21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 1 - Wednesday September 7, 2011. Due Monday September 12

Exercise 1: Let G be a group such that $g^2 = e$ for all $g \in G$. Show that G is Abelian.

Exercise 2: i) Let G be a group of order $2n$. Show that G contains an odd number of elements of order 2.
ii) Assume that n is odd. Show that if G is Abelian there is exactly one element of order 2, but that it is not always true if G is non-Abelian.

Exercise 3: i) Show that a group G cannot be the union of two proper subgroups.
ii) Give an example of a group G which is the union of three proper subgroups.

Exercise 4: Show that a group which only has a finite number of subgroups must be finite.

Exercise 5: i) Let G be an Abelian group containing elements a and b of orders m and n respectively. Show that G contains an element whose order is the least common multiple of m and n (one may start by the case where $(m, n) = 1$).
ii) Is it true if G is not Abelian?

Exercise 6: i) Show that in an Abelian group G, the set H of all elements of G with finite order is a subgroup of G.
ii) In the group $G = GL(2; \mathbb{Q})$ (the multiplicative group of non-singular 2×2 matrices with rational entries), compute the orders of $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, and $A\,B$.
iii) Find in $\mathbb{Z}_2 \times \mathbb{Z}$ two elements a, b of infinite order such that $a + b$ has order 2.

Exercise 7: If G is the multiplicative group of odd integers modulo 2^{k+2}, and $k \geq 1$, show that G is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_2$ with $m = 2^k$.

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

Assignment 2 - Friday September 16, 2011. Due Wednesday September 21

Exercise 8: If G is a group (not necessarily finite), show that every subgroup H of index $[G\!:\!H] = 2$ is a normal subgroup.

Is it true if H has index 3?

Exercise 9: If G is a group and H, K are two subgroups of G, show that $H\,K$ is a subgroup of G if and only if $H\,K = K\,H$.

Exercise 10: (Putnam 1968-B2) If A is a subset of a finite group G, and A contains more than one half of the elements of G, show that each element of G is the product of two elements of A.

Exercise 11: (Putnam 1969-B1) Let n be a positive integer such that $n = 23 \pmod{24}$. Show that the sum of all the divisors of n is divisible by 24.

Exercise 12: (Putnam 1972-A5) Show that if n is an integer ≥ 2, then n does not divide $2^n - 1$.

Exercise 13: (Putnam 1972-B3) Let a and b be two elements in a group such that $a\,b\,a = b\,a^2\,b$, $a^3 = e$ and $b^{2n-1} = e$ for some positive integer n. Show that $b = e$.

Exercise 14: (Putnam 1976-B2) Suppose that G is a group generated by two elements a and b, and that $a^4 = b^7 = a\,b\,a^{-1}b = e$, with $a^2 \neq e$ and $b \neq e$.

i) How many element of G are of the form c^2 with c in G?

ii) Write each such square as $a^m b^n$ for some $m, n \in \mathbb{Z}$.

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

Assignment 3 - Saturday September 24, 2011. Due Friday September 30

Exercise 15: Prove that D_{12} and S_4 are not isomorphic.

Exercise 16: Write the cycle decompositions of all the elements of order 4 in S_4, and of all the elements of order 2 in S_4.

Exercise 17: Let σ the 8-cycle $(1\,2\,3\,4\,5\,6\,7\,8)$, τ the 12-cycle $(1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12)$, and ω the 14-cycle $(1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14)$. For which positive integer i is σ^i an 8-cycle? For which positive integer j is τ^j a 12-cycle? For which positive integer k is ω^k a 14-cycle?

Exercise 18: Show that in the three following cases, the centralizer of H is H, and the normalizer of H is G:

i) $G = S_3$ and $H = \{e, (123), (132)\}$,
ii) $G = D_4$ and $H = \{e, a^2, b, a^2 b\}$,
iii) $G = D_5$ and $H = \{e, a, a^2, a^3, a^4\}$.

[In a group G, for any subset $X \subset G$, the centralizer of X is $C_G(X) = \bigcap_{x\in X} C_G(x)$ (where the centralizer $C_G(x)$ is the stabilizer of x for the action of conjugation, i.e. $\{g \in G \mid g\,x = x\,g\}$). In D_n, a denotes an element of order n and b an element of order 2, satisfying $b\,a = a^{-1}b$.]

Exercise 19: For $m \geq 1$ and $q_1, \ldots, q_m \in \mathbb{Q}^*$, prove that the (finitely generated) subgroup $H = \langle q_1, \ldots, q_m\rangle$ of $\mathbb{Q}$ is a subgroup of $K = \left\langle \frac{1}{D}\right\rangle$, where D is the least common multiplier of the denominators of $q_1, \ldots, q_m$. Show that H is cyclic (hence $\mathbb{Q}$ is not finitely generated).

Exercise 20: A non trivial Abelian group G is called *divisible* if for each $a \in G$ and each positive integer k there exists $b \in G$ with $k\,b = a$. Show that $\mathbb{Q}$ is divisible, that no finite Abelian group is divisible, and that $G_1 \times G_2$ is divisible if and only if both G_1 and G_2 are divisible.

Exercise 21: Show that the group of rigid motion symmetries of a platonic solid (tetrahedron, cube, octahedron, dodecahedron, icosahedron) have respectively orders 12, 24, 24, 60, 60, i.e. $2E$, where E is the number of edges. Show that for the tetrahedron this group is isomorphic to a subgroup of S_4, and that for the cube or the octahedron this group is isomorphic to S_4.
[A Platonic solid is a convex polyhedron which is regular, so that its faces all are regular polygons with k sides, and ℓ edges arrive at each vertex, so that the number of faces F, of edges E, and of vertices V satisfy $k\,F = \ell\,V = 2E$; using $k, \ell \geq 3$ (which implies $k, \ell \leq 5$) and the relation $F - E + V = 2$ (that the Euler characteristic of the sphere $\mathbb{S}^2$ is 2), one finds there are five such regular polyhedron: the tetrahedron (4 triangular faces), the hexahedron = cube (6 square faces), the octahedron (8 triangular faces), the dodecahedron (12 pentagonal faces), and the icosahedron (20 triangular faces).]

21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 4 - Saturday October 1, 2011. Due Friday October 7

Exercise 22: Let p be a prime, and for $n \geq 1$ let $E_{p^n} = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (with n factors). How many subgroups of order p are there in E_{p^n}?

Exercise 23: For a group G, the *exponent of* G is the smallest positive integer n such that $g^n = e$ for all $g \in G$, and the exponent is ∞ if no such n exists.

Show that every finite group has a finite exponent n, without necessarily having an element of order n.

Give an example of an infinite group having a finite exponent.

Exercise 24: For a group G (written multiplicatively) and p a prime, one writes $G^p = \{g^p \mid g \in G\}$ and $G_p = \{x \in G \mid x^p = e\}$.

Show that G^p and G_p are subgroups of G.

If for groups H, K one has $G = H \times K$, show that $G^p = H^p \times K^p$ and $G_p = H_p \times K_p$.

Exercise 25: Notation of Exercice 24.

If $G = \mathbb{Z}_n$, what are G^p and G_p?

Show that for any finite Abelian group G, one has $G/G^p \simeq G_p$, and that the number of subgroups of G of order p is equal to the number of subgroups of G of index p.

Exercise 26: In S_5 one considers the 5-cycle $a = (1\,2\,3\,4\,5)$ and the 4-cycle $b = (1\,2\,4\,3)$. Show that $b\,a = a^2 b$, and that the group $\langle a, b\rangle$ generated by a and b has order 20, with elements $a^\alpha b^\beta$ with $0 \leq \alpha \leq 4, 0 \leq \beta \leq 3$, and that $(a^\alpha b^\beta)\,(a^\gamma b^\delta) = a^\epsilon b^\zeta$, where $\epsilon = \alpha + 2^\beta \gamma \pmod 5$ and $\zeta = \beta + \delta \pmod 4$.

Exercise 27: Let $p < q < r$ be primes.

Show that no group G of order $p\,q\,r$ is simple.

Show that no group G of order $p^2 q$ is simple.

Exercise 28: Show that a simple group G of order 90 must contain 60 elements of order 9. Deduce that no such simple group exists.

21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 5 - Saturday October 8, 2011. Due Friday October 14

Exercise 29: Let G be any *simple* group of order 168; let n_p be the number of Sylow p-subgroups of G (for $p = 2, 3, 7$).

a) Show that $n_2 \in \{7, 21\}$, $n_3 \in \{7, 28\}$, and $n_7 = 8$.

b) If H is a Sylow-7 subgroup of G, show that its normalizer $N = N_G(H)$ contains seven subgroups of order 3, and that $n_3 = 28$.

Exercise 30: Notation of Exercise 29.

For K a Sylow-2 subgroup of G, let $P = N_G(P)$ be its normalizer. Find how many Sylow-3 subgroups P has, and show that $n_2 = 21$, and $P = K$.

Exercise 31: Show that a ring R, not necessarily unital, which satisfies $r^2 = r$ for all $r \in R$ is necessarily commutative.

Exercise 32: An element r of a ring R is said to be nilpotent if $r^n = 0$ for some $n \geq 1$.

i) If R is a *commutative* ring, show that if a and b are nilpotent then $a + b$ is nilpotent. Show that this result may be false if R is not commutative.

ii) If R is a *commutative* ring, show that if a is nilpotent and $r \in R$ then $a\,r$ is nilpotent. Show that this result may be false if R is not commutative.

Exercise 33: Show that the subset J of $\mathbb{Z}[x]$ of all polynomials $a_0 + a_1 x + \ldots$ (with integer coefficients) such that $a_0 = 0 \pmod 6$ and $a_1 = 0 \pmod 3$ is an ideal, and deduce that $\mathbb{Z}[x]$ is not a Principal Ideal Domain.

Exercise 34: Let R be a (non necessarily commutative) ring and for $n \geq 1$ let $\mathcal{M}_n(R)$ be the ring of $n \times n$ matrices with entries in R. Let $\mathcal{J}$ be a two-sided ideal of $\mathcal{M}_n(R)$, and let J be the subset of elements of R which appear as the entry in row 1 – column 1 of some matrix belonging to $\mathcal{J}$; show that J is a two-sided ideal of R and that $\mathcal{J}$ is the set of all $n \times n$ matrices with entries in J.

Exercise 35: For J an ideal in a *commutative* ring R, one defines $Rad(J) = \{r \in R \mid r^n \in J \text{ for some } n \geq 1\}$.

i) Show that $Rad(J)$ is an ideal, and that $Rad\big(Rad(J)\big) = Rad(J)$.

ii) If $J_1, \ldots, J_m$ are ideals of R (and $m \geq 2$), show that $Rad(J_1 \cdots J_m) = Rad(\cap_{i=1}^m J_i) = \cap_{i=1}^m Rad(J_i)$, where $J_1 \cdots J_m$ denotes the ideal generated by products of the form $a_1 \cdots a_m$ with $a_i \in J_i$ for $i = 1, \ldots, m$, i.e. finite sums of such products.

21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 6 - Saturday October 15, 2011. Due Monday October 24

Exercise 36: Let R be an integral domain equipped with a function V from $R \setminus \{0\}$ into $\mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = b\,q + r$ and either $r = 0$ or $r \neq 0$ and $V(r) < V(b)$. For a non-zero $x \in R$, one defines $W(x) = \min\{V(x\,y) \mid y \in R, y \neq 0\}$. Show that $W(\xi\,\eta) \geq W(\xi)$ for all non-zero $\xi, \eta \in R$, and that for all $a, b \in R$ with $b \neq 0$ there exist $q_*, r_* \in R$ such that $a = b\,q_* + r_*$ and either $r_* = 0$ or $r_* \neq 0$ and $W(r_*) < W(b)$.

Exercise 37: Let R be a commutative unital ring.
i) Show that if $a_1, \ldots, a_n \in R$ are nilpotent, then $a_1x + \ldots + a_nx^n$ is nilpotent in $R[x]$, and $1 + a_1x + \ldots + a_nx^n$ is a unit in $R[x]$ (i.e. it has an inverse in $R[x]$).
ii) Show that $a_0 + a_1x + \ldots + a_nx^n$ is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent.

Exercise 38: Let $P(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ with $a_n \neq 0$. Suppose that for some prime p and some k such that $0 < k < n$ one has p divides a_i for $i = 0, \ldots, k-1$, but p divides neither a_k nor a_n, and p^2 does not divide a_0. Show that P has a factor Q of degree at least k which is irreducible in $\mathbb{Z}[x]$ (the excluded case $k = n$ corresponds to Eisenstein's criterion).

Exercise 39: i) Show that all the integer solutions of $x^3 = y^2 + 2$ have x and y odd.
ii) $\mathbb{Z}[\sqrt{-2}] = \{a + i\sqrt{2}\,b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a Unique Factorization Domain, so that every element which is not a unit (here ± 1) has a factorization as a product of irreducible elements, unique up to reordering the factors or replacing them by associates. Deduce that any integer solution of $x^3 = y^2 + 2$ satisfies $y \pm \sqrt{-2} = (a \pm b\sqrt{-2})^3$ for some $a, b \in \mathbb{Z}$.
iii) Find all the integer solutions of $x^3 = y^2 + 2$.

Exercise 40: One says that an ideal P in a ring R is prime if $P \neq R$ and if for any two ideals A, B of R satisfying $A\,B \subset P$ one has $A \subset P$ or $B \subset P$ (recall that $A\,B$ is the set of finite sums of terms like $a\,b$ with $a \in A$ and $b \in B$). Let R be a unital ring (not necessarily commutative).
i) Show that if P is a prime ideal and A is an ideal such that $A^n \subset P$ for some $n \geq 1$, then one has $A \subset P$ (recall that A^n is the set of finite sums of terms like $a_1 \cdots a_n$ with $a_i \in A$ for $i = 1, \ldots, n$).
ii) Show that if P is a prime ideal and $r, s \in R$ are such that $r\,R\,s \subset P$, then $(r)\,(s) \subset P$, so that $r \in P$ or $s \in P$.

Exercise 41: i) Show that if J is a prime ideal in a commutative ring R, then $Rad(J) = J$.
ii) In the case $R = \mathbb{Z}$, show that every ideal J is such that $Rad(J)$ is the intersection of all the prime ideals containing J.

Exercise 42: For a ring R, the ring of formal power series $R[[x]]$ is made of the sequences $(a_0, a_1, \ldots)$ interpreted as $A = a_0 + a_1x + \ldots$ with the natural operations: if $B = b_0 + b_1x + \ldots$, then $A + B = C$ and $A\,B = D$ have coefficients $c_k = a_k + b_k$, $d_k = \sum_{j=0}^{k} a_jb_{k-j}$ for $k = 0, \ldots$. If R is an integral domain, then $R[[x]]$ is an integral domain, hence it has a field of fractions. Find necessary conditions for an element $q_0 + q_1x + \ldots \in \mathbb{Q}[[x]]$ to be equal to $\frac{A}{B}$ for $A, B \in \mathbb{Z}[[x]]$ with $B \neq 0$, and deduce that the field of fractions of $\mathbb{Z}[[x]]$ is strictly smaller than the field of fractions of $\mathbb{Q}[[x]]$.

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

Assignment 7 - Sunday November 6, 2011. Due Friday November 11

Exercise 43: i) Prove that the ring $2\mathbb{Z}$ and the ring $3\mathbb{Z}$ are not isomorphic.
ii) Prove that the ring $\mathbb{Z}[x]$ and the ring $\mathbb{Q}[x]$ are not isomorphic.

Exercise 44: Decide which of the following are ideals of the ring $\mathbb{Z}[x]$:
i) the set of all polynomials whose constant term is a multiple of 3,
ii) the set of all polynomials whose coefficient of x^2 is a multiple of 3,
iii) the set of all polynomials whose constant term, coefficient of x, and coefficient of x^2 are zero,
iv) the set of all polynomials in which only even powers of x appear (i.e. $\mathbb{Z}[x^2]$),
v) the set of all polynomials whose sum of all coefficients is zero,
vi) the set of all polynomials whose sum of all coefficients of even powers of x is zero, and whose sum of all coefficients of odd powers of x is zero,
vii) the set of all polynomials P such that $P'(0) = 0$.

Exercise 45: Let R be a commutative unital ring, and let $P_1, \ldots, P_n$ be prime ideals.
i) Suppose that A is an ideal such that for $i = 1, \ldots, n$ there exists $a_i \in A \cap P_i$ such that $a_i \notin P_j$ for all $j \neq i$, and let $b = a_1 + (a_2 \cdots a_n)$; show that $b \in A$ but $b \notin P_1 \cup \cdots \cup P_n$.
ii) Show that if an ideal B is such that $B \subset P_1 \cup \cdots \cup P_n$, then $B \subset P_i$ for some $i \in \{1, \ldots, n\}$.

Exercise 46: Let R be a ring with at least one non-zero element, and such that for each non-zero $a \in R$ there is a *unique* $b \in R$ satisfying $a\,b\,a = a$, which one writes $b = \psi(a)$.
i) Show that multiplication is regular (i.e. for each non-zero $r \in R$, $r\,x = r\,y$ implies $x = y$ and $x\,r = y\,r$ implies $x = y$).
ii) Show that $a\,b\,a = a$ implies $b\,a\,b = b$, i.e. if $b = \psi(a)$, then $a = \psi(b)$.
iii) Show that there is an identity for multiplication, and that R is a division ring.

Exercise 47: Let p be an odd prime, and let $R \subset \mathbb{Q}$ be the set of rational numbers whose denominator in reduced form (i.e. $\frac{a}{b}$ with $b \in \mathbb{Z}^*$ and $a \in \mathbb{Z}$ satisfying $(a, b) = 1$) is not divisible by p, and let $J \subset R$ be the set of such rational numbers whose numerator in reduced form is a multiple of p.
i) Show that R is a subring of $\mathbb{Q}$ and J is an ideal of R.
ii) If $\frac{a}{b}, \frac{c}{d} \in R$ (so that $b, d \neq 0 \pmod{p}$), one writes that $\frac{a}{b} = \frac{c}{d} \pmod{p}$ if $\frac{a}{b} - \frac{c}{d} \in J$. Show that $1 + \frac{1}{2} + \ldots + \frac{1}{p-1} = 0 \pmod{p}$.

Exercise 48: (Putnam 1996-A5) If p is a prime greater than 3, and $k = \lfloor 2p/3 \rfloor$, prove that the sum

$$\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$$

of binomial coefficients is divisible by p^2.
(For example $\binom{7}{1} + \binom{7}{2} + \binom{7}{3} + \binom{7}{4} = 7 + 21 + 35 + 35 = 2.7^2$.)

Exercise 49: One considers the ring of Gaussian integers, $\mathbb{Z}[i] = \{z = a + i\,b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, with $V(z) = z\,\overline{z} = a^2 + b^2$.
i) If x_0 is a positive integer and $y_0 = a + b\,i \in \mathbb{Z}[i]$, show that there exists $q, r \in \mathbb{Z}[i]$ with $y_0 = q\,x_0 + r$ with either $r = 0$ or $r \neq 0$ and $V(r) \leq \frac{V(x_0)}{2}$.
ii) If $x \in \mathbb{Z}[i]$ with $x \neq 0$ and $y \in \mathbb{Z}[i]$, show by considering $x_0 = x\,\overline{x}$ that $y = q\,x + r$ with either $r = 0$ or $V(r) \leq \frac{V(x)}{2}$, so that $\mathbb{Z}[i]$ is an Euclidean domain.
iii) Show that $Z[\sqrt{-2}] = \{z = a + i\,\sqrt{2}\,b \mid a, b \in \mathbb{Z}\}$ with $V(z) = z\,\overline{z} = a^2 + 2b^2$, is an Euclidean domain.

21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 8 - Monday November 14, 2011. Due Monday November 21

Exercise 50: For a field E, show that every element of $E(x_1,\ldots,x_n)$ which is not in E is transcendental over E.

Exercise 51: Let E be a field, and F a field extension of E. Assume that $a,b\in F$ are algebraic over E, of degrees m and n respectively, with $(m,n)=1$. Show that $[E(a,b)\,{:}\,E]=m\,n$.

Exercise 52: Let E be a field, and F a field extension of E.

i) Show that if $u\in F$ is algebraic over E then u^2 is algebraic over E.

ii) Show that if $v\in F$ is algebraic of odd degree over E, then the same is true of v^2 and one has $E(v^2)=E(v)$.

iii) If $w\in F$ is algebraic of even degree over E, can one have $E(w^2)=E(w)$?

Exercise 53: Let E be a field, and F a field extension of E. Assume that $u,v\in F$ are such that v is algebraic over $E(u)$, and that v is transcendental over E. Show that u is algebraic over $E(v)$.

Exercise 54: Let E be a field and let $F=E(x)$. Let $u=\frac{x^3}{x+1}\in F$ and let $K=E(u)$ (which is an intermediate field between E and F). Show that there exists $v\in F$ such that $F=K(v)$, and compute $[F\,{:}\,K]$.

Exercise 55: Let E be a field, and F a field extension of E. Let K_1,K_2 be two intermediate fields between E and F. One defines the composite field K_1K_2 as the smallest subfield of F containing $K_1\cup K_2$.

i) Show that $[K_1K_2\,{:}\,E]$ is finite if and only if $[K_1\,{:}\,E]$ and $[K_2\,{:}\,E]$ are finite.

ii) If $[K_1K_2\,{:}\,E]$ is finite, show that $[K_1\,{:}\,E]$ and $[K_2\,{:}\,E]$ divide $[K_1K_2\,{:}\,E]$, and that $[K_1K_2\,{:}\,E]\le[K_1\,{:}\,E]\,[K_2\,{:}\,E]$, with equality in the case where $[K_1\,{:}\,E]$ and $[K_2\,{:}\,E]$ are relatively prime.

iii) Show that if K_1 and K_2 are algebraic over E, then K_1K_2 is algebraic over E.

Exercise 56: Let E be a field, $P\in E[x]$ of degree $n\ge 1$ and let F be a splitting field extension for P over E. Show that $[F\,{:}\,E]$ divides $n!$.

21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
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 $p > n$.]

21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 10 - Wednesday November 30, 2011. Due Monday December 5

Exercise 64: Show that the polynomial $P = -1 + (x-1)\,(x-2)\cdots(x-n)$ is irreducible in $\mathbb{Z}[x]$ for all $n \geq 1$.

Exercise 65: For $n \geq 2$, show that $P = 1 + x + \ldots + x^{n-1}$ is irreducible in $\mathbb{Z}[x]$ if and only if n is prime.

Exercise 66: Determine the splitting field extensions $F \subset \mathbb{C}$ for P_j over $\mathbb{Q}$ and compute $[F\!:\!\mathbb{Q}]$ for

i) $P_1 = x^4 - 2$,
ii) $P_2 = x^4 + 2$,
iii) $P_3 = x^4 + x^2 + 1$,
iv) $P_4 = x^6 - 4$.

Exercise 67: Show that the product of the non-zero elements of any finite field E is -1.

Exercise 68: Find the number of monic irreducible polynomials of degree 4 in $\mathbb{Z}_3[x]$.

Exercise 69: Find the number of monic irreducible polynomials of degree d in $\mathbb{Z}_p[x]$, when both d and p are prime.

Exercise 70: (Putnam 2001-A3) For each integer m, consider the polynomial

$$P_m(x) = x^4 - (2m+4)x^2 + (m-2)^2.$$

For what values of m is $P_m(x)$ the product of two non-constant polynomials with integer coefficients?