

## Final Exam Solutions

- 1a. The Galois group of a splitting field  $E$  of  $f(x)$ , i.e. all field automorphisms  $E \rightarrow E$  which fix  $F$ .
- b.  $G$  is solvable if  $\exists$  a chain  
 $\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \dots \triangleleft G_n = G$  with each  $G_i/G_{i-1}$  abelian.
- c. A field automorphism of  $E$  is a function  $\phi: E \rightarrow E$  which is 1-1 and onto and has  
 $\phi(a+b) = \phi(a) + \phi(b)$ ,  $\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in E$ .
- d.  $G$  is simple if it has no normal subgroups other than  $\{e\}$  and  $G$ .
- e. An integral domain is a commutative ring w/ identity and no zero divisors.
- f.  $*$  is associative if  $(a*b)*c = a*(b*c) \quad \forall a, b, c \in S$

- 2.
- |          |          |
|----------|----------|
| a. False | i. False |
| b. True  | j. False |
| c. False | k. True  |
| d. True  |          |
| e. True  |          |
| f. True  |          |
| g. True  |          |
| h. True  |          |

3 Lagrange's Thm: Let  $H \leq G$ ,  $|G|$  finite. Then  $|H|$  divides  $|G|$ .

Cauchy's Thm: Suppose  $p \mid |G|$ ,  $p$  prime. Then  $G$  has an element of order  $p$ .

4 a.  $\left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & c & 0 \end{pmatrix} \mid a, b, c \in \mathbb{Q} \right\}$  is a noncomm. ring w/ unit  $I$ .

b.  $\mathbb{Z}_{10}$

c.  $A_5$

d.  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

e.  $15x^5 + 2x + 2$   $p=2$

f.  $i$

9.  $V = \{e, (12)(34), (13)(24), (14)(23)\}$

5a.  $x^2 - 7$   $E = \mathbb{Q}(\sqrt{7})$  degree 2 basis  $\{1, \sqrt{7}\}$

b.  $x^2 + 1$   $E = \mathbb{R}(i) \cong \mathbb{C}$  degree 2 basis  $\{1, i\}$

c.  $x^3 - 2$   $E = \mathbb{Q}(\sqrt[3]{2}, i)$  degree 6 basis  $\{1, \sqrt[3]{2}, \sqrt[3]{4}, i, i\sqrt[3]{2}, i\sqrt[3]{4}\}$

d.  $x^2 - \pi^4$   $E = \mathbb{Q}(\pi^2)$  degree 2 basis  $\{1, \pi^2\}$

6a. basis  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

Let  $\sigma(\sqrt{2}) = -\sqrt{2}$   $\sigma(\sqrt{3}) = \sqrt{3}$  so

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

Let  $\tau(\sqrt{2}) = \sqrt{2}$   $\tau(\sqrt{3}) = -\sqrt{3}$  so

$$\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

Then  $G(E/F) = \{e, \sigma, \tau, \sigma\tau\} \cong V$

b. Basis  $\{1, \sqrt[3]{7}, (\sqrt[3]{7})^2\}$

$$G(E/F) = \{e\}$$

7.  $H \trianglelefteq G$  so  $G/H$  is the quotient group and has order  $m$ .

We proved that  $g^{1/H}$  is always  $e$  so in  $G/H$  we have for any  $g$ ,

$$(gH)^m = H \quad \text{so } g^m H = H \quad \text{which holds if \& only if } g^m \in H.$$

8.  $113/25, \sqrt{1-\sqrt[4]{3}}, \sin(15^\circ), \sqrt[3]{3}$  YES

$\sqrt[3]{7}, \pi^2, e, \cos(10^\circ)$  NO

9. a.  $p(x) = x^2 + 1 = p(1/x)$  so  $p$  has no roots in  $\mathbb{Z}_2$  so it is irreducible since it has degree 2.

b.  $E = \mathbb{Z}_2(\alpha)$  where  $\alpha^2 + \alpha + 1 = 0$ , i.e.  $\alpha^2 = 1 + \alpha$

$+$	0	1	$\alpha$	$1+\alpha$
0	0	1	$\alpha$	$1+\alpha$
1	1	0	$1+\alpha$	$\alpha$
$\alpha$	$\alpha$	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	$\alpha$	1	0

  

$\cdot$	0	1	$\alpha$	$1+\alpha$
0	0	0	0	0
1	0	1	$\alpha$	$1+\alpha$
$\alpha$	0	$\alpha$	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	$\alpha$

c. Yes!

$$(x+\alpha)(x+1+\alpha) = x^2 + \alpha x + (1+\alpha)x + \alpha^2 + \alpha + 1 + \alpha$$

$$= x^2 + x + 1 \quad \text{in } E[x]$$

d.  $x^2 + x + \alpha$  has no roots in  $\mathbb{Z}_2(\alpha)$  so is irreducible

10.

Let  $x \in \Phi^{-1}(\Phi(g))$  so  $\Phi(x) = \Phi(g)$  so  $\Phi(g)^{-1}\Phi(x) = e$   
so  $\Phi(g^{-1}x) = e$  so  $g^{-1}x \in K$  so  $x \in gK$ , so LHS  $\subseteq$  RHS

Let  $gK \in gK$ . Then  $\Phi(gK) = \Phi(g)\Phi(K) = \Phi(g)e = \Phi(g)$ .

Thus  $gK \in \Phi^{-1}(\Phi(g))$  so RHS  $\subseteq$  LHS //

11a. order  $g$  is smallest  $n \geq 1$  such that  $g^n = e$ .

b.  $(1234567)(89101112)(131415) = \sigma$   
has order 105

12a. Given  $H \leq G$  Let

$$E_1 = \{a \in E \mid f(a) = a \quad \forall f \in H\}$$

$E_1$  is the fixed field of  $H$ .

b. Given  $F \subseteq E_1 \subseteq E$  Let  $G(E/E_1) = \{\sigma \in G(E/F) \mid \sigma \text{ fixes } E_1\}$

Then  $G(E/E_1) \leq G$ .

13

a. Let  $k \in K, g \in G$ . Then  $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1})$   
 $= \phi(g)\phi(g)^{-1}$  since  $k \in K$   
 $= e$ .

Thus  $gkg^{-1} \in K$  so  $K \triangleleft G$ .

b.  $G/K \cong H$  by Fundamental Hom. Thm.

c.  $g$  has order 6  $\Rightarrow \phi(g)$  has order 1, 2, 3 or 6