Exam MA3202 : Galois Theory
June 2, 2014.

Problem 1

a) Write down the irreducible polynomials over $GF(2)(= \mathbf{Z}_2)$ of degrees two and three, respectively.

b) How many irreducible polynomials of degree four are there over $GF(2)$?

Problem 2

Let $\begin{matrix} E \\ | \\ F \end{matrix}$ where $F = GF(5^3)$, $E = GF(5^{24})$. Describe the Galois group $G(E|F)$, and list the fields K such that $F \subseteq K \subseteq E$.

Problem 3

Let $f(x) \in F[x]$ be a non-zero polynomial over the field F with various properties as described below. Let $\alpha \in \overline{F}$, where $\overline{F}$ denotes the algebraic closure of F.

a) Let $f(\alpha) = 0$. Assume that whenever $g(\alpha) = 0$ for some non-zero $g(x) \in F[x]$, then degree $(f(x)) \leq$ degree $(g(x))$. Show that $f(x)$ is irreducible over F.

b) Show the converse of a), that is: Assume $f(x)$ is irreducible over F and $f(\alpha) = 0$. Let $g(\alpha) = 0$ for some non-zero $g(x) \in F[x]$. Show that degree $(f(x)) \leq$ degree $(g(x))$.

Problem 4

a) Let $\begin{matrix} F(\theta) \\ | \\ F \end{matrix}$ and $\begin{matrix} F(\gamma) \\ | \\ F \end{matrix}$ be two Galois extensions of the field F, where char $(F) = 0$. Show that $\begin{matrix} F(\theta,\gamma) \\ | \\ F \end{matrix}$ is a Galois extension of F.

b) Assume $G(F(\theta)|F)$ and $G(F(\gamma)|F)$ are both abelian groups. Show that $G(F(\theta,\gamma)|F)$ is an abelian group.

Problem 5

a) Let $\alpha = \sqrt{2+\sqrt{2}} \in \mathbf{R}_+$. Find the minimal polynomial of α over $\mathbf{Q}$.

b) Show that $\mathbf{Q}(\alpha)$ is a normal extension of $\mathbf{Q}$.

(Hint: Consider $\alpha\sqrt{2-\sqrt{2}}$.)

c) Determine $G(\mathbf{Q}(\alpha)|\mathbf{Q})$ and all the intermediate fields K, where $\mathbf{Q} \subsetneq K \subsetneq \mathbf{Q}(\alpha)$.

(Hint: Consider $\sigma \in G(\mathbf{Q}(\alpha)|\mathbf{Q})$ such that $\sigma(\alpha) = \sqrt{2-\sqrt{2}}$.)

Problem 6

a) Let $R = \mathbf{Z}[2i] = \{a+2bi|a,b \in \mathbf{Z}\}$. So R is a subintegral domain of the Gaussian integers $\mathbf{Z}[i] = \{a+bi|a,b \in \mathbf{Z}\}$. Show that 2 and $2i$ are irreducibles in R.

b) Show that R is not a UFD.

Problem 7

Show that $\sqrt{2} + \sqrt[3]{3} \notin \mathbf{Q}$.

(Hint: Consider an appropriate field extension of $\mathbf{Q}$.)

MA3202 : Galois Theory

Exam June 2, 2014: Solutions

Problem 1 a)

Degree 2 : x^2+x+1

Degree 3 : x^3+x^2+1, x^3+x+1

} These are the only polynomials with no roots in GF(2).

b) The number of irreducible polynomials of degree four over GF(2) is $16-13=3$

[Counting argument: The number of polynomials of degree four is $2^4=16$. The number of reducible polynomials of degree four is

$$2+2+1+2+2+3+1=13$$

(Respectively, the number of polynomials with roots 0 and 1, each of multiplicity four; with roots 0 and 1, one of them of multiplicity three; with roots 0 and 1, both of multiplicity two; with factor x^3+x^2+1; with factor x^3+x+1; with exactly one factor x^2+x+1; with factor x^2+x+1 of multiplicity two.)

Problem 2

$G(E|F)$ is cyclic of degree $[GF(5^{24}):GF(5^3)]=8$, the generator being $\psi: E\to E$ defined by $\psi(a)=a^{5^3}$. The intermediate fields are:

$$F=GF(5^3) \subsetneq GF(5^6) \subsetneq GF(5^{12}) \subsetneq GF(5^{24})=E$$

Problem 3 a)

Assume $f(x)$ is reducible, and let $f(x) = a(x)b(x)$, where $a(x), b(x) \in F[x]$, $1 \leq \text{degree}(a(x)) < \text{degree}(f(x))$, $1 \leq \text{degree}(b(x)) < \text{degree}(f(x))$. Since $f(\alpha) = 0$ we must have either $a(\alpha) = 0$ or $b(\alpha) = 0$. This contradicts the assumption, and so $f(x)$ is irreducible.

b) Assume $\text{degree}(g(x)) < \text{degree}(f(x))$. Then the greatest common divisor of $f(x)$ and $g(x)$ must be 1 (since $f(x)$ is irreducible). Since $F[x]$ is a Euclidean domain, and hence a PID, there exist $a(x), b(x) \in F[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1.$$

Since $f(\alpha) = g(\alpha) = 0$, we get a contradiction. Hence we must have $\text{degree}(f(x)) \leq \text{degree}(g(x))$.

(Actually, one can prove that $f(x)$ divides $g(x)$, which obviously will imply that $\text{degree}(f(x)) \leq \text{degree}(g(x))$.)

Problem 4 a)

$F(\theta)$ is the splitting field of some $f(x) \in F[x]$ over F, and $F(\gamma)$ is the splitting field of some $g(x) \in F[x]$ over F. Then clearly $F(\theta, \gamma)$ is the splitting field of $h(x) = f(x)g(x) \in F[x]$ over F. This proves that $F(\theta, \gamma)$ is a Galois extension of F.

b) An element $\sigma \in G(F(\theta,\gamma)|F)$ is uniquely determined by $\sigma(\theta)$ and $\sigma(\gamma)$. By our assumptions we get that $\sigma|_{F(\theta)} \in G(F(\theta)|F)$, $\sigma|_{F(\gamma)} \in G(F(\gamma)|F)$.
Now let $\tau, \sigma \in G(F(\theta,\gamma)|F)$. Then by our assumptions we get
$\tau\circ\sigma(\theta) = \sigma\circ\tau(\theta)$, $\tau\circ\sigma(\gamma) = \sigma\circ\tau(\gamma)$.
This implies that $\tau\circ\sigma = \sigma\circ\tau$, and so $G(F(\theta,\gamma)|F)$ is abelian.

Problem 5 a)

$\alpha^2 = 2 + \sqrt{2} \Rightarrow \sqrt{2} = \alpha^2 - 2$. Squaring we get:

$2 = \alpha^4 - 4\alpha^2 + 4$, and so $f(\alpha) = 0$, where

$f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. By Eisenstein's criterion ($p = 2$) we get that $f(x)$ is irreducible over $\mathbb{Q}$, and so is the minimal polynomial of α over $\mathbb{Q}$

b) The roots of $f(x)$ are

$$x = \pm\sqrt{2 \pm \sqrt{2}}.$$

Clearly $\sqrt{2} \in \mathbb{Q}(\alpha)$, since $\sqrt{2} = \alpha^2 - 2$.

$$\alpha\sqrt{2-\sqrt{2}} = \sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{2}.$$

This shows that $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\alpha)$, and so all roots of $f(x)$ lie in $\mathbb{Q}(\alpha)$. This proves that $\mathbb{Q}(\alpha)$ is a normal (and hence Galois) extension of $\mathbb{Q}$.

c) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, and so $|G(\mathbb{Q}(\alpha)/\mathbb{Q})| = 4$. There are exactly two groups of

order 4, namely the cyclic group of order 4, or Klein's vier-group $\mathbb{Z}_2 \times \mathbb{Z}_2$. We will show that $G = G(\mathbb{Q}(\alpha) \mid \mathbb{Q})$ is cyclic. (This will imply by the Galois correspondence that there is only one K, $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}(\alpha)$, namely $K = \mathbb{Q}(\sqrt{2})$.)

Let $\sigma \in G$ such that $\sigma(\alpha) = \sqrt{2-\sqrt{2}}$. Then $2 - \sqrt{2} = \sigma(\alpha^2) = \sigma(2+\sqrt{2})$, and so $\sigma(\sqrt{2}) = -\sqrt{2}$. Now

(*) $\alpha\,\sigma(\alpha) = \sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{2}$. Apply σ on both sides:

$\sigma(\alpha)\,\sigma^2(\alpha) = \sigma(\sqrt{2}) = -\sqrt{2}$. This, together with (*) implies that $\sigma^2(\alpha) \neq \alpha$, and so G can not be Klein vier-group. Hence G is cyclic.

Problem 6 a)

The units of R are ± 1. Hence 2 and $2i$ are not conjugates. Assume $2i = \alpha\beta$ (resp. $2 = \alpha\beta$), where $\alpha = a + 2bi$, $\beta = c + 2di$ lie in R. Taking norms on both sides we get:

$4 = (a^2 + 4b^2)(c^2 + 4d^2)$. It follows easily from this that either α or β is a unit, hence 2 and $2i$ are irreducibles.

b) $4 = 2 \cdot 2 = (-2i)(2i)$ shows that R is not a UFD.

Problem 7

Assume $\sqrt{2} + \sqrt[3]{3} \in \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt[3]{3})$. Now $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$, which is a contradiction, and so $\sqrt{2} + \sqrt[3]{3} \notin \mathbb{Q}$.