ALGEBRA COMPREHENSIVE EXAMINATION

Fall 2020

Brookfield, Krebs, Shaheen*

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: $\mathbb{R}$ denotes the set of real numbers; $\mathbb{Q}$ denotes the set of rational numbers; $\mathbb{Z}$ is the set of integers; $\mathbb{Z}_n$ is the set of integers modulo n; and $\mathbb{C}$ is the set of complex numbers. All of these should be thought of as groups under ordinary addition, and as rings under ordinary addition and multiplication.

Groups

(G1) Let G be a cyclic group and H be a subgroup of G. Prove that H is cyclic.
Solution: See Fraleigh, Theorem 6.6. Dummit and Foote, Theorem 7, p. 58.

(G2) Let G be a group of order 56. Prove that G is not simple.
Solution: See https://www.sas.upenn.edu/ htowsner/math502/practicefinalsolutions.pdf

(G3) Let H be a subgroup of a finite group G.
- (a) Show that, if H is a subgroup of G with index 3, then H may not be normal.
- (b) Show that, if H is the unique subgroup of G with index 3, then H is normal.

Solution:
- (a) For example, $H = \{1, (1\,2)\}$ as a subgroup of $G = S_3$.
- (b) For each element $a \in G$, the map $x \mapsto axa^{-1}$ is an isomorphism, so the subgroup aHa^{-1} is isomorphic to H. Since G has a unique subgroup of order $|H|$, namely H itself, we have $aHa^{-1} = H$ for any $a \in G$.

Rings

(R1) Let R be a commutative ring with identity $1 \neq 0$.
- (a) Let I be an ideal of R. Prove that $I = R$ if and only if I contains a unit of R.
- (b) Prove that R is a field if and only if the only ideals of R are the trivial ideal $\{0\}$ and the entire ring R.

Solution: See Dummit and Foote, Proposition 9, p. 253.

(R2) Let $\phi : F \to R$ be a ring homomorphism where F is a field and R is a ring. Prove:
- (a) The kernel of ϕ is an ideal of F
- (b) If ϕ is onto and $R \neq \{0\}$ then ϕ is an isomorphism.

Solution: For (a) see Dummit and Foote, Proposition 5, p. 240. The proof of (b) is as follows: Since the $\ker(\phi)$ is an ideal of F and F is a field, either $\ker(\phi) = \{0\}$ or $\ker(\phi) = F$. Since ϕ is onto and $R \neq \{0\}$ we must have that $\ker(\phi) \neq F$. Therefore $\ker(\phi) = \{0\}$. Thus ϕ is one-to-one. Thus ϕ is both onto (by assumption) and one-to-one. Therefore ϕ is an isomorphism.

(R3) Let R be an integral domain. Because of the axiom of choice, every proper ideal of R is contained in a maximal ideal of R. (No need to prove this.) Suppose that R has a unique maximal ideal I. (Such rings are called **local**.) Let U denote the group of

units of R. Show that R is the disjoint union of I and the group of units of R. [That is, show that $R = I \cup U$ and $I \cap U = \emptyset$.]
Solution: Let U be the group of units of R. Suppose $r \in R$ is not a unit. Then (r) is a proper ideal of R so is contained in the unique maximal ideal I, in particular, $r \in I$. This shows that $R = I \cup U$.

Suppose that $r \in U \cap I$. Then, since r is a unit we have $(r) = R$. On the other hand we have $r \in I$ and so $(r) \subseteq I$. This is a contradiction since I is a proper ideal of R.

Fields

(F1) Let $f(x) = x^5 - 2 \in \mathbb{Q}[x]$. Let E be the splitting field of f over $\mathbb{Q}$.
(a) Show that E contains both $\mathbb{Q}(\sqrt[5]{2})$ and ζ, where $\zeta = e^{2\pi i/5}$.
(b) What is $[E\colon \mathbb{Q}]$? Prove that your answer is correct.
Solution: See https://www.math.tamu.edu/ alperez/NewGalGroupofPoly.pdf

(F2) Let F be a field of charcteristic 0. Let $p(x) \in F[x]$ such that $p(x)$ is irreducible over F. Let K be the splitting field of $p(x)$ over F. Let G be the Galois group of K over F. Let $\alpha \in K$. Let
$$\beta = \sum_{\sigma \in G} \sigma(\alpha).$$
Prove that $\beta \in F$.
Solution sketch: Show that $\tau(\beta) = \beta$ for all $\tau \in G$. Thus β is in the fixed field of G, which by the Fundamental Theorem of Galois Theory is equal to F.

(F3) Construct the addition and multiplication tables for the field with four elements. Explain how the field properties determine these tables.
Solution 1: The polynomial $x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible over $\mathbb{Z}_2$ since it has no roots in $\mathbb{Z}_2$. Let $I = (x^2 + x + 1)$ and so $\mathbb{Z}_2[x]/I$ is a field with 4 elements, namely, the cosets $\{0 + I, 1 + I, x + I, 1 + x + I\}$.

$+$	$0+I$	$1+I$	$x+I$	$1+x+I$
$0+I$	$0+I$	$1+I$	$x+I$	$1+x+I$
$1+I$	$1+I$	$0+I$	$1+x+I$	$x+I$
$x+I$	$x+I$	$1+x+I$	$0+I$	$1+I$
$1+x+I$	$1+x+I$	$x+I$	$1+I$	$0+I$

$\times$	$0+I$	$1+I$	$x+I$	$1+x+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$x+I$	$1+x+I$
$x+I$	$0+I$	$x+I$	$1+x+I$	$1+I$
$1+x+I$	$0+I$	$1+x+I$	$1+I$	$x+I$

Solution 2: The group of units has order 3 so is cyclic and has the form $\{1, a, a^2\}$ with $a^3 = 1$. Thus the field is $\{0, 1, a, a^2\}$ and the multiplication table is determined by the equation $a^3 = 1$:

$\times$	0	1	a	a^2
0	0	0	0	0
1	0	1	a	a^2
a	0	a	a^2	1
a^2	0	a^2	1	a

$+$	0	1	a	a^2
0	0	1	a	a^2
1	1	0	a^2	a
a	a	a^2	0	1
a^2	a^2	a	1	0

The characteristic of the field is prime and divides the order of the field so is two. This means that any field element added to itself is zero. This, and the defining property of 0 fills in 10 of the entries of the addition table. Since this table is a group table, the entry for $1 + a$ can't be 0, 1 or a since these are entries in the same row or column. Thus $1 + a = a^2$. Similarly, $1 + a^2 = a$, and $a + a^2 = 1$, completing the addition table.