ALGEBRA COMPREHENSIVE EXAMINATION

Spring 2015

Brookfield*, Shaheen, Webster

Directions: Answer 5 questions only. If you answer more than five questions, only the first five will be graded. You must answer *at least one* from each of groups, rings, and fields. Be sure to show enough work so that your answers are adequately supported.

Groups

(1) Let $\phi : G \to H$ be a nontrivial group homomorphism with $|G| = 10$ and $|H| = 15$. Prove that G is abelian.

`Answer:` *The image of the homomorphism,* $\operatorname{im}\phi$*, is a subgroup of* H*, so has order that divides* $|H| = 15$*. But* $\operatorname{im}\phi$ *is also isomorphic to* $G/\ker\phi$*, so the order of* $\operatorname{im}\phi$ *must divide* $|G| = 10$*. This means* $|\operatorname{im}\phi|$ *is* 1 *or* 5*. But* ϕ *is nontrivial, so* $|\operatorname{im}\phi| = 5$*. Then* $K = \ker\phi$ *is a normal subgroup of* G *of order* $|G|/|\operatorname{im}\phi| = 2$*. By Sylow,* G *also has a subgroup* L *of order* 5 *which must be normal because it has index* 2 *in* G*.*

We now know that G *has normal subgroups* K *and* L *of orders* 2 *and* 5*. From here one proves* $K \cap L = \{1\}$*, and then* $G \cong K \times L \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10}$*, so* G *is cyclic. See, for example, Fraleigh Lemma 37.5, Algebra Exam Fall 2008.*

(2) Let $p < q$ be distinct primes numbers and G a group of order pq. Show that G is not simple.

`Answer:` *By the Sylow Theorems,* $n_q \equiv 1 \mod q$ *and* $n_q | pq$*. From the second condition we get* $n_q \in \{1, p, q, pq\}$*. But* q *and* pq *are congruent to* 0 *modulo* q*. And* p *cannot be congruent to* 1 *modulo* q *because* $1 < p < q$*. So this leaves* $n_q = 1$ *and so* G *has a normal Sylow subgroup of order* q*. In particular,* G *is not simple.*

(3) Let G be a group and $g \in G$.

(a) Show that $N(g) = \{h \in G : hg = gh\}$ is a subgroup of G.

(b) Show that, if G is finite, then $|G|/|N(g)|$ is the number of elements of G that are conjugate to g.

`Answer:`

(a) *$N(g)$ closed under the group operation: Suppose that* $h_1, h_2 \in N(g)$*. Then* $h_1 g = g h_1$ *and* $h_2 g = g h_2$*, so*

$$(h_1h_2)g = h_1(h_2g) = h_1(gh_2) = (h_1g)h_2 = (gh_1)h_2 = g(h_1h_2)$$

and so $h_1h_2 \in N(g)$*.*

$N(g)$ closed under taking inverses: If $h \in N(g)$*, then* $hg = gh$*. Multiplying this equation on the left and right by* h^{-1} *we get* $h^{-1}hgh^{-1} = h^{-1}ghh^{-1}$ *which implies that* $gh^{-1} = h^{-1}g$*, that is* $h^{-1} \in N(g)$*.*

(b) *Consider the function* $\phi : G \to G$ *defined by* $\phi(h) = hgh^{-1}$*. Warning: This function is not a group homomorphism. The image of* ϕ *is the set* *of conjugates of g. For $h_1, h_2 \in G$ we have*

$$\begin{aligned}\phi(h_1) = \phi(h_2) &\iff h_1 g h_1^{-1} = h_2 g h_2^{-1} \\ &\iff h_2^{-1} h_1 g = g h_2^{-1} h_1 \\ &\iff h_2^{-1} h_1 \in N(g) \\ &\iff h_1 N(g) = h_2 N(g)\end{aligned}$$

Thus h_1 and h_2 get sent to the same conjugate of g if and only if they are in the same left coset of $N(g)$. This implies that the number of conjugates of g equals the number of left cosets of $N(g)$, which by Lagrange, is $|G|/|N(g)|$.

OR

Let G act on G by conjugation. That is, let $\phi : G \to S_G$ be defined by $\phi_h(g) = hgh^{-1}$ for all $h, g \in G$. In other notation, let $h \cdot g = hgh^{-1}$ for all $h, g \in G$. Then the orbit of g is the set of conjugates of g, the stabilizer of g is $N(g)$ (called the centralizer of g), and so the number of elements in the orbit is the index of the stabilizer in G which is the number of left cosets (or right cosets) of $N(g)$. See Dummit and Foote, Section 4.3.

Rings

(1) Suppose that R and R' are rings. Let $\phi : R \to R'$ be a ring homomorphism.
   (a) Let I' be an ideal of R'. Prove that

$$\phi^{-1}(I') = \{x \in R \mid \phi(x) \in I'\}$$

   is an ideal of R.
   (b) Prove that the kernel of ϕ is an ideal of R.

(2) Let I be an ideal of a commutative ring R with identity and define

$$\mathrm{rad}(I) := \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}.$$

Show that $\mathrm{rad}(I)$ is an ideal containing I.
`Answer:` *(Algebra Comp S01, F01, S02, S03 and F07) First we notice that if $r \in I$, then $r^1 \in I$ and so $r \in \mathrm{rad}\, I$. Hence $I \subseteq \mathrm{rad}\, I$.*

It remains to show that $\mathrm{rad}\, I$ is an ideal, that is, $\mathrm{rad}\, I$ is closed under addition and under multiplication by elements of R.

First we notice that, because $RI \subseteq I$, if $a^n \in I$, then all higher powers of a are in I. Now suppose that $a, b \in \mathrm{rad}\, I$. Then there is an integer $n \in \mathbb{N}$ such that $a^m \in I$ and $b^m \in I$ for all $m \geq n$. Then each term of the binomial expansion of $(a+b)^{2n}$ has a sufficiently high power of a or of b so that the term is in I. (Here we used $RI \subseteq I$.) Since I is closed under addition, $(a+b)^{2n} \in I$ and so $a + b \in \mathrm{rad}\, I$.

Suppose that $a \in \mathrm{rad}\, I$ and $r \in R$. Then $a^n \in I$ for some $n \in \mathbb{N}$ and so $(ra)^n = a^n r^n \in I$. (Here we used $RI \subseteq I$.) Hence $ra \in \mathrm{rad}\, I$.

(3) Let R be a unique factorization domain.
   (a) Let $p \in R$ be irreducible. Show that $Rp = (p)$ is a prime ideal.
   `Answer:` *Suppose that $ab \in Rp$ for some $a, b \in R$. Then $pr = ab$ for some $r \in R$. Both sides of this equation can be factored into irreducible*

elements. Because of the uniqueness, the irreducible p on the left must be an associate of an irreducible element in the factorization of ab, that is, p is an associate of an irreducible element that divides a or p is an associate of an irreducible element that divides b. Thus $p|a$ or $p|b$, in other words, $a \in Rp$ or $b \in Rp$.

(b) Show that every nonzero prime ideal of R contains a prime ideal of the form $Rp = (p)$ for some irreducible $p \in R$.
`Answer:` *Let P be a nonzero prime ideal of R and r a nonzero element of P. Then r can be written as product of irreducible elements $r = p_1 p_2 \cdots p_n$. Because $r \in P$ and P is prime, one of these irreducible elements p_i is in P. Then Rp_i is a prime ideal (by (a)) that is contained in P.*

Fields

(1) Let E be an extension field of a field F. Let $\alpha \in E$ be algebraic over F. Prove that there exists a nonzero polynomial $f \in F[x]$ such that
(a) $f(\alpha) = 0$.
(b) If $g \in F[x]$ and $g(\alpha) = 0$, then f divides g
`Answer:` *Let $f \in F[x]$ be a nonzero polynomial of smallest degree having α as a root. (Such polynomials exist because α is algebraic over F.) Now suppose that $g \in F[x]$ has α as a root. Write $g = qf + r$ where $q, r \in F[x]$ and $r = 0$ or $\deg r < \deg f$. Plugging in α in this equation gives $r(\alpha) = 0$. This would contradict our choice of f unless $r = 0$. Hence $g = qf$, that is f divides g.*

(2) Show that $f(x) = x^4 + 1$ and $g(x) = x^4 - 2x^2 + 9$ have the same splitting field over $\mathbb{Q}$.
`Answer:` *The roots of f are $(\pm 1 \pm i)/\sqrt{2}$. The roots of g are $\pm i \pm \sqrt{2}$. So both splitting fields are in $\mathbb{Q}(i, \sqrt{2})$. In fact, the opposite inclusions also hold: The equations*

$$\sqrt{2} = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}} \qquad i = \frac{(1+i)/\sqrt{2}}{(1-i)/\sqrt{2}}$$

show that $\mathbb{Q}(i, \sqrt{2})$ is contained in the splitting field of f. The equations

$$\sqrt{2} = \frac{1}{2}\Big((i+\sqrt{2}) + (-i+\sqrt{2})\Big) \qquad i = \frac{1}{2}\Big((i+\sqrt{2}) + (i-\sqrt{2})\Big)$$

show that $\mathbb{Q}(i, \sqrt{2})$ is contained in the splitting field of g. Thus the splitting field of both these polynomials is $\mathbb{Q}(i, \sqrt{2})$.

(3) Let $\sigma = e^{2\pi i/7} \in \mathbb{C}$, a primitive seventh root of unity, and $F = \mathbb{Q}(\sigma)$. F is the splitting field for $x^7 - 1$ over $\mathbb{Q}$ so is a Galois extension of $\mathbb{Q}$. The minimum polynomial for σ over $\mathbb{Q}$ is the seventh cyclotomic polynomial

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

so you can express elements of F uniquely in the form $\alpha = a + b\sigma + c\sigma^2 + d\sigma^3 + e\sigma^4 + f\sigma^5 \in F$ for suitable $a, b, c, d, e, f \in \mathbb{Q}$. Let $\phi \in \mathrm{Gal}(F, \mathbb{Q})$ be the automorphism such that $\phi(\sigma) = \sigma^4$. Find the fixed field of ϕ.

`Answer:` *Let* $\alpha = a + b\sigma + c\sigma^2 + d\sigma^3 + e\sigma^4 + f\sigma^5$ *with* $a, b, c, d, e \in \mathbb{Q}$. *Then*

$$\begin{aligned}\phi(\alpha) &= a + b\sigma^4 + c\sigma + d\sigma^5 + e\sigma^2 + f\sigma^6 \\ &= (a - f) + (b - f)\sigma^4 + (c - f)\sigma + (d - f)\sigma^5 + (e - f)\sigma^2 - f\sigma^3\end{aligned}$$

If $\phi(\alpha) = \alpha$, *then by the uniqueness of these expressions we get*

$$a = a - f \quad b = c - f \quad c = e - f \quad d = -f \quad e = b - f \quad f = d - f$$

with solutions

$$d = f = 0 \qquad b = c = e.$$

Thus α *is in the fixed field of* ϕ *if and only if*

$$\alpha = a + b(\sigma + \sigma^2 + \sigma^4)$$

for some $a, b \in \mathbb{Q}$. *Thus the fixed field of* ϕ *is* $\mathbb{Q}(\sigma + \sigma^2 + \sigma^4)$.