Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam:
Christian Skau, phone 91755

Continuation Exam in MA3202 Galoisteori

English
Thursday, Aug. 8, 2013
Time: 09.00-13.00
Permitted aids: None
Results: Aug. 25, 2013

Problem 1

a) Is $1+i$ irreducible in $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$? Give reasons.

b) Let $a = 3 + 2i$ and $b = 4 - 6i$ be two elements in $\mathbb{Z}[i]$. Find q and r in $\mathbb{Z}[i]$ such that $a = bq + r$, and $N(r) < N(b)$, where $N(x + iy) = x^2 + y^2$.

Problem 2

a) Let p be a prime and let n be a natural number. Show that there exists an irreducible polynomial $f(x)$ over $\mathbb{Z}_p$ $(= GF(p))$ of degree n, using the fact that $F^* = F \setminus \{0\}$ is a cyclic group for every finite field F.

b) Determine the number of irreducible polynomials of degree 2 over $F = GF(3^2)$.

c) Let $F = GF(5^{12})$, and let $\phi : F \to F$ be the Frobenius automorphism $\phi(x) = x^5$. Let $K = \{x \in F \mid \phi^3(x) = x\}$. Describe the Galois field K.

Problem 3

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree four with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Let $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be the splitting field of $f(x)$ over $\mathbb{Q}$. Assume that the Galois group $G = G(E|\mathbb{Q})$ is isomorphic to S_4, the symmetric group on four symbols.

a) Show that $\mathbb{Q}(\alpha_1, \alpha_2) \subsetneq \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$.

b) Show that $\mathbb{Q}(\alpha_1\alpha_2 + \alpha_3\alpha_4) \subsetneq \mathbb{Q}(\alpha_1 + \alpha_2)$ by using the Fundamental Theorem of Galois Theory.

c) Is $\mathbb{Q}(\alpha_1 + \alpha_2) = \mathbb{Q}(\alpha_1\alpha_2)$? Give reasons.

Problem 4

Let $f(x) \in F[x]$ be an irreducible polynomial of prime degree p over the field F, with $\text{char}(F) = 0$. Let $K = F(\alpha)$, where α is a root of an irreducible polynomial $g(x) \in F[x]$ of prime degree q over the field F. Assume $f(x)$ is reducible in $K[x]$. Show that $p = q$.

Problem 5

Determine the Galois group of $f(x) = x^4 - 25$ over $\mathbb{Q}$.

Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam: Christian Skau, phone 91755

Exam in MA3202 Galoisteori

English
Thursday 16. May 2013
Time: 09.00 - 13:00
Permitted aids: None

Results: 10. June 2013

Problem 1

a) Let E be the splitting field of $f(x) = x^{14} - 1$ over $\mathbf{Q}$. Show that the Galois group $G = G(E|\mathbf{Q})$ is abelian.

b) Let $\tilde{E}$ be the splitting field of $g(x) = x^7 + 1$ over $\mathbf{Q}$. Show that the Galois group $\tilde{G} = G(\tilde{E}|\mathbf{Q})$ is abelian.

Problem 2

a) List all fields K such that $\mathbf{Q} \subseteq K \subseteq \mathbf{Q}(\omega, \sqrt[3]{2})$, where $\sqrt[3]{2} \in \mathbf{R}, \omega = e^{\frac{4\pi i}{3}}$. How many of these are normal extensions of $\mathbf{Q}$? Give explanation.

b) Which of the following fields are isomorphic? Give reasons by referring to theorems.

(i) $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(i\sqrt[4]{2})$

(ii) $\mathbf{Q}(\sqrt[4]{1+\sqrt{3}})$ and $\mathbf{Q}(\sqrt[4]{1-\sqrt{3}})$

(iii) $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$.

Problem 3

a) Let α be an algebraic number over the field F such that $[F(\alpha) : F]$ is an odd number. Show that this implies that $F(\alpha^2) = F(\alpha)$.

b) Give an example to show that the converse implication is not true.
(Hint: Cyclotomic extensions.)

Problem 4

a) Show that $\mathbf{Z}[\sqrt{-10}]$ is not a euclidean domain.

b) Show that $\mathbf{Z}[\sqrt{2}]$ is a unique factorization domain.

Problem 5

a) Let $F = GF(2)(\alpha)$, where $\alpha^4 + \alpha + 1 = 0$. Determine $a, b, c, d \in GF(2)$ such that

$$\frac{1}{\alpha} = a + b\alpha + c\alpha^2 + d\alpha^3$$

b) Let $f(x)$ be an irreducible polynomial over $GF(p)$, where p is a prime. Show that $f(x)$ divides the polynomial $g(x) = x^{p^n} - x$ in $GF(p)[x]$ if and only if $deg(f(x))$ divides n.

Problem 6

Let L be a Galois extension of F such that $G(L|F)$ is abelian. Let $f(x) \in F[x]$ be the minimal polynomial of $\alpha \in L$. Show that all the roots of $f(x)$ lie in $F(\alpha)$.

Problem 7

Let $[E : F] < \infty$, where E is an extension of the field F. If $M_1(\subseteq E)$ and $M_2(\subseteq E)$ are two normal extensions of F show that M_1M_2 is a normal extension of F. (Here M_1M_2 denotes the subfield of E generated by M_1 and M_2.)

Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam: Christian Skau, phone 91755

Exam in MA3202 Galoisteori

English
Saturday 19. may 2012
Time: 09.00 - 13:00
Permitted aids: No printed or handwritten aids permitted
Results: 15. june 2012

Problem 1

a) Show that $2+i$ is irreducible in $\mathbf{Z}[i] = \{m + ni \mid m, n \in \mathbf{Z}\}$, and that 5 is reducible in $\mathbf{Z}[i]$.

b) Which of the numbers $11, 13$ and 19 are irreducible in $\mathbf{Z}[i]$? Give reasons.

Problem 2

Let $\omega \in \mathbf{C}$ be a primitive 13th root of unity, and let $E = \mathbf{Q}(\omega)$.

a) Show that E is a normal extension of $\mathbf{Q}$, and determine the cyclic Galois group $G = G(E|\mathbf{Q})$.

b) How many proper intermediate fields K, $\mathbf{Q} \underset{\neq}{\subset} K \underset{\neq}{\subset} E$, are there? Give reasons.

Problem 3

Let $f(x) = x^7 - 2 \in \mathbf{Q}[x]$, and let E be the splitting field of $f(x)$ over $\mathbf{Q}$.

a) Determine the order of the Galois group $G = G(E|\mathbf{Q})$.

b) Show that there exists a non-normal subgroup H of G.

c) Show that there exists a normal subgroup N of G such that G/N is abelian.

Problem 4

Let $E = \mathbb{Q}(\sqrt{2} - 3\sqrt{3})$.

a) Show that E is a normal extension of $\mathbb{Q}$, and determine $G = G(E|\mathbb{Q})$.

b) List all the intermediate fields $K, \mathbb{Q} \subseteq K \subseteq E$.

Problem 5

We denote by $GF(p^n)$ the finite field with p^n elements, where p is a prime.

a) Let $f(x)$ be an irreducible polynomial of degree 36 over $GF(5)$. By referring to relevant theorems show that $f(x)$ divides the polynomial

$$x^{5^{36}} - x$$

in $GF(5)[x]$, and that $f(x)$ has distinct roots.

b) Let E be the splitting field of $f(x)$ over $GF(5)$. Exhibit by a diagram the inclusion of the intermediate fields $K, GF(5) \subseteq K \subseteq E$.

Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam: Christian Skau, phone 91755

Exam in MA3202 Galoisteori

English
Friday May 27. 2011
Time: 09.00 - 13:00
Permitted aids: No printed or handwritten aids permitted

Results: Friday June 17. 2011

Problem 1

Show that $\mathbf{Z}[\sqrt{-13}]$ is not a unique factorization domain (UFD) by showing that $r = 6+\sqrt{-13}$ is a divisor of $49 = 7 \cdot 7$, but r is not a divisor of 7.

Problem 2

a) Let $N = GF(5^{30})$ be a field extension of $F = GF(5^2)$. Determine the number of intermediate fields K, i.e. fields K such that $F \subseteq K \subseteq N$.

b) Determine the number of monic irreducible polynomials of degree 2 over $F = GF(5^2)$.

Problem 3

Let $f(x) = \frac{x^8}{8!} + \frac{x^7}{7!} + \cdots + \frac{x}{1!} + 1 = \sum_{k=0}^{8} \frac{x^k}{k!} \in \mathbf{Q}[x]$. Let E be the splitting field of $f(x)$ over $\mathbf{Q}$.

One can show that the Galois groups $G(E|\mathbf{Q})$ is isomorphic to A_8, the alternating group on 8 symbols. Use this to show that $f(x)$ is irreducible over $\mathbf{Q}$.

Problem 4

Let E be the splitting field over $\mathbf{Q}$ of $f(x) = x^{13} - 2$, and let $G = G(E|\mathbf{Q})$ be the Galois group.

a) Determine the order $|G|$ of G.

b) Show that G is non-abelian.

c) Show that there exists an intermediate field $K, \mathbf{Q} \subseteq K \subseteq E$, such that K corresponds by the Galois correspondence to a normal subgroup H of G such that the order $|H|$ of H is 13.

d) Show that there exists an intermediate field N such that $[N : \mathbf{Q}] = 39$.

Problem 5

Let $\mathbf{Q}_2$ denote the subset of $\mathbf{Q}$ consisting og all rational numbers $\frac{a}{b}$ such that $a, b \in \mathbf{Z}$ and b an odd number.

a) Show that $\mathbf{Q}_2$ is a sub-integral domain of $\mathbf{Q}$, and find the units of $\mathbf{Q}_2$

b) Show that the irreducible elements in $\mathbf{Q}_2$ consist of 2 and elements associated to 2.

c) Is $\mathbf{Q}_2$ a unique factorization domain? Give reasons.

Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen: Christian Skau, telefon 91755

Eksamen i MA3202 Galoisteori

Bokmål
Fredag 21. mai 2010
Tid: 09.00 - 13:00
Hjelpemidler: Ingen

Sensur: Fredag 11. juni 2010

Oppgave 1

La ω være en primitiv n'te enhetsrot, og la F være en kropp slik at $p \nmid n$, der $p = \text{char}\,(F)$. Vis at $F(\omega)$ er rotkroppen over F til $x^n - 1 \in F[x]$, og at Galoisgruppen $G(F(\omega)|F)$ er abelsk.

Oppgave 2

La $f(x) = x^3 + 9x - 2 \in \mathbf{Q}[x]$, og la E være rotkroppen til $f(x)$ over $\mathbf{Q}$. Vis at det finnes nøyaktig tre mellomkropper K, $\mathbf{Q} \subsetneq K \subsetneq E$, slik at $\begin{array}{c} K \\ | \\ \mathbf{Q} \end{array}$ ikke er en normal utvidelse.

Oppgave 3

Ved veltemperert stemming av et piano trenger man å bestemme forholdet $\alpha = \sqrt[12]{2} \in \mathbf{R}_+$. Begrunn hvorfor α ikke kan konstrueres fra $\mathbf{Q}$ med passer og linjal.

Oppgave 4

La F være en kropp av karakteristikk 0. La $f(x) \in F[x]$ være et polynom av grad n med n distinkte røtter $\alpha_1, \alpha_2, \cdots, \alpha_n$. La

$$\beta = \alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + n\alpha_n$$

Anta at man får $n!$ forskjellige verdier dersom man permuterer $1, \cdots, n$, dvs. mengden

$$\{k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n | k_1 k_2 \cdots k_n \text{ er en permutasjon av } 12\cdots n\}$$

består av $n!$ distinkte tall.

Vis at $F(\beta)$ er rotkroppen til $f(x)$ over F. [Hint: Benytt hovedteoremet i Galoisteorien.]

Oppgave 5

a) La $E = GF(3^{12})$ være en kroppsutvidelse av $F = GF(3^4)$. Hvor mange mellomkropper finnes det mellom F og E?

b) Bestem antall irredusible moniske polynomer av grad 2 over $GF(7)$.

Oppgave 6

La $\alpha = \sqrt{5 + \sqrt{5}} \in \mathbf{R}_+$, og la $E = \mathbf{Q}(\alpha)$.

a) Vis at $\sqrt{5 - \sqrt{5}} \in E$.
(Hint: Betrakt $\frac{1}{\alpha}$.)

b) Vis at E er rotkroppen til et polynom $f(x) \in \mathbf{Q}[x]$.

c) Bestem Galoisgruppen $G = G(E|\mathbf{Q})$ (som abstrakt gruppe), ved først å bestemme ordenen til G.

Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam: Sverre O. Smalø, phone 91750

Exam in MA3202 Galoisteori

English
Monday May 18 2009
Time: 09.00 - 13:00
Permitted aids: No printed or handwritten aids permitted.

Results: Friday June 5. 2009

Problem 1

Show that $\sqrt{-5}|(a+b\sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$ if and only if $5|a$, and use this to show that $\sqrt{-5}$ is a prime in $\mathbf{Z}\sqrt{-5}$.

Problem 2

Let F be a finite field such that $\text{char}(F) = 7$. Show that every element $a \in F$ ha a unique 7th root $\sqrt[7]{a}$, i.e. $b^7 = a$, where $b = \sqrt[7]{a}$.

Problem 3

a) Let $f(x) = x^3 + 27x + 6 \in \mathbf{Q}[x]$ and let E be the splitting field of $f(x)$ over $\mathbf{Q}$. Determine $G(E|\mathbf{Q})$.

(Hint: Investigate the real roots of $f(x)$.

b) Show that there exists one and only one field K such that $\mathbf{Q} \subsetneq K \subsetneq E$ and K is a normal extension of $\mathbf{Q}$.

Problem 4

a) Let $\begin{array}{c}K\\ |\\ F\end{array}$ be a Galois extension and let L be an intermediate field $\begin{array}{c}K\\ |\\ L\\ |\\ F\end{array}$. Show that $\begin{array}{c}K\\ |\\ L\end{array}$ is a Galois extension.

b) Give an example that shows that $\begin{array}{c}L\\ |\\ F\end{array}$ does not have to be a Galois extension.

Problem 5

Let $\begin{array}{c}K\\ |\\ F\end{array}$ be a Galois extension such that $G(K|F)$ is cyclic of order n and let σ be a generator for $G(K|F)$. Assume that F contains a primitive n'th root ω of unity. Let $\alpha \in K \backslash F$, and let $(\omega, \alpha) \neq 0$ be the Lagrange resolvent defined by

$$(\omega, \alpha) = \alpha + \omega\sigma(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha)$$

a) Show that $a = \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)$ is an element in F.

b) Show that $K = F((\omega, \alpha))$.

c) Let $b = (\omega, \alpha)^n$. Show that $b \in F$ and that K is the splitting field of $x^n - b \in F[x]$ over F.

d) Give an argument why $x^n - b$ is an irreducible polynomial over F.

Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen: Professor Christian Skau
(telefon: 91755)

Eksamen i MA3202 Galoisteori

Torsdag 1. juni 2006
Tid: 09.00 - 13:00
Hjelpemidler: Ingen
Bokmål

Sensur: 22. juni 2006

Oppgave 1

La $f(x) \in F[x]$ være et irredusibelt polynom over kroppen F, der F har karakteristikk 0. La E være rotkroppen til $f(x)$ over F, og anta at Galoisgruppen $G = G(E|F)$ er abelsk.

Vis at hver rot α til $f(x)$ er et primitivt element, dvs. $E = F(\alpha)$.

Oppgave 2

Vis at den diofantiske ligningen

$$y^2 + 2 = z^4$$

ikke har noen løsninger i $\mathbb{Z}$.

[Hint: $\mathbb{Z}[\sqrt{-2}]$ er et entydig faktoriseringsområde.]

Oppgave 3

La F være en kropp av karakteristikk p, der p er et primtall. La $f(x) \in F[x]$ være et irredusibelt polynom med multiple røtter. Vis at det finnes $s \in \{1, 2, 3, \ldots\}$ og et irredusibelt og *separabelt* polynom $g(x) \in F[x]$, slik at $f(x) = g(x^{p^s})$.

Oppgave 4

a) La K være en Galoisk utvidelse av F. La $g(x) \in K[x]$ være irredusibel over K, og la $\sigma \in G(K|F)$.

   Vis at $\sigma(g(x)) \in K[x]$ er irredusibel over K.

b) La $f(x) \in F[x]$ være et (monisk) irredusibelt polynom over F av primtallsgrad p.

   Vis at dersom $f(x)$ er redusibel i $K[x]$, så vil alle røttene til $f(x)$ ligge i K.

   [F og K er som i a).]

Oppgave 5

La $f(x) = x^3 - 21x + 6 \in \mathbb{Q}[x]$, og la E være rotkroppen til $f(x)$ over $\mathbb{Q}$. Man kan vise at $E \subset \mathbb{R}$. Vis at E ikke er et radikaltårn over $\mathbb{Q}$.

Norwegian University
of Science and Technology
Department of Mathematical Sciences

Contact during til exam:
Christian Skau, Telefon: 91755

MA3202 Commutativ algebra and Galois theory

English
Friday May 14, 2004
Kl. 9-13
Permitted aids: None
Grades to be announced: Monday May 24, 2004

Problem 1

a) Prove that if D is a domain that is not a field, then $D[x]$ is not a Euclidean domain.

b) Show that 3 is irreducible, but not prime, in the integral domain $\mathbb{Z}[\sqrt{-5}]$.

Problem 2

a) Determine the Galois group of $x^3 - 7 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

b) Let E denote the splitting field of $x^3 - 7$ over $\mathbb{Q}$. How many intermediate fields $F(\mathbb{Q} \subset F \subset E)$, such that $[F : \mathbb{Q}] = 2$, are there? Give reasons.

Problem 3

Let p be a prime. Let E be the splitting field of $x^p - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

a) Prove that $G(E/\mathbb{Q})$ is abelian of order $p - 1$.

b) Let $\omega = e^{\frac{2\pi i}{31}}$. Prove that there exists a subfield F of $\mathbb{C}$ such that $[F(\omega) : F] = 5$.

Problem 4

a) Let F be a field of characteristic p, where $0 < p \neq 3$. Let α be a root of $f(x) = x^p - x + 3 \in F[x]$ that lies in F. Show that $f(x)$ has p distinct roots in F.

[HINT: Show that $\alpha + 1$ is a root.]

b) Without actually computing, find the number of monic irreducible polynomials of degree 2 over the field $\mathbb{Z}_7 = GF(7)$.

Problem 5

Prove that $\sqrt{2} + \sqrt[3]{3}$ is irrational.

[HINT: Consider $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{3})$.]