

MTH 532, Final Exam

Ayman Badawi

ALL RINGS ARE COMMUTATIVE with $1 \neq 0$

QUESTION 1. (i) Let M, N be two maximal ideals of R such that $N \cap M = \{0\}$.

a. Prove that R is ring-isomorphic to $F_1 \times F_2$ for some fields F_1 and F_2.

b. Let Q_1, Q_2 be co-prime ideals of R that are not maximal ideals of R. Prove that $Q_1 \cap Q_2 \neq \{0\}$

c. How many idempotent elements does R have?

QUESTION 2. (i) Convince me that $f(y) = y^3 + 2y + 2$ is irreducible in $Z_3[y]$.

(ii) Find the smallest m so that $f(y)$ has all its roots in $GF(3^m)$.

(iii) Convince me that $f(y) = y^2 + 3$[illegible] is irreducible in $Z_5[y]$. Then $f(y)$ has all its roots in $Z_5[x]/(x^2 + 3$[illegible]$)$. Find all the roots of $f(y)$.

QUESTION 3. (a) Assume that $[E : Q] = 15$. Let $f(x)$ be a monic irreducible polynomial in $Q[x]$ that has a root in E. What are the possibilities of $deg(f(x))$?

(b) Assume that $[E : Q] = 6$ and E is a Galois extension of Q. Assume that $f(x) \in Q[x]$ is monic irreducible in $Q[x]$ and $f(a) = 0$ for some $a \in E$. Can we conclude that E is the splitting field of $f(x)$? explain. If your answer is no, then let F be the splitting field of of $f(x)$. Find $[F : Q]$.

(c) We know $E = Q(\sqrt{2}, \sqrt{7})$ is a Galois extension of Q. Find $Aut_Q(E)$. Find all subfields of E. Find all subgroups of $Aut_Q(E)$.

(d) Let E be the splititing field of $x^{50} - 1$. Find $[E : Q]$. How many subfields does E have?

QUESTION 4. Let D be a group such that $|D| = 7^2 \times 1$[illegible]. Up to isomorphism, find all such groups.

11^2

Faculty information

Ayman Badawi, Department of Mathematics & Statistics, American University of Sharjah, P.O. Box 26666, Sharjah, United Arab Emirates.
E-mail: abadawi@aus.edu, www.ayman-badawi.com

Question 1: let M, N be two maximal ideals of R st. $N \cap M = \{0\}$

a). Prove that R is ring isomorphic to $F_1 \times F_2$ for some fields F_1 and F_2

Proof: first, notice that M, N are coprime.

since M is maximal then $M + aR = R \quad \forall a \in R \setminus M$

similarly N is " then $N + aR = R \quad \forall a \in R \setminus N$

let $a \in N \setminus M$ then $M + aR = R$

Hence M, N are coprime.

Now, by the chinese remainder thrm:

46/50

$$R/_{M \cap N} \simeq R/_N \times R/_M$$

$$\text{so } R \simeq R/_{\{0\}} \simeq R/_N \times R/_M \simeq F_1 \times F_2$$

and by class result $R/_M$, $R/_N$ are fields since M, N are maximal ideals

b). let Q_1, Q_2 be coprime ideals of R, both not maximal ideals of R

Prove that $Q_1 \cap Q_2 \neq \{0\}$

suppose $Q_1 \cap Q_2 = \{0\}$ by chinese remainder thm

then $R/_{Q_1 \cap Q_2} \simeq R/_{Q_1} \times R/_{Q_2}$

then $R \simeq R/_{Q_1} \times R/_{Q_2} \simeq F_1 \times F_2$ Fields

then $R/_{Q_1}$ and $R/_{Q_2}$ are fields

a contradiction since Q_1, Q_2 are not maximal ideals.

c). How many idempotent elements does R have?

$$R \simeq R/M \times R/N \simeq F_1 \times F_2$$

in fields the only idempotent elements are $1, 0$

so $(1,0)$, $(0,1)$, $(0,0)$, $(1,1)$

are idempotents of R

5

2

Question 2: 1) Convince me that $f(y) = y^3 + 2y + 2$ is irreducible in $\mathbb{Z}_3[y]$

$f(1) = 1 + 2 + 2 = 2 \neq 0$ in $\mathbb{Z}_3$

$f(2) = 2^3 + 4 + 2 = 2 \neq 0$ in $\mathbb{Z}_3$

$f(0) = 2 \neq 0$ in $\mathbb{Z}_3$

thus by HW result $f(y)$ is irreducible. 5

2). Find the smallest m so that $f(y)$ has all its roots in $GF(3^m)$

since $f(y)$ is irreducible of degree 3 over $\mathbb{Z}_3[x]$

then $\dfrac{\mathbb{Z}_3[x]}{(f(y))} \approx F$, such that F is a finite GF of $\mathbb{Z}_3$ and $|F| = 3^m$ where $m =$ degree of $f(y)$. thus $m = 3$ 5

3) convince me that $f(y) = y^2 + 3$ is irreducible in $\mathbb{Z}_5[y]$

$f(1) = 1 + 3 \neq 0$ in $\mathbb{Z}_5$

$f(2) = 4 + 3 = 2 \neq 0$ in $\mathbb{Z}_5$

$f(3) = 9 + 3 = 2 \neq 0$ in $\mathbb{Z}_5$

$f(4) = 16 + 3 = 4 \neq 0$ in $\mathbb{Z}_5$

$f(0) = 3 \neq 0$ in $\mathbb{Z}_5$

by HW result $f(y)$ is irreducible in $\mathbb{Z}_5[y]$

Find all the roots of $f(y)$.

$f(y)$ has all its roots in $\dfrac{\mathbb{Z}_5[x]}{(x^2+3)}$ 5

$\dfrac{\mathbb{Z}_5[x]}{(x^2+3)} \approx GF(5^2) = \{a + bx + (x^2+3) \mid a, b \in \mathbb{Z}_5[x]\}$

let $y \in GF(5^2)$ since $f(y) = y^2 + 3 \in (x^2+3)$

y is a root of $f(x)$.

then y^5 is the second root

roots are $\{\cancel{x}, 4\cancel{x}\}$

3

$$f(y^5) = (y^5)^2 + 3 = (y^1 y^2 y^2)^2 + 3 = (y(-3)(-3))^2 + 3$$

$$= (4y)^2 + 3 = y^3 + 3 = 0 \ (\mathrm{mod}\ f(11)).$$

Thus $y^5 = y(-3)(-3) = 4y$ is the second root.

not needed

4

Question 3:

1). Assume that $[E:\mathbb{Q}] = 15$ let $f(x)$ be a monic irreducible polynomial in $\mathbb{Q}[x]$ that has a root in E what are the possibities of $\deg(f(x))$?

let $a \in E$ (a could be in $\mathbb{Q}$).

then $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq E$

and $\frac{\mathbb{Q}[x]}{(f(x))} \simeq \mathbb{Q}(a)$.

Now $[E:\mathbb{Q}] = [E:\mathbb{Q}(a)][\mathbb{Q}(a):\mathbb{Q}] = 15$

let m be $\deg(f(x))$. then $m \mid 15$

so $m = 1, 3, 5$ or 15

2). Assume that $[E:\mathbb{Q}] = 6$ and E is a galois extension of $\mathbb{Q}$. Assume that $f(x) \in \mathbb{Q}[x]$ is monic irreducible in $\mathbb{Q}[x]$ and $f(a) = 0$ for some $a \in E$. Can we conclude that E is the splitting field of $f(x)$?

why cyclotomic !?

Now $[E:\mathbb{Q}] = 6 = |Aut_{\mathbb{Q}}(E)|$.

$6 = 3 \times 2$, $Aut_{\mathbb{Q}}(E) \not\simeq \mathbb{Z}_1 \times \mathbb{Z}_2 \ldots \mathbb{Z}_3$ for some n

thus no $f(x)$ with only real roots can split over E with order 6

then we are left with complex roots. thus

$E = \mathbb{Q}(\alpha)$ where $\alpha = e^{\frac{2\pi i}{n}}$ s.t $\phi(n) = 6$

$\phi_n(x) = \pi(x - \alpha^k) \in \mathbb{Q}[x]$

so we can conclude that E is the splitting field of some irreducible of order 6

so E has to be a splitting field since it is a Galois

No

0/5

5

7. We know $E = \mathbb{Q}(\sqrt{2}, \sqrt{7})$ is a Galois extension of $\mathbb{Q}$.
Find $Aut_{\mathbb{Q}}(E)$. Find all subfields of E.
Find all subgroups of $Aut_{\mathbb{Q}}(E)$.

$$[E:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{7}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = \underset{2}{} \times \underset{2}{} = 4$$

thus $|Aut_{\mathbb{Q}}(E)| = 4$ and $Aut_{\mathbb{Q}}(E) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (abelian group).

$$\begin{tikzcd}
 & Aut_{\mathbb{Q}}(E) = G_4 \simeq \mathbb{Z}_2\times\mathbb{Z}_2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
Aut_{\mathbb{Q}(\sqrt{14})}(E) \arrow[dr, dash] & Aut_{\mathbb{Q}(\sqrt{7})}(E) \arrow[d, dash] & Aut_{\mathbb{Q}(\sqrt{2})}(E) \arrow[dl, dash] \\
 & Aut_E(E) &
\end{tikzcd}$$

$$\begin{tikzcd}
 & E = \mathbb{Q}(\sqrt{2},\sqrt{7}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{14}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{7}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$Aut_{\mathbb{Q}}(E) =$

$Aut_{\mathbb{Q}(\sqrt{2})}(E) = \{ f : E \to E,\ f(\sqrt{2}) = \sqrt{2},\ f(\sqrt{7}) = -\sqrt{7} \}$

$Aut_{\mathbb{Q}(\sqrt{7})}(E) = \{ f : E \to E,\ f(\sqrt{7}) = \sqrt{7},\ f(\sqrt{2}) = -\sqrt{2} \}$

$Aut_{\mathbb{Q}(\sqrt{14})}(E) = \{ f : E \to E,\ f(\sqrt{2}) = -\sqrt{2},\ f(\sqrt{7}) = -\sqrt{7}$

6

d). let E be the splitting field of $x^{50}-1$

Find $[E:\mathbb{Q}]$. How many subfields does E have?

so $[E:\mathbb{Q}] = \phi(50) = (2-1)2^{1-1} \times (5-1)5^{2-1}$
$= 4 \cdot 5 = 20$

so $[E:\mathbb{Q}] = 20$. $\phi(50)$

so. $E = \mathbb{Q}(\alpha)$ where $\alpha = e^{\frac{2\pi i}{50}}$

$Aut_{\mathbb{Q}}(E) \approx U(\mathbb{Z}_{50})$

and since $50 = 2 \cdot 5^2$. then $U(\mathbb{Z}_{50})$ is cyclic

thus is $Aut_{\mathbb{Q}}(E)$ which implies for every factor of 20

$Aut_{\mathbb{Q}}(E)$ has a subgroup, i.e of order $1, 2, 4, 5, 10, 20$

each subgroup fixes a unique subfield in E.

so E has 6 subfields.

Question 4: let D be a group such that $|D| = 7 \times 13$
up to isomorphism. find all such groups.

$|Syl(7)| = 7^2$ $\quad n_7 | 11^2$ and $n_7 = 1 \pmod 7$

so $n_7 = 1$

$|Syl(11)| = 11^2$ $\quad n_{11} | 7^2$ and $n_{11} = 1 \pmod{11}$ so $n_{11} = 1$

let $H = Syl(11) \trianglelefteq D$, $K = Syl(7) \trianglelefteq D$ $\Big\}$ then $HK \trianglelefteq D$ since $H \cap K = \{e\}$

and $|HK| = 13^2 \times 7^2 = |D|$

then $D \cong H \times K$

Syl(7) and Syl(13) are finite groups with p^2 elements.
there are both abelian. so D is abelian (product of two abelian groups)

then $D \cong (\mathbb{Z}_7 \times \mathbb{Z}_7) \times (\mathbb{Z}_{11} \times \mathbb{Z}_{11})$

$D \cong \mathbb{Z}_7 \times (\mathbb{Z}_7 \times \mathbb{Z}_{121})$

$D \cong \mathbb{Z}_{49} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$

$D \cong \mathbb{Z}_{49 \times 121}$ cyclic

8