4\alpha\}$ e $\sigma(\omega) \in \{\omega, \omega^2, \omega^3, \omega^4\}$. Quindi per motivi di cardinalità abbiamo che esistono σ e τ nel grupo di galois tale che:

$$\sigma(\alpha) = \alpha \quad \text{e} \quad \sigma(\omega) = \omega^2 \qquad\qquad \tau(\alpha) = \omega\alpha \quad \text{e} \quad \tau(\omega) = \omega.$$

Osserviamo che σ ha ordine 4 e τ ha ordine 5 quindi il gruppo generato da σ e τ ha almeno ordine 20. Quindi σ e τ generano il gruppo di Galois.

Le relazioni di σ e τ sono $\sigma^4 = \tau^5 = \mathrm{id}$ e $\sigma\tau\sigma^{-1} = \tau^2$ (il gruppo con queste relazioni si vede subito ha ordine minore o uguale a 20 e quindi queste relazioni generano le relazioni tra σ e τ.

Come permutazioni abbiamo $\sigma = (2354)$ e $\tau = (12345)$.

3) Osserviamo che F contiene le radici quinte dell'unità. Quindi $E = F[\beta]$ è una estensione ciclica di grado un divisore di 5. Se dimostriamo che $\beta \notin F$ allora ha grado 5 e quindi E ha grado 120 su $\mathbb{Q}$. Sia $\beta = \sum a_i\alpha^i$ con $a_i \in \mathbb{Q}[\omega]$. Allora $\tau(\beta) = \omega^j\beta$ implica $a_i = 0$ per $i \neq j$. Quindi $\beta = a\alpha^j$. Allora $3 = \beta^5 = a^5 2^j$ ovvero $a^5 = 3/2^j$. Ma l'ultima equazione ha grado 5 su $\mathbb{Q}$ (infati $2^j x^5 - 3$ è irriducibile su $\mathbb{Q}$ per Eisenstein) e quindi anche su $\mathbb{Q}[\omega]$ (come nel punto 1)).

36. Compito 24 settembre

Esercizio 172. Esistono $\alpha \in \mathbb{R}$ e $\beta \in \mathbb{C} \smallsetminus \mathbb{R}$ tali che $\mathbb{Q}[\alpha]$ è isomorfo a $\mathbb{Q}[\beta]$?

Esercizio 173. Sia α una radice del polinomio $f(x) = x^4 + 3x + 3$ e sia $\beta = \alpha^2$.

1) Dimostrare che $\mathbb{Q}[\alpha] = \mathbb{Q}[\beta]$;
2) Calcolare il polinomio minimo di β su $\mathbb{Q}$.

Esercizio 174. Sia $L \supset \mathbb{Q}$ il campo di spezzamento del polinomio $x^5 - 5x^4 - 10x^3 + 5$. Calcolare $\mathrm{Gal}(L : \mathbb{Q})$.

Esercizio 175. Sia $\mathbb{Q} \subset E \subset \overline{\mathbb{Q}}$. Supponiamo che E contenga tutte le radici dell'unità. Dimostrare che

1) se $\mathrm{Gal}(\overline{\mathbb{Q}} : E)$ è un gruppo ciclico generato da σ e $\sigma^p = \mathrm{id}$ con p primo allora $E = \overline{\mathbb{Q}}$;
2) se $\overline{\mathbb{Q}}$ è una estensione finita di E allora $E = \overline{\mathbb{Q}}$.

37. Tracce di soluzioni degli esercizi del compito del 24 settembre

Soluzione esercizio 172. Basta prendere $\alpha = \sqrt[3]{2}$ e $\beta = e^{\frac{2\pi \mathrm{i}}{3}}\sqrt[3]{2}$. Poiché questi due numeri hanno lo stesso polinomio minimo (ovvero $x^3 - 2$) su $\mathbb{Q}$ le due estensioni sono isomorfe.

Soluzione esercizio 173. Chiaramente $\beta \in \mathbb{Q}[\alpha]$ quindi $\mathbb{Q}[\beta] \subset \mathbb{Q}[\alpha]$. Viceversa osserviamo che $\alpha = -\frac{1}{3}\alpha^4 - 1 = -\frac{1}{3}\beta^2 - 1$, quindi anche $\alpha \in \mathbb{Q}[\beta]$ da cui $\mathbb{Q}[\alpha] \subset \mathbb{Q}[\beta]$;

Osserviamo ora che f è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein. Quindi $[\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\beta] : \mathbb{Q}] = 4$. In particolare il polinomio minimo di β ha grado 4. Infine da $\alpha = -\frac{1}{3}\beta^2 - 1$ ricaviamo $\beta = \alpha^2 = (-\frac{1}{3}\beta^2 - 1)^2 = \frac{1}{9}\beta^4 + \frac{2}{3}\beta^2 + 1$ da cui $\beta^4 + 6\beta^2 - 9\beta + 9 = 0$. Il polinomio minimo di β su $\mathbb{Q}$ è quindi $x^4 + 6x^2 - 9x + 9$.

Soluzione esercizio 174. Sia $G = \mathrm{Gal}(L : \mathbb{Q})$. Osserviamo che per il criterio di Eisenstein f è un polinomio irriducibile su $\mathbb{Q}$ quindi G è un sottogruppo di S_5 e $5 | \mathit{card}(G)$. In particolare G contiene un elemento di ordine 5 ovvero un 5-ciclo.

Inoltre se riduciamo il polinomio modulo due troviamo il polinomio $\bar{f} = x^5 + x^4 + 1 = (x^2 + x + 1)(x^3 + x + 1)$. Quindi G contiene un $2,3$ ciclo σ. Osserviamo che $\tau = \sigma^3$ è un 2 ciclo. Quindi G contiene un 2 ciclo e un 5 ciclo, quindi $G = \mathsf{S}_5$.

Alternativamente possiamo dimostrare che G contiene un 2 ciclo studiando le radici reali di f. Sia $f' = 5x^2(x^2 - 4x - 6)$ che ha radici 0, $\alpha = 2 - \sqrt{10} \in [-2,-1]$ e $\beta = 2 + \sqrt{10} \in [5,6]$. In particolare f è crescente in $(-\infty,\alpha) \cup (\beta,\infty)$ e decrescente in (α,β). Quindi ha al massimo tre radici reali. Inoltre $f(0) = 5 > 0$ e $f(1) = -9 < 0$, quindi ha esattamente tre radici reali. Quindi il coniugio $z \mapsto \bar{z}$ è un elemento del gruppo di Galois che lascia fisse 3 radici e scambia le altre 2 ovvero è un 2 ciclo. Concludiamo quindi come sopra che $G = \mathsf{S}_5$.

Soluzione esercizio 175. Per assurdo sia p primo che divide il grado dell'estensione. Esiste allora un elemento σ del gruppo di Galois di ordine p e sia F il campo fissato da σ. Osserviamo che $\overline{\mathbb{Q}} \supset F$ è una estensione ciclica di ordine p il cui gruppo di Galois è generato da σ (ci siamo quindi ridotti a dimostrare il punto (1) dell'esercizio). In particolare per il teorema sulle estensioni cicliche è un'estensione della forma $\overline{\mathbb{Q}} = F[\alpha]$ con il polinomio minimo di α della forma $x^p - a$ con $a \in F$. Sia ora $\beta \in \overline{\mathbb{Q}}$ tale che $\beta^p = \alpha$. Osserviamo che $\beta^{p^2} = a \in F$. Allora $\sigma(\beta) = \zeta\beta$ con $\zeta^{p^2} = 1$. Inoltre da $\sigma^p = \mathrm{id}$ ricaviamo $\sigma^p(\beta) = \zeta^p\beta = \beta$ ovvero $\zeta^p = 1$. Quindi $\sigma(\alpha) = \sigma(\beta^p) = \beta^p = \alpha$ e α è fissato dal gruppo di Galois ma allora $\alpha \in F$ contro $F[\alpha] \supset F$ estensione di grado p.

38. Compito venerdì 27 gennaio 2006

Esercizio 176. Enunciare il teorema di struttura dei moduli finitamente generati su un anello ad ideali principali.

Esercizio 177. Sia $f \in \mathbb{Q}[t]$ un polinomio di grado 2 e sia $\mathbb{Q} \subset E$ una estensione finita di grado dispari. Sia $\alpha \in E$ tale che $f(\alpha) = 0$ allora $\alpha \in \mathbb{Q}$.

Esercizio 178. Sia p un numero naturale primo. Siano $f_p(x) = x^3 + 3\,p\,x + p$, $g_p(x) = (x^2 - p)\,f_p(x)$, E_p il campo di spezzamento su $\mathbb{Q}$ di f_p e K_p il campo di spezzamento su $\mathbb{Q}$ di g_p.

1) Si calcoli $\mathrm{Gal}(E_p, \mathbb{Q})$;
2) Si calcoli $\mathrm{Gal}(K_p, \mathbb{Q})$.

Esercizio 179. Sia $\zeta_h = e^{\frac{2\pi\,\mathrm{i}}{h}}$. Sia $n \geqslant m$, dimostrare che $\mathbb{Q}[\zeta_n] = \mathbb{Q}[\zeta_m]$ se e solo se $n = m$ o $n = 2m$ e m è dispari.

Esercizio 180. Sia V uno spazio vettoriale di dimensione finita n su un campo $\Bbbk$ e sia $T : V \longrightarrow V$ una applicazione lineare.

1) Dimostrare che V è ciclico (esiste $v \in V$ tale che $\{T^i(v) : i \in \mathbb{N} \cup \{0\}\}$ genera V) se e solo se il polinomio minimo di T ha grado n.
2) Sia $\mathbb{F}_p \subset \mathbb{F}$ una estensione di grado n. Dimostrare che esiste $\alpha \in \mathbb{F}$ tale che $\{\phi(\alpha) : \phi \in \mathrm{Gal}(\mathbb{F}, \mathbb{F}_p)\}$ è una $\mathbb{F}_p$ base di $\mathbb{F}$.

39. Soluzioni del compito del 27 gennaio 2006

Soluzione dell'esercizio 176. Ogni modulo M finitamente generato su un anello ad ideali principali A è isomorfo a un modulo della forma $A/(f_1) \oplus \cdots \oplus A/(f_r)$ con $f_1 | f_2 | \ldots | f_r$. [Alcuni hanno scritto della forma $A/(p_1^{m_1}) \oplus \cdots \oplus A/(p_r^{m_r})$ con p_i primi e andava bene uguale.]

Soluzione dell'esercizio 177. Consideriamo $\mathbb{Q} \subset \mathbb{Q}[\alpha] \subset E$. Poiché $\mathbb{Q}[\alpha]$ risolve un polinomio di grado 2 l'estensione $\mathbb{Q} \subset \mathbb{Q}[\alpha]$ ha grado 1 o 2. Inoltre poiché $[E : \mathbb{Q}] = [E : \mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha] : \mathbb{Q}]$ è un numero dispari ricaviamo che $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 1$ e quindi $\alpha \in \mathbb{Q}$.

Soluzione dell'esercizio 178. 1) Osserviamo che f è irriducibile per il criterio di Eisenstein, quindi $H_p = \mathrm{Gal}(E_p, \mathbb{Q})$ è uguale a A_3 o a S_3. Inoltre poiché $f' > 0$, il polinomio f ha una unica radice reale. Quindi la coniugazione complessa definisce un elemento non banale di ordine 2 del gruppo di Galois da cui concludiamo $H_p = \mathsf{S}_3$.

2) Dimostriamo innanzitutto che $\sqrt{p} \notin E_p$. Infatti i sottocampi di E_p di grado 2 su $\mathbb{Q}$ sono in corrispondenza con i sottogruppi di H_p di indice 2. Quindi $\sqrt{p} \in E_p$ se e solo se $\mathbb{Q}[\sqrt{p}] = E_p^{\mathsf{A}_3}$. Ma quest'ultimo campo è uguale a $\mathbb{Q}[\sqrt{\Delta}]$ con Δ il discriminante che in questo caso è uguale a $-4(3p)^3 - 27(p)^2 = -27\,p^2\,(4\,p + 1)$. In particolare $\Delta < 0$ quindi $\mathbb{Q}[\sqrt{\Delta}] \not\subset \mathbb{R}$ al contrario di $\mathbb{Q}[\sqrt{p}]$.

Quindi E_p e $\mathbb{Q}[\sqrt{p}]$ sono due estensioni normali di $\mathbb{Q}$ la cui intersezione è uguale a $\mathbb{Q}$, da cui $\mathrm{Gal}(K_p, \mathbb{Q})$ è il prodotto dei due gruppi di Galois e quindi è isomorfo a $\mathsf{S}_3 \times \mathbb{Z}/2$.

Soluzione dell'esercizio 179. Analizziamo prima il caso in cui m divide n: sia $n = mh$, allora $\zeta_m = \zeta_n^h$ da cui $\mathbb{Q} \subset \mathbb{Q}[\zeta_m] \subset \mathbb{Q}[\zeta_n]$ e quindi $\mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_n]$ se e solo se $\varphi(m) = [\mathbb{Q}[\zeta_m] : \mathbb{Q}] = [\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n) = \varphi(mh)$ con φ la funzione di Eulero. Sia $h = k\ell$ con ℓ primo con m e k tale che se p è primo e p divide k allora p divide m. Dalla espressione esplicita di φ ricaviamo $\varphi(mh) = k\varphi(m)\varphi(\ell)$. Quindi $\varphi(mh) = \varphi(m)$ se e solo se $k = 1$ e $\ell = 1$ o 2. Quindi $n = m$ o $n = 2m$ con m dispari.

Supponiamo ora $K = \mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_n]$ e sia $\ell = m.c.m.(n, m)$. Osserviamo che se $M.C.D.(m, n) = am + bn$ allora $\zeta_\ell = \zeta_m^b\,\zeta_n^a$. Quindi abbiamo m e n dividono ℓ e $\mathbb{Q}[\zeta_\ell] = \mathbb{Q}[\zeta_m] = \mathbb{Q}[\zeta_n]$, e dalla discussione precedente ricaviamo $\ell = m$ o $\ell = 2m$ e m dispari e analogamente per n. Da cui la tesi.

Soluzione dell'esercizio 180. 1) Consideriamo V come un $A = \Bbbk[t]$ modulo nel solito modo: se $f \in A$ e $v \in V$ definiamo $f \cdot v = (f(T))(v)$.

Osserviamo innanzitutto che la condizione di essere ciclico del testo è equivalente al fatto che $V \simeq A/(f)$ con f polinomio di grado n. Infatti se $V = A/(f)$ allora $v = \overline{1}$ ha le proprietà enunciate, infatti $v = \overline{1}, T(v) = \overline{t}, \ldots, T^{n-1}(v) = \overline{t}^{n-1}$ sono una base di V se f ha grado n, viceversa se v è come nel testo dell'esercizio l'applicazione di A-moduli $\phi : A \longrightarrow V$ definita da $\phi(f) = f \cdot v$ è surgettività, quindi $V \simeq A/\ker\phi$. Ma essendo A ad ideali principali $\ker\phi = (f)$ per qualche f e essendo V di dimensione n ricaviamo che anche il grado di f è n.

Osserviamo inoltre che se $V \simeq A/(f_1) \oplus \cdots \oplus A/(f_r)$ con $f_1 | f_2 | \ldots | f_r$ allora il polinomio minimo di T è uguale (a meno di uno scalare non nullo) a f_r e che (se V ha dimensione finite su $\Bbbk$ gli f_i sono non nulli e la dimensione di V è uguale alla somma dei gradi dei polinomi f_i. La tesi segue immediatamente.

2) Applicando il punto 1) al caso di $\Bbbk = \mathbb{F}_p$, $V = \mathbb{F}$ e $T = \varphi$ l'automorfismo di Frobenius, $x \mapsto x^p$, e ricordando che $\mathrm{Gal}(\mathbb{F}, \mathbb{F}_p) = \{\mathrm{id}, \varphi, \ldots, \varphi^{n-1}\}$ otteniamo che esiste α con le proprietà richieste se e solo se il polinomio minimo di φ ha grado n. Ma il polinomio minimo ha sicuramente grado minore o uguale a n e se avesse grado minore avremmo che esisterebbe un polinomio non nullo di grado minore o uguale a p^{n-1} che annulla tutti gli elementi di $\mathbb{F}$. Ma gli elementi di $\mathbb{F}$ sono p^n e quindi un tale polinomio non può esistere.

40. Compito giovedì 23 febbraio 2006

Esercizio 181. Enunciare, con tutte le ipotesi, il teorema di corrispondenza tra sottocampi e sottogruppi.

Esercizio 182. Sia $f \in \mathbb{Q}[t]$ un polinomio di quinto grado e F il suo campo di spezzamento. Se $\mathrm{Gal}(F, \mathbb{Q}) = \mathbb{Z}/5$ allora le sue radici sono reali.

Esercizio 183. Sia A un dominio ad ideali principali. Sia M un A modulo libero finitamente generato e sia N un sottomodulo di M. Dimostrare che N è un modulo libero.

Esercizio 184. Sia $f(x) = x^5 - 10x + 2$ (di discriminante pari a $-2^4 \cdot 5^5 \cdot 7 \cdot 73$) e sia $g_n(x) = f(x)(x^2 + n)$. Sia F il campo di spezzamento di f su $\mathbb{Q}$ e K_n il campo di spezzamento di g_n su $\mathbb{Q}$;

1) Calcolare $\mathrm{Gal}(F, \mathbb{Q})$;
2) Calcolare $[K_n : \mathbb{Q}]$ al variare di $n \in \mathbb{Z}$.

Esercizio 185. Sia L il minimo sottocampo di $\mathbb{C}$ contenente tutte le radici quadrate dei numeri razionali.

1) per quali n, $\mathbb{Q}[\zeta_n] \cap L \neq \mathbb{Q}$?
2) calcolare $[\mathbb{Q}[\zeta_n] \cap L : \mathbb{Q}]$ al variare di n numero naturale.

[Potrebbe essere utile ricordarsi che $(\mathbb{Z}/p^n)^*$ è ciclico per p primo dispari e è isomorfo a $\mathbb{Z}/2 \times \mathbb{Z}/2^{n-2}$ per $p = 2$ e $n \geqslant 2$]

41. Soluzioni del compito del 23 febbraio 2006

Soluzione dell'esercizio 181. Sia $E \subset F$ una estensione di Galois di dimensione finita e sia G il suo gruppo di Galois. Inoltre sia $\mathcal{G}$ l'insieme dei sottogruppi di G e $\mathcal{C}$ l'insieme dei sottocampi di F contenti E. Se $H \in \mathcal{G}$ l'insieme F^H degli elementi fissati da H è un elemento di $\mathcal{C}$ e se $K \in \mathcal{C}$ il gruppo di Galois di $K \subset F$ è un sottogruppo di G che denotiamo con G_K. Allora le applicazioni $H \mapsto F^H$ da $\mathcal{G}$ in $\mathcal{C}$ e $K \mapsto G_K$ da $\mathcal{C}$ in $\mathcal{G}$ sono una l'inversa dell'altra.

Soluzione dell'esercizio 182. Se f non ha tutte le radici reali allora la coniugazione complessa definisce un elemento non banale di ordine 2 e quindi il gruppo di Galois non può essere $\mathbb{Z}/5$.

Soluzione dell'esercizio 183. Sia $M \simeq A^n$ e osserviamo che se $a\,m = 0$ allora $a = 0$ o $m = 0$. Poichè A è notheriano, anche M lo è. Quindi N è finitamente generato e per il modulo di struttura dei moduli finitamente genreati su un anello ad ideali principali è isomorfo ad un modulo della forma $A/(a_1) \oplus \cdots \oplus A/(a_r)$ e possiamo supporre $(a_i) \neq A$ per ogni i. Osserviamo che nel modulo così descritto $a_1(1, 0, \ldots, 0) = 0$ quindi esiste $n \in N \subset M$ non nullo tale che $a_1 n = 0$. Quindi $a_1 = 0$. Analogamente $a_i = 0$ per ogni i. Quindi $N \simeq A^r$ è un modulo libero.

Soluzione dell'esercizio 184. 1) Per il criterio di Eisenstein f è irriducibile quindi il gruppo di Galois G di F su E è un sottogruppo di S_5 il cui ordine è divisibile per 5. G contiene quindi un elemento di ordine 5 di S_5 ovvero un 5-ciclo. Inoltre osserviamo che $f' = 5(x^4 - 2)$ ha due radici reali $\pm\alpha$ con $\alpha = \sqrt[4]{2}$ e se ristretta alla retta reale ha segno positivo fuori dell'intervallo $(-\alpha, \alpha)$ e negativo all'interno dell'intervallo . Inoltre $f(-\alpha) = 8\alpha + 2 > 0$ e $f(\alpha) = -8\alpha + 2 < -8 + 2 = -6 < 0$. Quindi f ha esattamente 3 radici reali. Il coniugio complesso φ è quindi un elemento del gruppo di Galois che fissa tre radici e ne scambia 2 ed è quindi una trasposizione. Ma un sottogruppo di S_5 che contiene un 5 ciclo e una trasposizione è tutto S_5, quindi $G = \mathsf{S}_5$.

2) Sia $m = -n$. Studiamo quando $\sqrt{m} \in F$. Sicuramente $\sqrt{m} \in F$ se m è un quadrato in $\mathbb{Z}$. Supponiamo quindi che m non sia un quadrato in questo caso $L = \mathbb{Q}[\sqrt{m}]$ è una estensione di grado 2 di $\mathbb{Q}$. Osserviamo che i sottocampi di F di grado 2 su $\mathbb{Q}$ sono in corrispondenza con i sottogruppi di $G = \mathsf{S}_5$ di indice 2. Ma tali sottogruppi sono tutti normali. Esiste quindi uno solo di tali sottogruppi ed è A_5. Quindi $\sqrt{m} \in F$ se e solo se $\mathbb{Q}[\sqrt{m}] = F^{\mathsf{A}_5} = \mathbb{Q}[\sqrt{\Delta}]$ con Δ il discriminante di f. Si tratta quindi di studiare quando $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{\Delta}]$. Supponiamo che siano uguali e osserviamo che se σ è l'elemento non banale del gruppo di Galois di L su $\mathbb{Q}$, poiché $\sqrt{m}$ e $\sqrt{\Delta} \notin \mathbb{Q}$ allora $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$ e se $\sigma(\sqrt{n}) = -\sqrt{n}$. Quindi $\sigma(\frac{\sqrt{\Delta}}{\sqrt{n}}) = \frac{\sqrt{\Delta}}{\sqrt{n}}$ ovvero $\frac{\sqrt{\Delta}}{\sqrt{n}} \in \mathbb{Q}$ da cui $\Delta = \lambda^2 n$ con $\lambda \in \mathbb{Q}$. Quindi $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{\Delta}]$ se e solo se $m = -5 \cdot 7 \cdot 73 \cdot u^2$ con $u \in \mathbb{Z}$.

Quindi se $-n$ è un quadrato o $n = 5 \cdot 7 \cdot 73 \cdot u^2$ con $u \in \mathbb{Z}$ allora $K_n = F$ e quindi $[K_n : \mathbb{Q}] = 120$. Nei rimanenti casi avremo $K_n = F[\sqrt{-n}]$ e $\sqrt{-n} \notin F$ da cui $[K_n : \mathbb{Q}] = 2[F : \mathbb{Q}] = 240$.

Soluzione dell'esercizio 185. 2) Sia C_n il gruppo ciclico con n elementi. Osserviamo che una estensione normale finita F di $\mathbb{Q}$ è contenuta in L se e solo $\mathrm{Gal}(F, \mathbb{Q}) = \mathsf{C}_2^r$. Infatti se $\mathrm{Gal}(F, \mathbb{Q}) = \mathsf{C}_2^r$ sia F_i il sottocampo fissato da $\mathsf{C}_2^{i-1} \times \{1\} \times \mathsf{C}_2^{r-i}$. Allora F_i è una estensione di grado 2 di $\mathbb{Q}$, F è il prodotto delle estensioni F_i. Quindi $F_i = \mathbb{Q}[\sqrt{d_i}]$ per qualche d_i in $\mathbb{Q}$ che non sia un quadrato $F = \mathbb{Q}[\sqrt{d_1}, \ldots, \sqrt{d_r}] \subset L$. Viceversa osserviamo che $L \supset \mathbb{Q}$ è di Galois, che $\mathrm{Gal}(L, \mathbb{Q})$ è abeliano e che ogni elemento di $\mathrm{Gal}(L, \mathbb{Q})$ ha ordine 2. Quindi se $F \subset L$ è una estensione finita, poiché ogni automorfismo di F si può estendere a uno di L ricaviamo che anche $\mathrm{Gal}(F, \mathbb{Q})$ è abeliano e che ogni suo elemento ha ordine 2. Quindi è isomorfo a C_2^r per qualche r.

Quindi si tratta di calcolare il massimo sottocampo di $\mathbb{Q}[\zeta_n]$ che ha un gruppo di Galois di questa forma. Ma i gruppi di Galois dei sottocampi di $\mathbb{Q}[\zeta_n]$ sono i quozienti di $\mathrm{Gal}(\mathbb{Q}[\zeta_n], \mathbb{Q}) = (\mathbb{Z}/n)^* = \Gamma$, quindi si tratta di calcolare il massimo quoziente di Γ di questa forma. Sia $n = 2^m p_1^{m_1} \cdots p_s^{m_s}$ con p_i primi dispari distinti e $m_i > 0$. Sia inoltre

$n' = p_1^{m_1-1} \cdots p_s^{m_s-1}$. Allora ricordando che $(\mathbb{Z}/p^t)^*$ è ciclico per p primo dispari e che $(\mathbb{Z}/2^m)^* \simeq \mathsf{C}_2 \times \mathsf{C}_{2^{m-2}}$ per $m > 2$ ricaviamo che

$$\Gamma = (\mathbb{Z}/n)^* = \begin{cases} \mathsf{C}_{p_1-1} \times \mathsf{C}_{p_s-1} \times \mathsf{C}_{n'} & \text{se} \quad m = 1; \\ \mathsf{C}_2 \times \mathsf{C}_{p_1-1} \times \mathsf{C}_{p_s-1} \times \mathsf{C}_{n'} & \text{se} \quad m = 2; \\ \mathsf{C}_2 \times \mathsf{C}_{2^{m-2}} \times \mathsf{C}_{p_1-1} \times \mathsf{C}_{p_s-1} \times \mathsf{C}_{n'} & \text{se} \quad m > 2. \end{cases}$$

Sia ora H un sottogruppo di Γ tale che $\Gamma/H \simeq \mathsf{C}_2^r$ allora poiché tutti gli elementi al quoziente hanno ordinne che divide 2 abbiamo $H \supset \Gamma^2$. Viceversa Γ^2 è un sottogruppo di Γ e Γ/Γ^2 è un gruppo abeliano finito in cui tutti gli elementi hanno ordine 2 quindi è isomorfo a C_2^r. Quindi Γ/Γ^2 è il massimo quoziente di Γ della forma cercata e $[\mathbb{Q}[\zeta_n] \cap L : \mathbb{Q}] = card(\Gamma/\Gamma^2)$ da cui $[\mathbb{Q}[\zeta_n] \cap L : \mathbb{Q}] = s$ se $m = 1$, $[\mathbb{Q}[\zeta_n] \cap L : \mathbb{Q}] = s + 1$ se $m = 2$ e $[\mathbb{Q}[\zeta_n] \cap L : \mathbb{Q}] = s + 2$ se $m > 2$.

Da 2) ricaviamo anche $\mathbb{Q}[\zeta_n] \cap L = \mathbb{Q}$ se e solo se $n = 2, 1$ [per questa parte ovviamente bastava molto meno].

42. Compito mercoledì 7 giugno 2006

Esercizio 186. Sia E un campo di caratteristica 0 contenente tutte le radici dell'unità. Descrivere (senza dare le dimostrazioni) le estensioni finite di Galois con gruppo di Galois un gruppo ciclico finito.

Esercizio 187. Sia $E = \mathbb{C}(z)$ il campo delle funzioni razionali a coefficienti in $\mathbb{C}$ nella variabile z e sia F una chiusura algebrica di E. Se n è un numero naturale sia $f_n \in E[t]$ definito come $f_n(t) = t^2 - z^n$. Sia $E_n \subset F$ il campo di spezzamento di f_n su E.

i) Per quali n, m si ha $E_n = E_m$?
ii) Per quali n, m i campi E_n e E_m sono isomorfi come campi (cioè non come estensioni di E ma semplicemente come campi)?

Esercizio 188. Sia $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ e sia $E = \overline{\mathbb{Q}}^{\sigma}$. Dimostrare che ogni estensione finita di E è ciclica.

Esercizio 189.

i) Determinare il gruppo di Galois del campo di spezzamento del polinomio $x^3 + 3x + 1$ su $\mathbb{Q}$;
ii) Determinare il gruppo di Galois del campo di spezzamento del polinomio $(x^3 - 3x + 1)(x^2 - 5)$.

Esercizio 190. Sia $f \in \mathbb{Q}[t]$ un polinomio irriducibile di quinto grado.

i) Dimostrare che esiste $g \in \mathbb{Q}[t]$ diverso da t e di grado minore o uguale a 4 tale che $f(t)$ divide $f(g(t))$ se e solo se il gruppo di Galois del campo di spezzamento di f è isomorfo a $\mathbb{Z}/5$.
ii) Se si elimina l'ipotesi che il grado di g sia minore o uguale a 4 o l'irriducibilità di f l'affermazione rimane vera?
iii) Esibire due polinomi f e g con le proprietà enunciate al punto i).