ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2014

Brookfield, Shaheen, Webster*

Directions: *Answer 5 questions only.* You must answer *at least one* from each of groups, rings, and fields. Indicate CLEARLY which problems you want us to grade—otherwise, we will select which ones to grade, and they may not be the ones that you want us to grade. Be sure to show enough work that your answers are adequately supported.

Notation: $\mathbb{Q}$ denotes the rational numbers; $\mathbb{Z}_n$ denotes the integers modulo n.

Groups

G1 Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

`Answer:` *Fraleigh, Theorem 11.5, p. 106.*

G2 Give an explicit example of a Sylow-3 subgroup of S_6. How many such subgroups are there?

`Answer:` *Since* $|S_6| = 6! = 720 = 2^4 \cdot 3^2 \cdot 5$, *a Sylow-3 subgroup has order* $3^2 = 9$. *Groups of order* 9 *are either cyclic or isomorphic to* $\mathbb{Z}_3 \times \mathbb{Z}_3$. *Since* S_6 *has no elements of order* 9, *its Sylow-3 subgroups are isomorphic to* $\mathbb{Z}_3 \times \mathbb{Z}_3$ *and are generated by two commuting elements of order* 3. *For example, since* (123) *and* (456) *commute, the subgroup they generate*

$$\begin{aligned} G &= \langle (123), (456) \rangle \\ &= \{1, (123), (321), (456), (123)(456), (321)(456), (654), \\ &\quad (123)(654), (321)(654)\} \end{aligned}$$

has order 9 *and is a Sylow-3 subgroup of* S_6.

In S_4 *there are 10 pairs of commuting order* 3 *elements and so there are* 10 *such Sylow-3 subgroups. Note that* 10 *divides the order of* S_6, *and* $10 \equiv 1 \mod 3$ *in accordance with the Sylow theorems.*

G3 Let a, b be the elements of a group G. Assume that a has order 5 and $a^3b = ba^3$. Prove that $ab = ba$.

`Answer:` *[See S09]* $ab = a^6b = a^3a^3b = a^3ba^3 = ba^3a^3 = ba^6 = ba$.

Rings

R1 Let R be a ring of characteristic p. Prove that if a is nilpotent then $1 + a$ is unipotent, that is, some power of $1 + a$ is equal to 1.

`Answer:` *Reminder: In a commutative ring* R *of characteristic* p, $(a + b)^p = a^p + b^p$ *for all* $a, b \in R$. *An easy induction shows that, more generally,* $(a + b)^{p^k} = a^{p^k} + b^{p^k}$ *for all* $a, b \in R$ *and* $k \in \mathbb{N}$. *See Fraleigh, Lemma 33.9, p. 303.*

Now to the exam question... Since a is nilpotent, $a^n = 0$ for some $n \in \mathbb{N}$. Consequently, $a^m = 0$ for all $m \geq n$. Now choose $k \in \mathbb{N}$ such that $p^k \geq n$. Then

$$(1+a)^{p^k} = 1^{p^k} + a^{p^k} = 1 + 0 = 1.$$

R2 Let F be a field and $p(x)$ be a non-zero polynomial in $F[x]$. Prove that the ideal $\langle p(x) \rangle$ is maximal if and only if $p(x)$ is irreducible in $F[x]$.

`Answer:` *See Fraleigh, Lemma 45.12, p. 393.*

OR

Suppose that $\langle p \rangle$ is maximal. If $p = fg$ for some $f, g \in F[x]$, then $p \in \langle f \rangle$ and so $\langle p \rangle \subseteq \langle f \rangle \subseteq F[x]$. By the maximality of $\langle p \rangle$, we have two cases:

(a) If $\langle f \rangle = \langle p \rangle$, then $f = ph$ for some $h \in F[x]$ and so $p(hg-1) = phg - p = fg - p = p - p = 0$. Since $p \neq 0$ and $F[x]$ is a domain this implies $hg = 1$, that is, g is a unit.

(b) If $\langle f \rangle = F[x]$, then $1 \in \langle f \rangle$ meaning that $1 = fh$ for some $h \in F[x]$. That is, f is a unit.

This shows that p is irreducible.

Now suppose that p is irreducible. Suppose that $\langle p \rangle \subseteq I \subseteq F[x]$ for some ideal I. Since $F[x]$ is a PID, $I = \langle g \rangle$ for some $g \in F[x]$. Because $\langle p \rangle \subseteq \langle g \rangle$, we have $p = fg$ for some $f \in F[x]$. By the irreducibility of p we have two cases:

(a) If g is a unit, then $I = \langle g \rangle = F[x]$.

(b) If f is a unit, then p and g are associates and $I = \langle g \rangle = \langle p \rangle$.

This shows that $\langle p \rangle$ is maximal.

R3 Show that $f(x) = x^5 - 5x + 1$ is irreducible over $\mathbb{Q}$.

`Answer:` *f is irreducible because $f(x-1) = x^5 - 5x^4 + 10x^3 - 10x^2 + 5$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 5$.*

Fields

F1 Let p be a prime and r be a positive integer. Prove that a field of size $q = p^r$ exists.

`Answer:` *[See S09 and S10] Fraleigh, Lemma 33.10, p. 303.*

F2 Show that $\alpha = \sqrt{a}+\sqrt{b} \in \mathbb{C}$ with $a, b \in \mathbb{Q}$ is algebraic over $\mathbb{Q}$ with degree of at most 4. Note: a and b could be negative numbers, and $\sqrt{a}$ and $\sqrt{b}$ can represent either square root of these numbers.

`Answer:` *The number α is a root of the polynomial*

$$f(x) = x^4 - 2(a+b)\,x^2 + (a-b)^2 \in \mathbb{Q}[x].$$

The roots of f are $\pm\sqrt{a} \pm \sqrt{b}$.

F3 Let K be a field generated over F by two elements α and β of relatively prime degrees m and n, respectively. Prove that $[K : F] = mn$.

`Answer:` *We have $F \subseteq F(\alpha) \subseteq F(\alpha, \beta) = K$ and so $[K : F] = [K : F(\alpha)][F(\alpha) : F]$. Since $\deg(\alpha, F) = [F(\alpha) : F] = m$, this implies that m divides $[K : F]$. We also have $\deg(\beta, F) = n$ and so β is a root of a polynomial $f \in F[x]$ of degree n. Since f is also in $F(\alpha)[x]$ this means that $\deg(\beta, F(\alpha)) \leq n$, that $[K : F(\alpha)] = [F(\alpha)(\beta) : F(\alpha)] \leq n$, and that $[K : F] \leq mn$.*

Reversing the roles of α and β in the above we see that n divides $[K : F]$ too. Since m and n are relatively prime, this implies that mn divides $[K : F]$, in particular, $mn \leq [K : F]$.

We have shown that $mn \leq [K : F] \leq mn$ and so $[K : F] = mn$.