Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 9 - Tuesday November 22, 2011. Due Wednesday November 30

Exercise 57: Let K be a finite field. Show that every $k \in K$ can be written as $k = a^2 + b^2$ for some $a, b \in K$.

Exercise 58: Let E be a field, and let $F = E(x)$. Let $P, Q \in E[x]$ with P, Q relatively prime.

i) Show that x is algebraic over $E\big(\frac{P}{Q}\big)$, and $\big[F : E\big(\frac{P}{Q}\big)\big] = \max\{degree(P), degree(Q)\}$.

ii) $x \mapsto \frac{P}{Q}$ induces a ring-homomorphism σ from $F = E(x)$ into itself: if $\varphi, \psi \in E[x]$, then $\sigma(\varphi) = \varphi\big(\frac{P}{Q}\big)$, and $\sigma\big(\frac{\varphi}{\psi}\big) = \frac{\sigma(\varphi)}{\sigma(\psi)}$. Show that σ is an automorphism of F if and only if $\max\{degree(P), degree(Q) = 1$, and that $Aut_E(F)$ consists of all those automorphisms induced by $x \mapsto \frac{a\,x+b}{c\,x+d}$ with $a, b, c, d \in E$ and $a\,d - b\,c \neq 0$.

iii) Show that if K is an intermediate field (between E and F) with $K \neq E$, one has $[F : K] < \infty$. Deduce that if E is infinite, then the fixed field of $Aut_E(F)$ is equal to E.

Exercise 59: Show that $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$, but that it is reducible in $\mathbb{Z}_p[x]$ for all prime p, and more precisely that

i) $x^4 + 1$ has a root (in $\mathbb{Z}_p$) if and only if either $p = 2$ or p has the form $8n + 1$,

ii) excluding the case i) $x^4 + 1$ factors as $(x^2 + b)\,(x^2 - b)$ (for some $b \in \mathbb{Z}_p$) if and only if p has the form $8n + 5$,

iii) excluding the case i) $x^4 + 1$ factors as $(x^2 + a\,x + 1)\,(x^2 - a\,x + 1)$ (for some $a \in \mathbb{Z}_p$) if and only if p has the form $8n + 7$,

iv) excluding the case i) $x^4 + 1$ factors as $(x^2 + a\,x - 1)\,(x^2 - a\,x - 1)$ (for some $a \in \mathbb{Z}_p$) if and only if p has the form $8n + 3$.

[Besides recalling that -1 is a quadratic residue for an odd prime q if and only if q has the form $4n + 1$, it is useful to know that 2 is a quadratic residue for an odd prime q if and only if q has the form $8n \pm 1$.]

Exercise 60: (Putnam 1971-A2): Determine all polynomials $P(x)$ such that $P(x^2 + 1) = \big(P(x)\big)^2 + 1$ and $P(0) = 0$.

[Implicitly, the above Putnam problem assumed that one works on $\mathbb{R}$, but here the question is

i) for any field E of characteristic 0, show that the only $P \in E[x]$ satisfying $P(x^2 + 1) = \big(P(x)\big)^2 + 1$ and $P(0) = 0$ is the "trivial solution" $P = x$.

ii) for any field E of characteristic p, show that there are infinitely many solutions $P \in E[x]$.]

Exercise 61: (Putnam 1972-B4) Let n be an integer greater than 1. Show that there exists a polynomial $P(x, y, z)$ with integral coefficients such that $x \equiv P(x^n, x^{n+1}, x + x^{n+2})$.

Exercise 62: (Putnam 1975-A4): Let $n = 2m$, where m is an odd integer greater than 1. Let $\theta = e^{2\pi\, i/n}$. Express $(1 - \theta)^{-1}$ explicitly as a polynomial in θ,

$$a_k\theta^k + a_{k-1}\theta^{k-1} + \ldots + a_1\theta + a_0,$$

with *integer* coefficients a_i.

[Note that θ is a primitive n-th root of unity, and thus it satisfies all of the identities which hold for such roots.]

Exercise 63: (Putnam 1985-B6): Let G be a finite set of real $n \times n$ matrices $\{M_i\}$, $1 \leq i \leq r$, which form a group under matrix multiplication. Suppose that $\sum_{i=1}^r \mathrm{tr}(M_i) = 0$, where $tr(A)$ denotes the trace of the matrix A. Prove that $\sum_{i=1}^r M_i$ is the $n \times n$ zero matrix.

[Consider the above Putnam problem by replacing $\mathbb{R}$ by a field E (i.e. the matrices have entries in E), and prove the same conclusion if E has characteristic 0, and if E has characteristic p with p satisfying the two conditions $p > r$ and $p > n$.]