Algebra Graduate Exam

Fall 2012

Work all the problems. Be as explicit as possible in your solutions, and justify your statements with specific reference to the results that you use. Partial credit will be given for partial solutions.

1. Use Sylow's theorems directly to find, up to isomorphism, all possible structures of groups of order $5 \cdot 7 \cdot 23$.

2. Let A, B, and C be finitely generated $F[x] = R$ modules, for F a field, with C torsion free. Show that $A \otimes_R C \cong B \otimes_R C$ implies that $A \cong B$. Show by example that this conclusion can fail when C is not torsion free.

3. Working in the polynomial ring $\boldsymbol{C}[x, y]$, show that some power of $(x + y)(x^2 + y^4 - 2)$ is in $(x^3 + y^2, y^3 + xy)$.

4. For integers $n, m > 1$, let $A \subseteq M_n(\mathbf{Z}_m)$ be a subring with the property that if $x \in A$ with $x^2 = 0$ then $x = 0$. Show that A is commutative. Is the converse true?

5. Let F be the splitting field of $f(x) = x^6 - 2$ over $\mathbf{Q}$. Show that $\mathrm{Gal}(F/\mathbf{Q})$ is isomorphic to the dihedral group of order 12.

6. Given that all groups of order 12 are solvable show that any group of order $2^2 \cdot 3 \cdot 7^2$ is solvable.

Fall 2012

① use sylow to find $|G| = 5 \cdot 7 \cdot 23$

Pf $n_{23} \equiv 1 \bmod 23$ & $n_{23} = 1, 5, 7, 35 \Rightarrow \exists P \trianglelefteq G \ |P| = 23$.

$n_7 \equiv 1 \bmod 7$ & $n_7 = 1, 23, 5 \cdot 23 \Rightarrow \exists Q \trianglelefteq G \ ; |Q| = 7$

so $\exists |PQ| = 23 \cdot 7 \Rightarrow PQ \trianglelefteq G$ & $PQ \simeq P \times Q$ (b/c $P \cap Q = \{1\}$)

so consider $\varphi : R \longrightarrow Aut(P \times Q)$ where R - sylow subgp.

Then $Aut(P \times Q) \simeq \mathbb{Z}_6 \times \mathbb{Z}_{22}$, but $(5,6) = 1$ & $(5,22) \neq 1$

so $\varphi \equiv 0 \Rightarrow G \simeq R \times P \times Q \simeq \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_{23}$.

② A, B fin. gen. $F[x] = R$ modules, F - field, C torsion free.

Show, $A \otimes_R C \simeq B \otimes_R C \Rightarrow A \simeq B$.

Show this fails if C is not torsion free.

Pf $F[x]$ - PID since F is a field

So then by fund thm of f.g. modules over PID:

$A \simeq tA \oplus R^k$ $B \simeq tB \oplus R^m$ $C \simeq R^j$ since C is torsion free

so $A \otimes_R C \simeq B \otimes C \Rightarrow (tA \oplus R^k) \otimes (R^j) \simeq (tB \oplus R^m) \otimes R^j$

$\Rightarrow tA \otimes R^j \simeq tB \otimes R^j$ and $R^{k+j} \simeq R^{m+j} \Rightarrow m = k$

and $tA \simeq tB \Rightarrow A \simeq B$.

Consider $A = B \oplus Ann(C)$. Then $A \otimes_R C \simeq (B \otimes_R C) \oplus (Ann(C) \otimes_R C) \simeq B \otimes_R C$

but $A \not\simeq B$

(3) $\mathbb{C}[x,y]$, show $(x+y)(x^2+y^4-2) \in \sqrt{I}$

$I = \langle x^3+y^2, y^3+xy \rangle$

Pf $p(x) \in \sqrt{I}$ iff $Var(I) \subseteq Var(p(x))$ by nullstellensatz.

So $Var(I) \Rightarrow$ $x^3 = -y^2$ $\quad$ $y^3 = -xy$

$(-x)^3 = y^2$ $\quad$ $y \neq 0$ or $y = 0 \Rightarrow x = 0$

$\Downarrow$ $\quad$ $\Downarrow$

$-x^3 = -x$ $\Leftarrow$ $y^2 = -x$

$x \neq 0$ $\quad$ $x = 0$

$\Downarrow$ $\quad$ $\Downarrow$

$x^2 = 1$ $\quad$ $y = 0$

$\Downarrow$ $\quad$ $\downarrow$

$x = \pm 1$ $\quad$ $(0,0)$

$(1, \pm i)$ $\quad$ $(-1, \pm 1)$

So $Var(I) = \{(0,0), (1, \pm i), (-1, \pm 1)\}$.

Now $p(0,0) = 0$, $p(1, \pm i) = 0$ & $p(-1, \pm 1) = 0$

So $p(x) \in \sqrt{I}$.

(4) $n, m > 1$, $A \leq M_n(\mathbb{Z}_m)$ be a subring w/ property that if $x \in A$ w/ $x^2 = 0 \Rightarrow x = 0$. Show A is commutative.

Is converse true?

pf $\mathbb{Z}_m$ is finite ring, M_n is finite alg over finite ring.

$\Rightarrow M_n(\mathbb{Z}_m)$ is a finite ring $\Rightarrow M_n(\mathbb{Z}_m)$ is artinian.

$\Rightarrow A$ is artinian. $\Rightarrow J(A)$ is nilpotent

Now if $x \in A \ni x^n = 0$ for n-smallest such integer > 0. Then:

n even $\Rightarrow$ $x^n = x^{n/2} x^{n/2} = 0 \Rightarrow x^{n/2} = 0 \Rightarrow \in \frac{n}{2} < n$.

n odd $\Rightarrow$ $(x^n)x = x^{n+1} = x^{n+1/2} x^{n+1/2} = 0 \Rightarrow x^{\frac{n+1}{2}} = 0 \Rightarrow \in \frac{n+1}{2} < n$ for $n > 1$.

so $\text{Nil}(A) = 0 \Rightarrow J(A) = 0$ so A is art + Jac. semisimple

$\Rightarrow A$ is semisimple $\Rightarrow$ can apply artin Wedderburn.

so $A \cong M_{n_1}(\Delta_1) \times \cdots \times M_{n_k}(\Delta_k)$

A is finite $\Rightarrow \Delta_i = F_i$ - fields by little Wedderburn.

$\text{Nil}(A) = 0 \Rightarrow n_i = 1 \ \forall i$

so $A \cong F_1 \times \cdots \times F_n$ - commutative.

Now suppose $A \leq M_2(\mathbb{Z}_2)$ w/ $A = \left\langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\rangle$.

Then $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq 0$ but $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = 0$. so the converse is false.

(5) F - splitting field of $f(x) = x^6 - 2$ over $\mathbb{Q}$.

Show $Gal(F/\mathbb{Q}) \cong D_{12} = \langle \sigma, \tau \mid \sigma^6 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$.

Pf $x^6 = 2$

$x = \sqrt[6]{2}\,\omega \leftarrow$ prim 6th root. $\Rightarrow$

F } deg 6

$\mathbb{Q}(\omega)$

} deg $\varphi(6) = \varphi(2)\cdot\varphi(3) = 2$

$\mathbb{Q}$

so $|Gal(F/\mathbb{Q})| = 12$.

Now, w/ τ: $\omega \mapsto \bar{\omega}$, $\sqrt[6]{2} \mapsto \sqrt[6]{2}$ & σ: $\sqrt[6]{2} \mapsto \sqrt[6]{2}\,\omega$, $\omega \mapsto \omega$

Then $K\langle\tau\rangle| = 2$ & $|\langle\sigma\rangle| = 6$.

w/ $\tau\sigma\tau(\sqrt[6]{2}\,\omega) = \tau\sigma(\sqrt[6]{2}\,\bar{\omega}) = \tau(\sqrt[6]{2}\,\omega\cdot\bar{\omega}) = \sqrt[6]{2}\,\omega\cdot\bar{\omega}$

but $\bar{\omega} = \omega^5$ so $\Rightarrow \sqrt[6]{2} = \sigma^{-1}(\sqrt[6]{2}\,\omega)$.

Thus, $Gal(F/\mathbb{Q}) = D_{12}$

(6) If any grp of order 12 is solvable $\Rightarrow$ since $|G| = 2^2\cdot 3\cdot 7^2$ is solvable.

Pf Consider $n_7 = 1 \bmod 7$ & $n_7 = 1, 2, 4, 3, 12, 6$. $\Rightarrow n_7 = 1$

hence $P \trianglelefteq G$ w/ $|P| = 7^2 \Rightarrow |G/P| = 12$. & is solvable.

so then $\exists$ H_i $0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_n = G/P$ & so:

$0 \trianglelefteq P \trianglelefteq PH_1 \trianglelefteq PH_2 \trianglelefteq \dots \trianglelefteq PH_n = G$. (since P is also solvable! b/c p-grp.

since $PH_i/PH_{i-1} \cong (PH_i/P)/(PH_{i-1}/P) \cong (H_i/H_i\cap P)/(H_{i-1}/H_i\cap P) \cong (H_i/P)/(H_{i-1}/P) \cong H_i/H_{i-1}$

so each quotient is cyclic & of prime order $\Rightarrow G$ is solvable.

ALGEBRA QUALIFYING EXAM SPRING 2012

Work all of the problems. *Justify the statements in your solutions by reference to specific results*, as appropriate. Partial credit is awarded for partial solutions. The set of rational numbers is $\boldsymbol{Q}$ and set of the complex numbers is $\boldsymbol{C}$.

1. Let I be an ideal of $R = C[x_1, \ldots, x_n]$. Show that $\dim_C R/I$ is finite $\Leftrightarrow$ I is contained in only finitely many maximal ideals of R.

2. If G is a group with $|G| = 7^2 \cdot 11^2 \cdot 19$, show that G must be abelian and describe the possible structures of G.

3. Let F be a finite field and G a finite group with GCD$\{char\ F, |G|\} = 1$. The group algebra $F[G]$ is an algebra over F with G as an F-basis, elements $\alpha = \sum_G a_g g$ for $a_g \in F$, and multiplication that extends $ag \cdot bh = ab \cdot gh$. Show that any $x \in F[G]$ that is not a zero left divisor (i.e. if $xy = 0$ for $y \in F[G]$ then $y = 0$) must be invertible in $F[G]$.

4. If $p(x) = x^8 + 2x^6 + 3x^4 + 2x^2 + 1 \in \boldsymbol{Q}[x]$ and if $\boldsymbol{Q} \subseteq M \subseteq \boldsymbol{C}$ is a splitting field for $p(x)$ over $\boldsymbol{Q}$, argue that Gal$(M/\boldsymbol{Q})$ is solvable.

5. Let R be a commutative ring with 1 and let $x_1, \ldots, x_n \in R$ so that $x_1y_1 + \cdots + x_ny_n = 1$ for some $y_i \in R$. Let $A = \{(r_1, \ldots, r_n) \in R^n \mid x_1r_1 + \cdots + x_nr_n = 0\}$. Show that $R^n \cong_R A \oplus R$, that A has n generators, and that when $R = F[x]$ for F a field then A_R is free of rank $n - 1$.

6. For p a prime let F_p be the field of p elements and K an extension field of F_p of dimension 72.
   i) Describe the possible structures of $Gal(K/F_p)$.
   ii) If $g(x) \in F_p[x]$ is irreducible of degree 72, argue that K is a splitting field of $g(x)$ over F_p.
   iii) Which integers $d > 0$ have irreducibles in $F_p[x]$ of degree d that split in K?

spring 2012

① $I = R = \mathbb{C}[x_1 \dots x_n]$

Show R/I has finite dim over $\mathbb{C} \iff I$ is contained in finitely many max ideals.

($\Rightarrow$) R-ring $\Rightarrow$ R/I ring w/ $\dim_{\mathbb{C}} R/I < \infty$.

Thus R/I is artinian $\Rightarrow$ & commutative (since R is commutative) and thus has finitely many max ideals.

Hence by the correspondence theorem $\exists$ only finitely many max ideals $I \subseteq M \subseteq R$. $\Rightarrow$ $I \subseteq \bigcap_{\alpha=1}^{\kappa} M_\alpha$; $\kappa < \infty$.

($\Leftarrow$) Now suppose $I \subseteq \bigcap^{\kappa} M_\alpha$; M_α - maximal.

Then, in $R \Rightarrow M_\alpha = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ so $Var(M_\alpha) = \{a_\alpha\} \subseteq \mathbb{C}^n$.

~~In particular $Var(I) = Var(\bigcap^{\kappa} M_\alpha) = \bigcup Var(M_i) = Var(\bigcap M_i)$~~

~~$\Rightarrow$ Note that if $I \subseteq \bigcap^{\kappa} M_\alpha \Rightarrow \sqrt{I} \subseteq \bigcap^{\kappa} M_\alpha$ since by nullstellensatz~~

~~$I \subseteq \sqrt{I} = Id(Var(I)) \subseteq Id(\bigcap^{\kappa} M_\alpha) = \bigcap^{\kappa} M_\alpha$, so WLOG, suppose $I = \sqrt{I}$.~~

~~Then, $Id(Var(I)) = Id(Var(\bigcap M_i)) = \bigcap M_i$~~

Note that if $I \subseteq \bigcap^{\kappa} M_\alpha \Rightarrow \sqrt{I} \subseteq \bigcap^{\kappa} M_\alpha$ by Nullstellensatz since $Id(Var(\bigcap^{\kappa} M_\alpha)) = \bigcap^{\kappa} M_\alpha$

so WLOG take $I = \sqrt{I}$.

Then recall that Max ideal in $\mathbb{C}[x \dots x_n]$ $\overset{\text{bij}}{\iff}$ pts in $\mathbb{C}^n$.

Then by the theorem $Var(I) = \{a_1 \dots a_n\} = Var(\bigcap M_\alpha)$ - var max ideals containing I. $< \infty$.

Thus $R/I = R/Id(Var(I)) = R/Id(\{a_i\}) = R/Id(Var(\bigcap^{\kappa} M_i)) = R/\bigcap^{\kappa} M_i$

now each m_i is prime & disjoint from each other, & since $\bigcap^{\kappa}$ is finite then

$R/\bigcap^{\kappa} M_i \simeq R/\prod^{\kappa} M_i \overset{\text{Chinese Rem. Thm.}}{=} \prod^{\kappa} R/m_i \simeq \prod^{\kappa} \mathbb{C} \simeq \mathbb{C}^{\kappa}$ since $R/M_i \simeq \mathbb{C}$ for M_i are maximal. w/ $\kappa < \infty$.

Spring 2012

② $|G| = 7^2 \cdot 11^2 \cdot 19$

G is abelian and describe structure

If $n_{19} \equiv 1 \bmod 19$ & $n_{19} = 1, \cancel{7}, \cancel{11}, \cancel{7^2}, \cancel{11^2}, \cancel{7\cdot 11}, \cancel{7\cdot 11^2}, \cancel{7^2 11^2}$

$n_{11} \equiv 1 \bmod 11$ & $n_{11} = 1, \cancel{7}, \cancel{7^2}, \cancel{19}, \cancel{7\cdot 19}, \cancel{7^2 19}$

$n_7 \equiv 1 \bmod 7$ & $n_7 = 1, \cancel{11}, \cancel{11^2}, \cancel{19}, \cancel{11\cdot 19}, \cancel{11^2 19}$.

So $n_{19} = 1$ & $n_7 = 1 \Rightarrow \exists$ normal subgrp $|PQ| = 19 \cdot 7^2$

Since $P \cap Q = \phi \Rightarrow PQ \cong P \times Q$ w/ Q - abelian since all grps of order p^2 are abelian let R - sylow 11 grp.

So consider $\varphi: R \longrightarrow Aut(P \times Q)$

then if $Q = \mathbb{Z}_7 \times \mathbb{Z}_7$ then $Aut(P \times Q) = Aut(P) \times Aut(Q)$

now $|Aut(P)| = 18$ and $|Aut(Q)| = (p^2 - p)(p^2 - 1) = (p-1)^2(p+1)\cdot p$

$= 6^2 \cdot 8 \cdot 7$

So then since $|R| = 11^2$ $\exists$ some elmt of order 11 in R,

however, $11 \nmid 6^2 \cdot 8 \cdot 7$ & $11 \mid 18 \Rightarrow \varphi$ must be trivial.

If $Q = \mathbb{Z}_{7^2} \Rightarrow |Aut(Q)| = 7^2 - 7 = 7(7-1) = 7(6)$

but again $11 \nmid 7 \cdot 6 \Rightarrow \varphi$ is trivial

So $G \cong R \times (P \times Q)$ which is abelian

w/ $R = \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ or $\mathbb{Z}_{11^2}$

& $Q \cong \mathbb{Z}_7 \times \mathbb{Z}_7$ or $\mathbb{Z}_{7^2}$

(3) F-finite field, G-finite group w/ $\{\text{char}F, |G|\}=1$.

$F[G] = \{\sum a_g g ;\ a_g \in F,\ g \in G\}$.

Show that any $x \in F(G)$ s.t. $xy=0 \Rightarrow y=0$ is invertible

Pf Since $\text{char}F \nmid |G| \Rightarrow FG$ is semisimple (Maschke's thm)

So $FG \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ by Artin Wedd.

F-finite field, G-finite gp $\Rightarrow FG$ is finite $\Rightarrow D_i = $ finite F_i-fields $/F$

$FG \cong M_{n_1}(F_1) \times \cdots \times M_{n_k}(F_k)$

So then given any $x \in FG \Rightarrow x = (a_1, \ldots, a_k)$ w/ $a_i \in M_{n_i}(F_i)$

so then if $a_i \cdot y = 0 \Rightarrow y=0$ then a_i must be invertible

since if a_i were not invertible then $\exists$ vector v s.t. $a_i v = 0$ for $v \neq 0$.

Hence $a_i \cdot [v\ 0\ \cdots\ 0] = 0$ for $y = [v\ 0\ \cdots\ 0] \neq 0$

so a_i must be invertible for $\forall i \Rightarrow x$ is invertible

(4) $p(x) = x^8 + 2x^6 + 3x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$, $\mathbb{Q} \leq M \leq \mathbb{C}$ is a splitting field for $p(x)$ over $\mathbb{Q}$, argue $\mathrm{Gal}(M/\mathbb{Q})$ is solvable.

If we let $y = x^2 \Rightarrow p(y) = y^4 + 2y^3 + 3y^2 + 2y + 1$.

Then if E - splitting field of $p(y)$ we have that if α is a root of $p(y)$, then $\pm\sqrt{\alpha}$ is a root of $p(x)$.

So then
$$\begin{array}{l} L = \mathbb{Q}(\sqrt{\alpha}) \\ | \quad \} \deg 2 \\ E = \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}$$

In particular E is the splitting field of a deg 4 polyn.
$\Rightarrow E$ is solvable by radicals. $\Rightarrow E/\mathbb{Q}$ is solvable ext.

Clearly L/E is also solvable by radicals (by above)

so then since $\mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/\mathbb{Q})$

$\Rightarrow \mathrm{Gal}(L/\mathbb{Q})$ is also solvable

(5) R - comm ring w/ 1. $\exists \sum x_i y_i = 1$ for some $y_i \in R$.

$A = \{(r_1 \dots r_n) \in R^n ; \sum x_i r_i = 0\}$, Show $R^n \simeq_R A \oplus R$, A has n gen. & when $R = F[x]$, F-field $\Rightarrow A_R$ is free of rank $n-1$.

If let $\varphi : R^n \twoheadrightarrow R$
$(r_1 \dots r_n) \mapsto \sum r_i x_i$

Then $\varphi(y_1 \dots y_n) = 1$ so φ is surjective and $\ker \varphi = A$.

So then since R is free, it is projective so that the s.e.s. splits

$$0 \to A \hookrightarrow R^n \twoheadrightarrow R \to 0$$

where $R^n = R \oplus A$

Now $\pi : R^n \sim R[x_1 \dots x_n] \twoheadrightarrow A$ so A has n-generators

And if $R = F[x] \Rightarrow R$ is a PID so by the fund. thm of f.g. mod over PID $\Rightarrow A \simeq tA \oplus R^k$

However $R^n \simeq A \oplus R \simeq tA \oplus R^{k+1} \Rightarrow tA = 0$ & $k+1 = n$, $k = n-1$

so $A \simeq R^{n-1} \Rightarrow \dim_R A = n-1$.

(6) p-prime, K ext of F_p of dim 72. $\Rightarrow$ $K = F_{p^{72}}$

(i) describe structure of $Gal(K/F_p)$

(ii) if $g(x) \in F_p(x)$ irred of deg 72, argue K is a splitting field of $g(x)$ over F_p.

(iii) which integers $d > 0$ have irreducibles in $F_p[x]$ of deg d that split in K.

If (i) Since K is a finite ext over a finite field then

$Gal(K/F_p)$ is cyclic $\Rightarrow$ $Gal(K/F_p) = \mathbb{Z}_{72}$

(ii) $g(x)$ irreducible over $\mathbb{F}_p$ $\Rightarrow$ if α is a root then $g(x)$ splits over $\mathbb{F}_p(\alpha)$. But then α has deg 72 $\Rightarrow [\mathbb{F}_p(\alpha) : F_p] = 72$

since extensions over finite fields are unique $\Rightarrow$ $\mathbb{F}_p(\alpha) = K$.

(iii) Now by the same logic if $d \mid 72$ then $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{72}}$

so any irreducible of deg $d \mid 72$ will split over $\mathbb{F}_{p^{72}}$.

Algebra Graduate Exam

Spring 2013

Work all the problems. Be as explicit as possible in your solutions, and justify your statements with specific reference to the results that you use. Partial credit will be given for partial solutions.

1. Let $p > 2$ be a prime. Describe, up to isomorphism, all groups of order $2p^2$.

2. Let R be a commutative Noetherian ring with 1. Show that every proper ideal of R is the product of finitely many (not necessarily distinct) prime ideals of R.
(Hint: Consider the set of ideals that are not products of finitely many prime ideals. Also, note that if R is not a prime ring then IJ=(0) for some non-zero ideals I and J of R)

3. In the polynomial ring $R = \mathbf{C}[x,y,z]$ show that there is a positive integer m, and polynomials f, g, h ∈ R such that

$$(x^{16}y^{25}z^{81} - x^7z^{15} - yz^9 + x^5)^m = (x - y)^3f + (y - z)^5g + (x + y + z - 3)^7h.$$

4. Let $R \neq (0)$ be a finite ring such that for any $x \in R$ there is $y \in R$ with $xyx = x$. Show that R contains an identity element and that, for a, b ∈ R, if ab=1 then ba=1.

5. Let $f(x) = x^{15} - 2$, and let L be the splitting field of f(x) over $\mathbf{Q}$.
a) What is $[L:\mathbf{Q}]$?
b) Show there exists a subfield F of degree 8 that is Galois over $\mathbf{Q}$.
c) What is $Gal(F/\mathbf{Q})$?
d) Show there is a subgroup of $Gal(L/\mathbf{Q})$ that is isomorphic to $Gal(F/\mathbf{Q})$.

6. Let $F/\mathbf{Q}$ be a Galois extension of degree 60, and suppose F contains a primitive ninth root of unity. Show $Gal(F/\mathbf{Q})$ is solvable.

7. Let n be a positive integer. Show that $f(x,y) = x^n + y^n + 1$ is irreducible in $\mathbf{C}[x,y]$.

4b) if $ab = 1$ w/ $\forall x \exists y \neq xyx = 1$ $\overset{\text{want}}{\Rightarrow}$ $ba = 1$

then consider $\varphi: R \to R$

$x \longmapsto xb$

then $\varphi(a) = ab = 1$ so $\varphi(ya) = y$ for any $y \in R$

hence φ is surjective. $\Rightarrow$ injective since R is finite

so $\ker \varphi = 0 \Rightarrow \varphi(x - xab) = \varphi(x - x) = 0$

so $\varphi(b - bab) = 0 \Rightarrow b(1 - ab) = 0$

$(1 - ba)b = 0$

$\Rightarrow \varphi(1 - ba) = 0$ since $\ker \varphi = 0$.

$\Leftrightarrow 1 - ba = 0 \Leftrightarrow ba = 1$

4a) R is a finite ring w/ $xyx = x$ $(\forall x \exists y)$

show $1 \in R$

R - commutative $\Rightarrow$ if if $xz = 0$ for $z \neq 0$

$\dashrightarrow xyxz = xz = 0$

$\varphi: R \to R$

$a \longmapsto xya$

$\varphi(x) = xyx = x$

$\Rightarrow \varphi(xa) = xyxa = xa$

$\varphi(ax) = xyax$

$\varphi(a) \cdot \varphi(x) = xya \cdot xyx$

Spring 2013

① $p>2$ prime. Describe all grps of order $2p^2$

Pf $n_p \equiv 1 \bmod p$ & $n_p = 1$ or $\not 2 \Rightarrow n_p = 1$ so $\exists P \trianglelefteq G$ w/ $|P| = p$.

now, let S - 2-sylowgroup. then consider $\varphi: \mathbb{Z}_2 \longrightarrow Aut(P)$.

CASE 1 $P = \mathbb{Z}_p \times \mathbb{Z}_p$, so $Aut(P) = GL_2(\mathbb{Z}/p)$ w/ order $(p^2-1)(p^2-p)$

so then $|Aut(P)| = (p+1)(p-1)^2 \cdot p$, so $2 \mid p+1$ & $2 \mid (p-1)$

In particular $\varphi(a)$ must have order 2, so $\varphi(a)$ must act under inversion, so if $\sigma: \underset{\langle a,b\rangle}{\mathbb{Z}/p \times \mathbb{Z}/p} \to \underset{\langle a,b\rangle}{\mathbb{Z}/p \times \mathbb{Z}/p}$; $\sigma(a,b) = (a,b)$
$= (a^{-1},b)$
$= (a,b^{-1})$
$= (a^{-1},b^{-1})$

for a total of 4 possibilities.

so $G = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes_\varphi \mathbb{Z}_2$.

CASE 2 $P = \mathbb{Z}_{p^2}$, so $Aut(P) = (\mathbb{Z}/p^2)^\times$ w/ order $p^2 - p = p(p-1)$

Now, again φ acts ... by inversion so $\sigma: \mathbb{Z}/p^2 \longrightarrow \mathbb{Z}/p^2$
$a \longmapsto a$ or a^{-1}.

three two choices for $G = P \rtimes_\varphi \mathbb{Z}_2$.

Thus we have a total of 5 choices for maps.

Now since all grps of order p^2 are abelian, we're done.

(3) $R = \mathbb{C}[x,y,z]$, Show $\exists\ m > 0$ and $f, g, h \in R$ s.t.

$$\underbrace{(x^{16}y^{25}z^{81} - x^7z^{15} - yz^9 + x^5)}_{g(x)}{}^m = (x-y)^3 f + (y-z)^5 g + (x+y+z-3)^7 h$$

Pf w.T.S. $g(x)^m \in Id((x-y)^3) + Id((y-z)^5) + Id((x+y+z-3)^7)$

$\Rightarrow g(x) \in \sqrt{\langle (x-y)^3, (y-z)^5, (x+y+z-3)^7 \rangle} = \sqrt{I}$

so if $Var(g(x)) \supseteq Var(I) \Rightarrow g(x) \in \sqrt{I}$ by Nullstellensatz

So then $Var(I) \Rightarrow x-y=0 \quad y-z=0 \quad x+y+z=3$

$x=y \quad y=z \Rightarrow 3z=3$

$z=1 \Rightarrow x,y=1$

So $Var(I) = \{(1,1,1)\}$

So $g(1,1,1) = 1-1-1+1 = 0 \Rightarrow g(x) \in \sqrt{I}$ ✓.

(4) $R \neq 0$ be a finite ring s.t. for any $x \in R$ $\exists y$ w/ $xyx = x$

Show R contains an identity 1 for $a, b \in R$ if $ab = 1 \Rightarrow ba = 1$.

Pf (a) ???

(b) Suppose $1 \in R$, Let $\varphi: R \to R$, $x \mapsto xb$. Then $\varphi(a) = ab = 1$

so for any $r \in R$

$\varphi(ra) = rab = r$

$\Rightarrow \varphi$ is surjective.

But R is a finite ring so φ is injective.

Thus $\varphi(a) = 0$ iff $a = 0 \Rightarrow \varphi(ab - ba) = abb - bab = b - b = 0$

$\Rightarrow ab - ba = 0$ so $ab = ba$.

spring 2013

② R comm. Noetherian ring

Show ∀ ideal (proper) in R can be the product of finitely many prime ideals

Pf Let S = {set of ideals that are not the product of finitely many prime ideals of R}.

Then since R is noetherian, all chains must terminate (so by noetherian induction / Zorn's lemma) ∃ a maximal element M ∈ S.

Now consider R/M. Clearly if I ∈ R/M ∋ I ≠ 0 then I ∉ S and thus I is the product of finitely many prime ideals.

If R/M is not prime ⇒ ∃ I, J ∋ I, J ≠ 0 but IJ = 0 in R/M.

That is, IJ = M. But M is not a finite product of prime ideals whereas I, J are ⇒⇐. Thus R/M must be prime.

However, since R is commutative ⇒ R/M is commutative.

Recall that a commutative ring is prime iff its zero ideal is a prime ideal.

Thus R/M prime ⇒ ∴ M is a prime ideal. ⇒⇐ since M ∈ S.

Thus S = ∅.

(5) $f(x) = x^{15} - 2$, L - splitting field of $f(x)$ over $\mathbb{Q}$.

(a) What is $[L : \mathbb{Q}]$

(b) Show $\exists$ subfield of degree 8 that is Galois over $\mathbb{Q}$.

(c) What is $Gal(F/\mathbb{Q})$

(d) Show $\exists$ subgp of $Gal(L/\mathbb{Q}) \simeq Gal(F/\mathbb{Q})$

Pf (a) $f(x) = x^{15} - 2 \Rightarrow x^{15} = 2$

$x = \sqrt[15]{2}\,\omega \leftarrow$ 15th root of unity.

So there $\exists\ \varphi(15) = \varphi(3)\cdot\varphi(5) = 2\cdot 4 = 8$ primitive roots of unity.

So then
$$\begin{array}{ccc} L = \mathbb{Q}(\omega, \sqrt[15]{2}) & & \\ | & \} \deg 15 & \\ F = \mathbb{Q}(\omega) & & \Rightarrow \quad [L : \mathbb{Q}] = 15 \cdot 8 \\ | & \} \deg 8 & \\ \mathbb{Q} & & \end{array}$$

(b) Clearly $\mathbb{Q}(\omega)$ is a subfield w/ min. poly $x^{15} - 1$ which is galois of deg $\varphi(15) = 8$

(c) $Gal(F/\mathbb{Q})$ is cyclic of degree 8 $\Rightarrow Gal(F/\mathbb{Q}) = \mathbb{Z}/8$

(d) Now intermediate field are in bijection w/ subgroups of $Gal(L/\mathbb{Q})$

In particular $\exists$ subgroup of index 8, $H \leq Gal(L/\mathbb{Q})$.

Furthermore, $\omega\sqrt[15]{2}$ has order 15 since $(\omega\sqrt[15]{2})^{15} \in \mathbb{Q}$ (15 is the smallest such number) so $[\mathbb{Q}(\omega\sqrt[15]{2}) : \mathbb{Q}] = 15$.

Thus $\mathbb{Q}(\omega\sqrt[15]{2}) \longleftrightarrow$ subgroup of $Gal(L/\mathbb{Q})$ of index 15

$\Rightarrow$ it has order 8.

Since $Gal(\mathbb{Q}(\omega)/\mathbb{Q}) = Gal(F/\mathbb{Q})$ $\Leftrightarrow$ normal subgroup of order 15

and $Gal(L/\mathbb{Q})/Gal(L/F) \simeq Gal(F/\mathbb{Q}) \simeq \mathbb{Z}/8$

Now $\exists$ natural embedding, $Gal(L/\mathbb{Q})/Gal(L/F) \hookrightarrow Gal(L/\mathbb{Q})$

$\Rightarrow H \in Gal(L/\mathbb{Q}) \Rightarrow H \simeq Gal(F/\mathbb{Q})$

(6) Let $F/\mathbb{Q}$ be galois of degree 60 w/ F containing a 9th root of unity. Show $Gal(F/\mathbb{Q})$ is solvable.

Pf if w. prim 9 root of $1 \Rightarrow \varphi(9) = \varphi(3^2) = 3^2 - 3 = 9 - 3 = 6$

so
$$\begin{array}{c} F \\ | \\ | \\ | \\ | \\ \mathbb{Q}(\omega) \\ | \\ | \\ \mathbb{Q} \end{array} \left\{ \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \end{array} \right. \begin{array}{l} 10 = 2 \cdot 5 \\ \\ \\ \\ \\ 6 \end{array}$$

Now $|Gal(\mathbb{Q}(\omega)/\mathbb{Q})| = 6 = 2 \cdot 3$.

So $n_3 = 1 \Rightarrow$ 7 normal by Syl 3 subgrp

So $0 \trianglelefteq N \trianglelefteq Gal(\mathbb{Q}(\omega)/\mathbb{Q})$

w/ $N \simeq \mathbb{Z}/3$. $\Rightarrow Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ is solvable.

Now $Gal(F/\mathbb{Q})/Gal(F/\mathbb{Q}(\omega)) \simeq Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ (*)

and $|Gal(F/\mathbb{Q}(\omega))| = 10 = 2 \cdot 5$ so again by Syl has a normal 5 subgrp $\Rightarrow$ so it is also solvable.

Thus $Gal(F/\mathbb{Q}(\omega))$ & $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$ are both solvable so by (*) $Gal(F/\mathbb{Q})$ is solvable

(7) $n > 0$, show $f(x,y) = x^n + y^n + 1$ is irreducible in $\mathbb{C}[x,y]$.

If consider $f(x,y) \in \mathbb{C}[x][y]$

so $f(x,y) = y^n + (x^n + 1)$.

Then over $\mathbb{C}$, $x^n + 1$ factors as n linearly independent irreducible factors, $x^n + 1 = \prod_{i=1}^{n} (x - \alpha_i)$ where $\alpha_i^n = -1$

Thus by eisenstein $x - \alpha_i$ is prime in $\mathbb{C}[x]$ (since irreducible)

but $(x-\alpha_i)^2 \nmid x^n + 1 \Rightarrow f(x,y)$ is irreducible.

Algebra Qualifying Exam - Fall 2013

1. Let H be a subgroup of the symmetric group S_5. Can the order of H be 15, 20 or 30?

2. Let R be a PID and M a finitely generated torsion module of R. Show that M is a cyclic R-module if and only if for any prime $\mathfrak{p}$ of R either $\mathfrak{p}M = M$ or $M/\mathfrak{p}M$ is a cyclic R-module.

3. Let $R = \mathbb{C}[x_1, \ldots, x_n]$ and suppose I is a proper non-zero ideal of R. The coefficients of a matrix $A \in M_n(R)$ are polynomials in $x_1, \ldots, x_n$ and can be evaluated at $\beta \in \mathbb{C}^n$; write $A(\beta) \in M_n(\mathbb{C})$ for the matrix so obtained. If for some $A \in M_n(R)$ and all $\alpha \in Var(I)$, $A(\alpha) = 0_{n\times n}$, show that for some integer m, $A^m \in M_n(I)$.

4. If R is a noetherian unital ring, show that the power series ring $R[[x]]$ is also a noetherian unital ring.

5. Let p be a prime. Prove that $f(x) = x^p - x - 1$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$. What is the Galois group? (Hint: observe that if α is a root of $f(x)$, then so is $\alpha + i$ for $i \in \mathbb{Z}/p\mathbb{Z}$.)

6. Let R be a finite ring with no nilpotent elements. Show that R is a direct product of fields.

7. Let $K \subset \mathbb{C}$ be the field obtained by adjoining all roots of unity in $\mathbb{C}$ to $\mathbb{Q}$. Suppose $p_1 < p_2$ are primes, $a \in \mathbb{C} \setminus K$, and write L for a splitting field of

$$g(x) = (x^{p_1} - a)(x^{p_2} - a)$$

over K. Assuming each factor of $g(x)$ is irreducible, determine the order and the structure of $Gal(L/K)$.

Fall 2013

① $H \leq S_5$, can H have order 15, 20, 30.

if $|H| = 20, 30, 15 \Rightarrow$ $[S_5, H] = 6$ or $[S_5, H] = 4$ or $[S_5, H] = 8$

However by #5 on spring 2014 $[S_5, H] = 1, 2$ or 5.

Hence these cannot occur.

② R - PID, M - fig. torsion module. M is a cyclic R module iff for any prime $p \in R$ either $pM = M$ or M/pM is cyclic.

$(\Rightarrow)$ If M is acyclic R module $\Rightarrow M \simeq R/\text{ann}(M) \simeq Rx$.

where $\text{ann}(M) = \{r \in R ; rx = 0\}$

But also $M \simeq M_{(p)} \leftarrow$ p-primary components; $M_{(p)} = \{m \in M ; p^n m = 0 \text{ some } n\}$

so then for any $q \neq p$ $qM = M$ since $q^n m \neq 0$

if $q = p$ then M/pM will be cyclic since M itself is cyclic.

$(\Leftarrow)$ if $pM = M$ or M/pM is cyclic for any given $p \in R$ then

Given $M \simeq M_{(p_1)} \oplus \cdots \oplus M_{(p_n)}$, then for $q \neq p_i$ obs $qM = M$ so suppose $q = p_i$

$M/p_i M = M_{(p_1)} \oplus \cdots \oplus M_{p_i}/p_i M \oplus \cdots N_{(p_n)}$ being cyclic

$\Rightarrow M/p_i M \simeq M_{(p_i)}/p_i M \Rightarrow M_{(p_u)} = 0 \ \forall \ u \neq i \Rightarrow M \simeq M_{(p_i)}$

so M is cyclic

(3) $R = \mathbb{C}[x_1, \dots x_n]$, I nonzero ideal in R.

If $A \in M_n(R)$ & $\forall \alpha \in \mathrm{Var}(I)$; $A(\alpha) = 0$, show $\exists m \geq A^m \in M_n(I)$

~~If~~ Since $R = \mathbb{C}[x \dots x_n]$ & $\mathbb{C}$ is alg. closed, R is noeth by Hilbert Basis theorem.

Now $A = (a_{ij})$ w/ $a_{ij} \in R$, then $a_{ij}(\beta) = 0$ $\forall \beta \in \mathrm{Var}(I)$

$\Rightarrow \mathrm{var}(I) \subseteq \bigcap_{ij} \mathrm{var}(a_{ij}) \Rightarrow \mathrm{Id}\,\mathrm{var}(I) \supseteq \bigcup_{ij} \mathrm{Id}(a_{ij}) = \bigcup_{ij} (a_{ij}) \ni a_{ij}$

so by Null stellensatz $\sqrt{I} \ni a_{ij}$ $\forall ij$ $\Rightarrow$ $\exists m_{ij} \geq a_{ij}^{m_{ij}} \in I$.

Now, R is noeth, so $\sqrt{I}$ is fin generated, $\sqrt{I} = \langle f_1, \dots, f_n \rangle$

w/ $f_i^{m_i} \in I$ some m_i. Let $M = \max\{m_i\}_{i=1}^n$, so $f_i^M \in I$ $\forall i$.

Now $a_{ij} \in \sqrt{I} \Rightarrow$ $a_{ij} = \sum_{k=1}^{n} c_{ij}^k f_k$, so $a_{ij}^s = \left(\sum^n c_{ij}^k f_k\right)^s$

$= \sum_{l=1}^{n \cdot s} B_l f_1^{\ell_1} \cdots f_n^{\ell_n} \geq \sum \ell_i = s$, so if $f_i^M \in I$, let $S = M \cdot k$

then atleast one $f_i^{k_i} \in I$ So $a_{ij}^s \in I$. Thus if let $m = n^2 \cdot M \cdot k$

then $A^m \in M_n(I)$.

(4) R - noetherian $\Rightarrow R[x]$ is noetherian.

Same as hilbert basis theorem proof but look at minimal coefficient (degree) instead of maximal.

(5) p - prime, Prime $f(x) = x^p - x - 1$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$

What is the Galois gp?

If observe that if $f(\alpha) = 0 \Rightarrow \alpha^p - \alpha - 1 = 0$

then $f(\alpha+n) = (\alpha+n)^p - \alpha - n - 1 = \alpha^p + n^p - \alpha - n - 1 = n^p - n = 0$

since $n \in \mathbb{Z}/p$ so $n^p = n$.

Thus the roots of $f(x)$ are precisely $\{\alpha + n \mid n \in \mathbb{Z}/p\mathbb{Z}\}$.

Now consider the frobenius automorphism $\sigma: F_{p^i} \longrightarrow F_{p^i}$

$x \longmapsto x^p$

then $\sigma(\alpha) = \alpha^p = \alpha + 1$ so σ acts transitively on the roots of f & fixes $\mathbb{Z}/p\mathbb{Z}$. In particular the roots of f are precisely

$\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \cdots, \sigma^{p-1}(\alpha)\}$, so by irreducibility of f we obtain $\mathrm{Gal}(f(x)) = \langle \sigma \rangle = \mathbb{Z}/p\mathbb{Z}$

6) R finite ring w/ no nilpotent elements. Show $R = \bigoplus F_i$ - fields

Pf R finite $\Rightarrow$ artinian $\Rightarrow$ $J(R)$ is nilpotent

$Nil(R) = 0$ + art $\Rightarrow$ $J(R) = 0$

$J(R) = 0$ + art $\Rightarrow$ R is semisimple $\Rightarrow$ can apply Artin Wedd.

So $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$

Since $Nil(R) = 0$ $\Rightarrow$ $n_i = 1$ $\forall i$

since R is finite $\Rightarrow$ D_i are finite $\Rightarrow$ D_i are fields by Little Wedderburn.

$\Rightarrow$ $R \cong F_1 \times \cdots \times F_k$.

(7) $K = \mathbb{Q}$ (roots of unity), let $\alpha \in \mathbb{C} \setminus K$, let L - splitting field of $g(x) = (x^{p_1} - a)(x^{p_2} - a)$ over K.

if $x^{p_i} - a$ is irred, determine order & structure of $Gal(L/K)$

Pf $x^{p_i} - a = 0$ ...

$x^{p_i} = a$

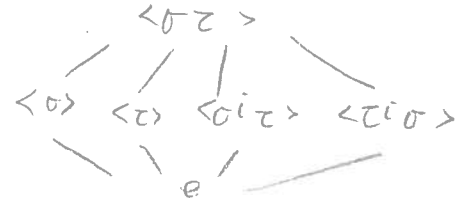
$x = \sqrt[p_i]{a}\,\omega$ ω - primitive p_ith root of unity.

So $L = K(\sqrt[p_1]{a}, \sqrt[p_2]{a})$, so then $K \overset{\sim}{-} K(\sqrt[p_1]{a}) \overset{\sim}{-} K(\sqrt[p_1]{a}, \sqrt[p_2]{a})$

so $[L : K] = p^2$, now let $\sigma : \sqrt[p_1]{a} \longmapsto \sqrt[p_1]{a}\,\omega$ $\tau : \sqrt[p_2]{a} \longmapsto \sqrt[p_2]{a}\,\eta$

then $|\langle\sigma\rangle| = p_1$, $|\langle\tau\rangle| = p_2$ and so $\langle\sigma, \tau\rangle$ generate L.

? $\sigma\tau\sigma^{-1} = \tau$, Hence the structure is



Algebra Exam September 2014

Show your work. Be as clear as possible. Do all problems.
Hand in solutions in numerical order.

1. Let G be a group of order 56 having at least 7 elements of order 7. Let S be a Sylow 2-subgroup of G.

   (a) Prove that S is normal in G and $S = C_G(S)$.

   (b) Describe the possible structures of G up to isomorphism. (Hint: How does an element of order 7 act on the elements of S?)

2. Show that a finite ring with no nonzero nilpotent elements is commutative.

3. If $R = M_n(\mathbb{Z})$, and A is an additive subgroup of R, show that as additive subgroups $[R : A]$ is finite if and only if $R \otimes_{\mathbb{Z}} \mathbb{Q} = A \otimes_{\mathbb{Z}} \mathbb{Q}$.

4. Let R be a commutative ring with 1, n a positive integer and $A_1, \ldots A_k \in M_n(R)$. Show that there is a noetherian subring S of R containing 1 with all the $A_i \in M_n(S)$.

5. Let $R = \mathbb{C}[x, y]$. Show that there exists a positive integer m such that $(x + y)(x^2 + y^4 - 2))^m$ is in the ideal $(x^3 + y^2, y^3 + xy)$.

6. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $n \geq 5$. Let L be the splitting field of f and let $\alpha \in L$ be a zero of f. Given that $[L : Q] = n!$, prove that $\mathbb{Q}[\alpha^4] = \mathbb{Q}[\alpha]$.

Fall 2014

① $|G| = 56$ having atleast 7 elmts of order 7

S-sylow 2 subgrp of G.

(a) Prove S is normal in G $\Leftrightarrow$ $S = C_G(S)$

(b) Describe all possible structures of G up to iso.

Pf (a) $|G| = 7 \cdot 8 = 7 \cdot 2^3$

now $n_7 \equiv 1 \bmod 7$ & $n_7 = 1, \cancel{2}, \cancel{4}, 8$ if $n_7 = 1 \Rightarrow$ only 6 elmts of ord 7 $\Rightarrow \Leftarrow$.

so $\boxed{n_7 = 8}$

if $n_2 \neq 1$, then $n_2 = 7$

so that there are $7(8-1) = 7(7) = 49$ nontrivial elmts of order 2^i

But since $n_7 = 8 \Rightarrow 8(7-1) = 8 \cdot 6 = 48$ elmts of order 7

$\Rightarrow 56 - 48 - 1 = 7$ - elmts l/t (nontrivial) so $n_2 \neq 7$

so $n_2 = 1 \Rightarrow |S| = 8$ & $S \trianglelefteq G$.

...

Now, if P is a sylow 7 subgrp, consider the actin P on S.

$\Rightarrow \alpha : P \times S \to S$ then by the orbit stabilizer formula

$(p, s) \mapsto psp^{-1}$

$7 = |P| = |O_s||Stab_s|$ for any $s \in S$.

so then $|O_s| = 1$ or 7. If $|O_s| = 7 \Rightarrow$ for any $s, \tilde{s} \in S \; \exists p \Rightarrow \tilde{s} = p s p^{-1}$

$\Rightarrow ord(s) = ord(\tilde{s}) \Rightarrow$ since S must contain an elmt of order 2 (p-grp) $\Rightarrow S = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

if $|O_s| = 1 \Rightarrow s = psp^{-1} \Rightarrow sp = ps \; \forall s, \forall p$

so $G = P \times S \Rightarrow \Leftarrow$ since

P is not normal. so $S = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Hence S is abelian & thus $S \subseteq C_G(S) = \{g \in G \mid gsg^{-1} = s \ \forall s \in S\}$

Now clearly if $C_G(S) \neq S$ then $C_G(S) = G$.

But then $G = P \times S \Rightarrow \in$. so $C_G(S) = S$.

(b) since $S = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ & $P = \mathbb{Z}_7$

then $G \cong P \times S$ or $G = P \rtimes S$ where

($P \times S$ cannot be since $P \not\trianglelefteq G$)

$\varphi : P \to \mathrm{Aut}(S) = GL_3(\mathbb{Z}_2)$ $(p:7)$

$\mathrm{Aut}(S)$: $a \mapsto a, b, c$; $b \mapsto a, b, c$; $c \mapsto a, b, c$

$p^3 : p^1 (p^3 - p)(p^3 - \cdot)$

$(\cdot 4)(\cdot 6)(7)$

$2^4 - 7$

s^3 $n_7 = 1 \bmod 7$

$n_7 = 1, 2, 4, 8$ (8)

$1, 2, 16, 24$

(2) R - finite ring w/ $Nil(R) = 0 \Rightarrow R$ is comm.

If R finite $\Rightarrow R$ is artinian $\Rightarrow J(R)$ is nilpotent

$Nil(R) = 0 \Rightarrow R$ is Jacobson semisimple & artinian

$\Rightarrow R$ is semisimple $\Rightarrow$ apply artin Wedderburn.

$\Rightarrow R = M_{n_1}(\Delta_1) \times \cdots \times M_{n_k}(\Delta_k)$

but $n_i = 1 \ \forall i$ since $Nil(R) = 0$ & R is finite $\Rightarrow \Delta_i$ is finite

$\Rightarrow$ field by little Wedderburn.

$\Rightarrow R = F_1 \times \cdots \times F_k \leftarrow$ commutative

4) R – commutative ring w/ 1. $n>0$

$A_1, \dots, A_k \in M_n(R)$

Show $\exists$ noetherian subring S of R $\ni$ $1 \in S$ & all the $A_i \in M_n(S)$

If Since R is commutative over some field K, then let $S = \langle \{a_{ij}^p\} \rangle$ be the subring gen. by all entries of A_p $p \in \{1, \dots, k\}$. Then S is fin. gen. over a field $\Rightarrow$ S is noetherian by Hilbert Basis theorem. (Since $F[x_1, \dots, x_{kn^2}] \twoheadrightarrow S$) so then $A_p \in M_n(S)$ $\forall p$.

(3) $R = M_n(\mathbb{Z})$, A - additive subgroup of R. Show $[R : A]$ is finite iff $R \otimes_{\mathbb{Z}} \mathbb{Q} = A \otimes_{\mathbb{Z}} \mathbb{Q}$.

Since $R = M_n(\mathbb{Z})$, we can consider $R = \begin{bmatrix} \mathbb{Z} & \cdots & \mathbb{Z} \\ \mathbb{Z} & & \mathbb{Z} \end{bmatrix}$ w/

$A = \begin{bmatrix} m_1\mathbb{Z} & \cdots & m_n\mathbb{Z} \\ & & \\ & & m_{n^2}\mathbb{Z} \end{bmatrix}$. Then $[R : A] < \infty$ iff $[\mathbb{Z} : m_i\mathbb{Z}] < \infty$ $\forall i$

iff $m_i \geq 1$ $\forall i$ iff $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = m_i\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$ iff $R \otimes_{\mathbb{Z}} \mathbb{Q} \simeq A \otimes_{\mathbb{Z}} \mathbb{Q}$.

(5) $R = \mathbb{C}[x,y]$. Show $(x+y)\cdot(x^2+y^4-2) \in \sqrt{I}$

$I = \langle x^3+y^2,\ y^3+xy \rangle$

If Consider $J = \langle (x+y)(x^2+y^2-1) \rangle = \langle p(x) \rangle$

Then $p(x) \in \sqrt{I} = Id(var(I))$ - Hollstellensatz

iff $\langle p(x) \rangle = J \subseteq \sqrt{I}$

iff $var(J) \supseteq var(I)$

so if $x^3+y^2 = 0$ & $y^3+xy = 0$

$\Rightarrow -x^3 = (-x)^3 = y^2$ $\quad y^3 = -xy \Rightarrow y = 0$

$\downarrow y \neq 0$

$y^2 = -x$

if $y = 0 \Rightarrow x = 0$

if $y = -x \Rightarrow -x^3 = (-x)^2 = x^2$

$\Rightarrow x = 0$ or $x \neq 0 \Rightarrow -x = 1 \Rightarrow x = -1,\ y = 1$

$\Downarrow$

$y = 0$

so

$Var(I) = \{(0,0), (-1,1)\}$.

Now $p(0,0) = 0$ & $p(-1,1) = 2(1+1-2) = 0$. so $p(x)^m \in I$.

Sep, Fall 2014

(6) $f(x) \in \mathbb{Q}[x]$ irred of deg $n \geq 5$. L - split field & let $\alpha \in L$, zero of f

If $[L:\mathbb{Q}] = n!$ prove $\mathbb{Q}[\alpha^4] = \mathbb{Q}[\alpha]$.

pf Recall: $\exists$ no subgroups of S_n $\Rightarrow$ $3 \leq [S^n : H] < n$ for $n \geq 5$.

Since α has min polyn. of degree $n \Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}] = n$ & $\mathbb{Q}(\alpha^4) \subseteq \mathbb{Q}(\alpha)$.

Now by galois correspondence deg $\mathbb{Q}(\alpha^4)/\mathbb{Q}$ = index of some $S \leq Gal(L/\mathbb{Q}) = S^n$

(Clearly since f has degree n & $Gal(L/\mathbb{Q}) \hookrightarrow S^n$ then $Gal(L/\mathbb{Q}) = S^n$).

So then, deg $\mathbb{Q}(\alpha^4)/\mathbb{Q}$ must be 1, 2 or n by the remark above.

Clearly if degree $= n \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^4)$ since $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha^4)][\mathbb{Q}(\alpha^4):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = n$

if degree $= 1$ then $\alpha^4 \in \mathbb{Q}$, but then $x^4 - \alpha^4$ is the minimal polyn. of α over $\mathbb{Q}$ $\Rightarrow\Leftarrow$ since $n \geq 5$.

So lastly if degree $= 2$ then $\alpha^4 = a + c\sqrt{b}$ for some $a, c, b \in \mathbb{Q}$

$\Rightarrow \alpha = \sqrt[4]{a + c\sqrt{b}}$ $\leftarrow$ solvable by radicals.

But $n \geq 5$ so f is not solvable by radicals $\Rightarrow\Leftarrow$.

Thus deg $= n \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^4)$.

ALGEBRA QUALIFYING EXAM SPRING 2014

Work all of the problems. Justify the statements in your solutions by reference to specific results, as appropriate. Partial credit is awarded for partial solutions. The set of rational numbers is $\boldsymbol{Q}$, and set of the complex numbers is $\boldsymbol{C}$. *Hand in solutions in order of the problem numbers.*

1. Let L be a Galois extension of a field F with $\mathrm{Gal}(L/F) \cong D_{10}$, the dihedral group of order 10. How many subfields $F \subseteq M \subseteq L$ are there, what are their dimensions over F, and how many are Galois over F?

2. Up to isomorphism, using direct and semi-direct products, describe the possible structures of a group of order $5 \cdot 11 \cdot 61$.

3. Let I be a nonzero ideal of $R = \boldsymbol{C}[x_1, \ldots, x_n]$. Show that R/I is a finite dimensional algebra over $\boldsymbol{C}$ if and only if I is contained in only finitely many maximal ideals of R.

4. Let R be a commutative ring with 1, and M a noetherian R module. For N a noetherian R module show that $M \otimes_R N$ is a noetherian R module. When N is an artinian R module show that $M \otimes_R N$ is an artinian R module.

5. For $n \geq 5$ show that the symmetric group S_n cannot have a subgroup H with $3 \leq [S_n : H] < n$ ($[S_n : H]$ is the index of H in S_n).

6. Let R be the group algebra $\boldsymbol{C}[S_3]$. How many nonisomorphic, irreducible, left modules does R have and why?

7. Let each of $g_1(x), g_2(x), \ldots, g_n(x) \in \boldsymbol{Q}[x]$ be irreducible of degree four and let L be a splitting field over $\boldsymbol{Q}$ for $\{g_1(x), \ldots, g_n(x)\}$. Show there is an extension field M of L that is a radical extension of $\boldsymbol{Q}$.

Spring 2014

① $Gal(L/F) = D_{10}$; F = field

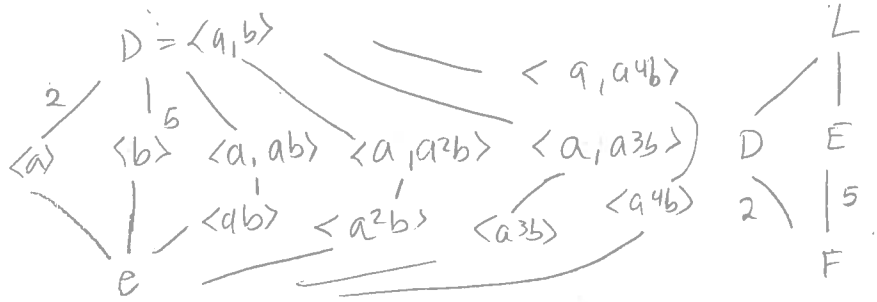
How many subfields $F \subseteq M \subseteq L$ are there? w/ what dimensions?

How many are galois?

If $D_{10} = \langle a, b \mid a^5 = e,\ b^2 = e,\ bab^{-1} = a^{-1} \rangle$

subfields of $F \subseteq M \subseteq L$ are in bij. w/ subgroups of D_{10}

now, then:



where $[L:D] = 2$ since subgroups of D_{2n} have the form $\langle a^d \rangle$ w/ $d|n$ & $\langle a^d, a^r b \rangle$ w/ $0 \le r < d$.

⇒ 10, nontrivial proper subgrps total.

Now galois ext $\leftrightarrow$ normal subgrps of D.

But by Sylow thms $\exists$ 5 sylow 2-subgrp's, so none of them are normal.

Thus $\langle a \rangle$ is normal (index 2) so only D is galois.

2) $|G| = 5 \cdot 11 \cdot 61$ Describe structure

Pf $n_{61} = 1$, so $\exists\ P \trianglelefteq G \Rightarrow |P| = 61$.

$5 \cdot 61 = 5 \cdot (-5) \equiv -25 \equiv 3 \bmod 11$

$n_{11} \equiv 1 \bmod 11$, $n_{11} = 1, 8, 61, 5 \cancel{61}$

so $n_{11} = 1 \Rightarrow \exists\ Q \trianglelefteq G \Rightarrow |Q| = 11$.

Thus $PQ \cong P \times Q \trianglelefteq G$.

Now let M be a subgp of S subgp. Then let $\varphi: M \longrightarrow Aut(P \times Q) \cong \mathbb{Z}_{10} \times \mathbb{Z}_{60}$

Then $\varphi(a)^5 = 1 \Rightarrow (0, 2, 4, 6, 8) \times (12, 24, 36, 48, 0)$

So then let $\phi: P \times Q \to P \times Q$
$(c, d) \mapsto (c^i, b^j)$ w/ $i^5 \equiv 1 \bmod 11$ $j^5 \equiv 1 \bmod 61$

then $i = 4$, then $4^5 = (2^5)^2 \equiv (1)^2 \equiv 1 \bmod 11$ (then $i^k \equiv 1 \bmod 11\ \forall k$)
and $j = \beta$ some β.

Then $G = \langle a, b, c \mid a^5 = b^{11} = c^{61} = e,\ aba^{-1} = b^{4^i},\ aca^{-1} = c^{\beta^k},\ bcb^{-1} = c \rangle$

(3) Let I be nonzero ideal of $R = \mathbb{C}[x_1 \cdots x_n]$. Show R/I fin dim alg over $\mathbb{C}$ iff $I \subseteq$ finitely many max ideals of R.

Pf $R = \mathbb{C}[x_1 \cdots x_n]$ is Noetherian & a UFD.

($\Rightarrow$) R/I has fin. dim as an alg over $\mathbb{C}$ then R/I is artinian and commutative. Thus R/I has finitely many max ideals.

By the correspondence theorem $\Rightarrow \exists$ finitely many max ideals

$I \subseteq N \subseteq R \Rightarrow I \subseteq \bigcap^{n} M_\alpha$ finitely many max ideals.

($\Leftarrow$) Suppose $I \subseteq$ finitely many max ideals.

If $I \subseteq \bigcap^{k} M_\alpha \Rightarrow \sqrt{I} \subseteq \bigcap^{k} M_\alpha$

since $var(I) \supseteq \bigcup^{k} var(M_\alpha) \Rightarrow \sqrt{I} \subseteq Id(\bigcup^{k} var(M_\alpha)) = \bigcap^{k} M_\alpha$.

So suppose $I = \sqrt{I}$.

Then max ideals in R have the form $\langle x-a \rangle$ for some $a \in \mathbb{C}^n$

so max ideals $\overset{bij}{\Longleftrightarrow}$ pts in $\mathbb{C}^n$.

Furthermore, $var(I) = \{a_1, \ldots\} = \bigcup \{a_i\} = \bigcup var(\langle x-a_i \rangle) = var(\cap M_\alpha)$

where $I \subseteq M_\alpha$. Thus $var(I) < \infty$.

But then: $R/\sqrt{I} = R/Id(var(I)) = R/Id(var(\cap M_\alpha)) = R/\cap M_\alpha$

since each $M_\alpha \cap M_\beta = \phi$ $= R/\bigcap^{k} M_\alpha = \prod^{k} R/M_\alpha \cong \mathbb{C}^k$ since $R/M_\alpha \cong \mathbb{C}$

↑ by the Chinese remainder thm

Thus, $R/\sqrt{I}$ has finite dim over $\mathbb{C}$.

Now since R is noetherian then all ideals are fin. gen, so then $\sqrt{I} \supseteq I$ are both fin. gen. in particular $I \subseteq \sqrt{I}$ so that $\sqrt{I}/I$ has finite dim over $\mathbb{C} \Rightarrow R/\sqrt{I}/\sqrt{I}/I \cong R/I$ is fin. dim over $\mathbb{C}$.

(5) $n \geq 5$, Show S_n cannot have a subgp of index $3 \leq [S_n : H] < n$

Pf Recall that for $n \geq 5$ A_n is simple and the only normal subgroups of S_n are $1, A_n, S_n$.

So if $H \leq S_n$ w/ index $m \Rightarrow 3 \leq m < n \Rightarrow H \neq S_n, A_n, \{0\}$.

Then consider $H \cap A_n \trianglelefteq A_n$, A_n is simple so $H \cap A_n = A_n$ or $H \cap A_n = \{0\}$

if $H \cap A_n = A_n \Rightarrow A_n \leq H \leq S_n \Rightarrow H = S_n \Rightarrow\Leftarrow$.

so $H \cap A_n = \{0\}$.

So consider rep'n of cosets $S_n \xrightarrow{\phi} S_m \Rightarrow \ker\phi \leq H$.

Then $\ker\phi \trianglelefteq S_n \Rightarrow \ker\phi = 0, S_n, A_n$.

But $A_n \nleq H$ and $S_n \nleq H \Rightarrow \ker\phi = 0$. So $S_n \hookrightarrow S_m$ w/ $m < n$.

$\Rightarrow\Leftarrow$. So H cannot exist.

(6) $R = \mathbb{C}S_3$, How many nonisomorphic, irreducible left modules does it have & why?

Pf By Maschke's theorem: $|G| = n_1^2 + n_2^2 + \cdots + n_k^2$ where $k = \#$ of irreducible left modules.

Since R is semisimple ($\because \mathbb{C}$ is alg closed) then $R = M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$

Now $n_1 = 1 \Rightarrow 6 = 1 + n_2^2 + n_3^2 + \cdots + n_k^2$

Furthermore, R cannot be abelian since S_3 is not, & $k = \#$ of conjugacy classes of $S_3 = 3$. So $6 = 1 + 1 + 4 \Rightarrow \mathbb{C}S_3 = \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$

So then R has exactly 2 nonisomorphic irreducible left modules $\mathbb{C} \not\cong M_2(\mathbb{C})$.

Spring 2014

④ R - com. ring w/ 1, M noetherian R module.
N - noetherian R-module; Show $M \otimes_R N$ is noeth. R-module
When N is artinian R-module show that $M \otimes_R N$ is artinian R-module.

Pf If M is noetherian, then all ideals are finitely generated (in particular $M \subseteq M$)
Thus $\exists\ \phi: R^n \twoheadrightarrow M$ (since M is an ideal in itself we can consider
$(m_1) \subseteq (m_1, m_2) \subseteq \dots = (m_1, m_2, \dots, m_k) = (m_1, \dots m_{k+1})$ where $m_i \in M \setminus \{m_1, \dots m_{i-1}\}$
By noetherianess this must terminate $\Rightarrow$ M is f.g.).
So then $N^n \simeq_R R^n \otimes_R N \twoheadrightarrow M \otimes_R N \Rightarrow M \otimes_R N$ is a quotient of N^n.
Thus if N is artinian/noetherian so is $N^n \Rightarrow$ so is $M \otimes_R N$.

Lemma: R - artinian + commutative $\Rightarrow \exists$ only finitely many max ideals.

Pf Suppose not. Then $\exists\ \{M_i\}_{i=1}^{\infty}$ max ideals, all distinct.
So consider $M_1 \supseteq M_1 \cdot M_2 \supseteq \dots \Rightarrow m_1 \dots m_k = m_1 \dots m_{k+1}$ since R artinian.
Thus $m_1 + m_{k+1} = R$ since m_1, m_k are relatively prime & maximal.
So then $m_1 m_2 \dots m_k + m_2 \dots m_{k+1} = m_2 \dots m_k$; by assumption
$m_1 \dots m_{k+1} = m_1 \dots m_k$ (* by commutativity) so $\Rightarrow m_1 \dots m_{k+1} + m_2 \dots m_{k+1} = m_2 \dots m_k$
& $m_1 \dots m_{k+1} \subseteq m_2 \dots m_{k+1} \Rightarrow m_2 \dots m_{k+1} = m_2 \dots m_k$
Repeating this $\Rightarrow m_k m_{k+1} = m_k \Rightarrow m_k \subsetneq m_{k+1}$ which contradicts maximality. So $\exists$ only finitely many.

(7) $g_1, \dots, g_n \in \mathbb{Q}[x]$ irreducible of degree 4. Let L splitting field over $\mathbb{Q}$ for $\{g_i(x)\}$. Show $\exists$ ext field M of L s.t. M is a radical ext of $\mathbb{Q}$

Pf
M
|
L
|
$\mathbb{Q}$

, Since each g_i has deg 4 $\Rightarrow$ each g_i is solvable by radicals so that $\mathbb{Q}$(roots of g_i) is solvable by radicals, i.e. a radical extension. Let $\{\alpha_k^i\}_{k=1}^4$ denote roots of g_i

But then $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_k^1) \subseteq \mathbb{Q}(\alpha_k^1, \alpha_k^2) \subseteq \dots = \mathbb{Q}(\alpha_k^1, \dots, \alpha_k^n) = L$

But each extension was solvable by radicals $\Rightarrow$ L is solvable by radicals $\Rightarrow$ L is a radical ext of $\mathbb{Q}$.

(7) $g_1, \dots, g_n \in \mathbb{Q}[x]$ irreducible of degree 4. Let L splitting field over $\mathbb{Q}$ for $\{g_i(x)\}$. Show $\exists$ ext field M of $L \supset M$ is a radical ext of $\mathbb{Q}$

Pf
M
|
L
|
$\mathbb{Q}$

, Since each g_i has deg 4 $\Rightarrow$ each g_i is solvable by radicals so that $\mathbb{Q}$(roots of g_i) is solvable by radicals, i.e. a radical extension. Let $\{\alpha_k^i\}_{k=1}^4$ denote roots of g_i

But then $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_k^1) \subseteq \mathbb{Q}(\alpha_k^1, \alpha_k^2) \subseteq \dots = \mathbb{Q}(\alpha_k^1, \dots, \alpha_k^n) = L$

But each extension was solvable by radicals $\Rightarrow$ L is solvable by radicals $\Rightarrow$ L is a radical ext of $\mathbb{Q}$.

Spring 2014

(5) $n \geq 5$ show S_n cannot have subgp. of order H w/

$$3 \leq [S_n : H] < n$$

- the only normal subgps of S_n are $1, A_n, S_n$
- A_n is simple for $n \geq 5$.

Suppose H has index m w/ $n \geq m \geq 3$

Then $H \cap A_n \trianglelefteq A_n \Rightarrow H \supseteq A_n$ or $H \cap A_n = \{0\}$.

$\Downarrow$

$H = S_n \Rightarrow \Leftarrow$

Note since A_n has index 2 in S_n for $n \geq 3$ then $A_n \neq H$.

Now, consider $\varphi : S_n \to S_m$ s $\ker \varphi \leq H$ (Rep'n of cosets)

Then, $\ker \varphi \trianglelefteq S_n$ so $\ker \varphi = 1, A_n, S_n$.

By above $\ker \varphi \neq A_n \Rightarrow A_n \leq H$

if $\ker \varphi = S_n \Rightarrow H = S_n \Rightarrow$ index $H < n$.

so $\ker \varphi = 1 \Rightarrow \varphi$ is injective $\Rightarrow S_n \hookrightarrow S_m$ w/ $n < m$.

$\Rightarrow \Leftarrow$.

...

Thus such an H cannot exist.

Spring 2014

(5) $n \geq 5$ show S_n cannot have subgp. of order H w/

$$3 \leq [S_n : H] < n$$

- the only normal subgps of S_n are $1, A_n, S_n$
- A_n is simple for $n \geq 5$.

Suppose H has index m w/ $n \geq m \geq 3$

Then $H \cap A_n \trianglelefteq A_n \Rightarrow H \supseteq A_n$ or $H \cap A_n = \{1\}$.

$\Downarrow$

$H = S_n \Rightarrow \Leftarrow$

Note since A_n has index 2 in S_n for $n \geq 3$ then $A_n \neq H$.

Now, consider $\varphi : S_n \to S_m$ s $\ker \varphi \leq H$ (Rep'n of cosets)

Then, $\ker \varphi \trianglelefteq S_n$ so $\ker \varphi = 1, A_n, S_n$.

By above $\ker \varphi \neq A_n \Rightarrow A_n \leq \ker H$

if $\ker \varphi = S_n \Rightarrow H = S_n \Rightarrow$ index $H < n$.

so $\ker \varphi = 1 \Rightarrow \varphi$ is injective $\Rightarrow S_n \hookrightarrow S_m$ w/ $n < m$.

$\Rightarrow \Leftarrow$.

Thus such an H cannot exist.

Spring 2014

(5) $n \geq 5$ show S_n cannot have subgp. of order H w/

$$3 \leq [S_n : H] < n$$

- the only normal subgps of S_n are $1, A_n, S_n$
- A_n is simple for $n \geq 5$.

Suppose H has index m w/ $n > m \geq 3$

Then $H \cap A_n \trianglelefteq A_n \Rightarrow H \supseteq A_n$ or $H \cap A_n = \{e\}$.

$\Downarrow$

$H = S_n \Rightarrow \Leftarrow$

Note since A_n has index 2 in S_n for $n \geq 3$ then $A_n \neq H$.

Now, consider $\varphi : S_n \to S_m$ s $\ker \varphi \leq H$ (Rep'n of cosets)

Then, $\ker \varphi \trianglelefteq S_n$ so $\ker \varphi = 1, A_n, S_n$.

By above $\ker \varphi \neq A_n \Rightarrow A_n \leq H$

if $\ker \varphi = S_n \Rightarrow H = S_n \Rightarrow$ index $H < n$.

so $\ker \varphi = 1 \Rightarrow \varphi$ is injective $\Rightarrow S_n \hookrightarrow S_m$ w/ $n < m$.

$\Rightarrow \Leftarrow$.

...

Thus such an H cannot exist.