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 $\mathbf{Z}[i] = \{m+ni | m,n \in \mathbf{Z}\}$, 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 $E = \mathbf{Q}(\sqrt{2} - 3\sqrt{3})$.

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

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

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 $K, GF(5) \subseteq K \subseteq E$.

Exam MA3202: Galois Theory, May 2012

Solutions.

Problem 1

a) Assume $2+i = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[i]$. Then $N(2+i) = N(\alpha)N(\beta)$, hence $5 = N(\alpha)N(\beta)$. Hence either $N(\alpha)$ or $N(\beta)$ equal 1, and so either α or β is a unit. This shows that $2+i$ is irreducible.

Now $5 = N(2+i) = (2+i)(2-i)$, and so 5 is reducible.

b) Since $11 \neq a^2+b^2$, $19 \neq a^2+b^2$ for any $a, b \in \mathbb{Z}$, we get that 11 and 19 are irreducible in $\mathbb{Z}[i]$.

[Indeed, if for example $11 = (a+bi)(c+di)$, then $N(11) = 11^2 = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2)$, which implies that $N(a+bi) = 1$ or $N(c+di) = 1$, hence $a+bi$ or $c+di$ is a unit.]

Since $13 = 2^2+3^2$, we get that $13 = (2+3i)(2-3i)$, and so 13 is reducible.

Problem 2

a) $E = \mathbb{Q}(\omega)$ is the splitting field of $x^{13} - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$, and so E is a normal extension of $\mathbb{Q}$. The minimal polynomial of ω is

$$\frac{x^{13}-1}{x-1} = x^{12} + x^{11} + \cdots + x + 1 \in \mathbb{Q}[x],$$

and so $[E : \mathbb{Q}] = 12 = |G(E|\mathbb{Q})|$. Furthermore, $G(E|\mathbb{Q})$ is cyclic of order 12. [In fact, 2 is a primitive element (mod 13), which means that $\{2, 2^2, 2^3, \cdots, 2^{12}\} = \{1, 2, 3, \cdots, 12\} \pmod{13}$. Then $\sigma \in G(E|\mathbb{Q})$, determined by $\sigma(\omega) = \omega^2$, generates $G(E|\mathbb{Q})$.]

b) By the Fundamental Theorem of Galois Theory, the proper intermediate fields correspond to proper subgroups of a cyclic group of order 12. There are (cyclic) subgroups of order 2, 3, 4, 6, and these are the only subgroups of G. So there are 4 proper intermediate fields.

Problem 3

a) The roots of $f(x)$ are $r = \sqrt[7]{2} \in \mathbb{R}$, $\omega r, \omega^2, \dots, \omega^6 r$, where ω is a primitive 7'th root of unity, for example $\omega = e^{\frac{2\pi i}{7}}$. The minimal polynomial of ω over $\mathbb{Q}$ is $x^6 + x^5 + \dots + x + 1$, and so $[\mathbb{Q}(\omega):\mathbb{Q}] = 6$. Also, $f(x)$ is irreducible over $\mathbb{Q}$, and so $[\mathbb{Q}(r):\mathbb{Q}] = 7$. Clearly, $E = \mathbb{Q}(r, \omega)$. This implies that $6 \mid |G|$ and $7 \mid |G|$, and so $|G| \geq 6 \cdot 7 = 42$. On the other hand,

$$[\mathbb{Q}(r,\omega):\mathbb{Q}] = [\mathbb{Q}(r,\omega):\mathbb{Q}(r)][\mathbb{Q}(r):\mathbb{Q}],$$

and so $[E:\mathbb{Q}] \leq 7 \cdot 6 = 42$, and so $[E:\mathbb{Q}] = 42 = |G|$.

b) $\mathbb{Q}(r) \subseteq E$ is a non-normal extension of $\mathbb{Q}$, and so the subgroup H of G it corresponds to by the Galois correspondence must be non-normal in G.

c) $\mathbb{Q}(\omega)$ is an intermediate field between $\mathbb{Q}$ and E. Clearly $\mathbb{Q}(\omega)$ is a normal extension of $\mathbb{Q}$ (being the splitting field of $x^7 - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$). Let N be the subgroup of G that corresponds to $\mathbb{Q}(\omega)$ by the Galois correspondence. Then N is normal and $N = G(E \mid \mathbb{Q}(\omega))$.

Furthermore

$$G/N \cong G(\mathbb{Q}(\omega) \mid \mathbb{Q})$$

and since $G(\mathbb{Q}(\omega) \mid \mathbb{Q})$ is cyclic of order 6 (and hence, in particular, abelian), we have proved that G/N is abelian.

Problem 4

a) We claim that $\mathbb{Q}(\sqrt{2}-3\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$

In fact, if $\alpha = \sqrt{2}-3\sqrt{3}$, then $\alpha^2 = 29 - 6\sqrt{2}\sqrt{3}$. Multiplying this last equation by $\sqrt{2}$ we get:

$$(29-\alpha^2)\sqrt{2} - 12\sqrt{3} = 0.$$

Combining this with

$$\sqrt{2} - 3\sqrt{3} = \alpha$$

we get that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$.

Since $\mathbb{Q}(\alpha)$ clearly is contained in $\mathbb{Q}(\sqrt{2},\sqrt{3})$, we get that

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

Now
$$\begin{array}{c} \mathbb{Q}(\sqrt{2},\sqrt{3}) = E \\ | \ \dim = 2 \\ \mathbb{Q}(\sqrt{2}) \\ | \ \dim = 2 \\ \mathbb{Q} \end{array}$$
, so we get that $[E:\mathbb{Q}] = 4$.

So $|G| = 4$, and as each $\sigma \in G(E|\mathbb{Q})$ is of the form $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$, we must have that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

b) The subgroups of G are $\{e\}$, $\mathbb{Z}_2 \times \{e\}$, $\{e\} \times \mathbb{Z}_2$, $\{e, (1,1)\}$, G. These subgroups

correspond by the Galois correspondence to the intermediate fields, and these must be

$E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6}(=\sqrt{2}\sqrt{3}))$, $\mathbb{Q}$, respectively, being the fix fields under these various subgroups.

Problem 5

a) $GF(5^{36})$ is the splitting field E of $f(x)$ over $GF(5)$. Now the elements of $GF(5^{36})$ are exactly the roots of the polynomial

$$g(x) = x^{5^{36}} - x \in GF(5)[x].$$

Hence $f(x)$ and $g(x)$ have a root in common, and so $f(x) \mid g(x)$ in $GF(5)[x]$.

Now $g'(x) = -1$, and so $g(x)$ must have distinct roots. But then $f(x)$ must also have distinct roots.

b) We have that all the intermediate fields K are of the form $K = GF(5^k)$ for some k. Also, $GF(5^k) \subseteq GF(5^l)$ iff $k \mid l$. So we get the following inclusion diagram for the intermediate fields (observing that $36 = 2^2 3^2$):