$gcd(n,m)=1 \Rightarrow an + bm = 1$

$(x \otimes y) \in \mathbb{Z}_n \otimes \mathbb{Z}_m$

$(an + bm)(x \otimes y) = (x \otimes y)$

$an(x \otimes y) + bm(x \otimes y) = (x \otimes y)$

$\Rightarrow (x \otimes y) = 0$

Algebra Qualifying Exam -Spring 2010

1. Let f(x)= x[illegible] +3 □ Q[x]. Show that the Galois group of f is S[illegible].

2. (a) Let G be a group of order pqr, where p<q<r are primes. Show that G contains a normal subgroup of index p.
(b) Determine up to isomorphism all groups of order 3 · 7 · 13.

3. Let R be a commutative Noetherian ring, and let I, J, and K be ideals of R. We say I is irreducible if I = J ∩ K ® I = J, or I = K.
(a) Show that every ideal of R is a finite intersection of irreducible ideals.
(b) Show that every irreducible ideal is primary. (An ideal I of R is primary if R/I ≠ 0, and every zero-divisor in R/I is nilpotent.)

4. Let A be a finite-dimensional algebra ever a field K, such that for every a □ A, a²= a. Show that A is a direct product (sum?) of fields. Which fields can arise?

5. Let G and H be finitely generated abelian groups such that G □$_Z$ H = 0. Show that G and H are finite and have relatively prime orders.

6. Let S and T be diagonalizable endomorphisms of a finite dimensional complex vector space. If S and T commute show that they are polynomials in each other.

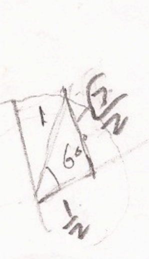
7. What are the prime ideals of Z[x]? What are the maximal ideals? Carefully explain your answers.

$\omega^3 = e^{\pi i} = \cos\pi + i\sin\pi = -1$

$\omega = e^{\frac{2\pi i}{6}} = e^{\frac{\pi i}{3}} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$

$1 = \frac{1}{2}^2 + a^2$

$\frac{3}{4} = a^2 \Rightarrow \frac{\sqrt{3}}{2}$



① $f(x) = x^6+3 \in \mathbb{Q}[x]$. Show $Gal(E/\mathbb{Q}) = S_3$ | Alg-Spr 10

1.

$x^6+3 = (x^3+\sqrt{3})(x^3-\sqrt{3})$ and roots are $\omega^j i \sqrt[6]{3}$ where ω is a primitive 6th root of unity and $j=1,\dots,6$ ($i\sqrt[6]{3} = \alpha$)

So then $E = \mathbb{Q}(\omega, i\sqrt[6]{3}) = \mathbb{Q}(\omega, \alpha)$ is a splitting field

Note that $\omega = e^{\frac{2\pi i}{6}} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, i.e. $i\sqrt{3} \in \mathbb{Q}(\omega)$ and $i\sqrt{3} = -\alpha^3$, hence $\alpha^3 \in \mathbb{Q}(\omega)$, hence α satisfies $x^3-\alpha^3$ over $\mathbb{Q}(\omega)$, hence min poly must divide.

Note that
$$x^3-\alpha^3 = (x-\alpha)(x^2+\alpha x+\alpha^2)$$
$$= (x-\alpha)(x-\beta)(x-\bar{\beta})$$
$$= (x-\alpha)(x+\alpha\bar{\omega})(x+\alpha\omega)$$

roots are $\frac{-\alpha \pm \sqrt{\alpha^2-4\alpha^2}}{2}$

$= \frac{-\alpha \pm \alpha\sqrt{-3}}{2}$

$\beta = \frac{-\alpha + \alpha i\sqrt{3}}{2}$

$\bar{\beta} = \frac{-\alpha - \alpha i\sqrt{3}}{2}$

$\hookrightarrow \beta = \alpha\left(\frac{-1+i\sqrt{3}}{2}\right)$

$\bar{\beta} = \alpha\left(\frac{-1-i\sqrt{3}}{2}\right)$

$\hookrightarrow \beta = \alpha(-\bar{\omega})$

$\bar{\beta} = \alpha(-\omega)$

Any degree 2 divisor will have constant term w/ $\alpha^2 \notin \mathbb{Q}(\omega)$,

[So $x^3-\alpha^3$ is min poly for α over $\mathbb{Q}(\omega)$

Thus

$\mathbb{Q}(\alpha,\omega) = E$
|) 3
$\mathbb{Q}(\omega)$
|) $\varphi(6) = \varphi(2)\varphi(3) = 2$
$\mathbb{Q}$

$\Rightarrow [E:\mathbb{Q}] = 6 = |Gal(E/\mathbb{Q})|$. ; groups order 6 are $\mathbb{Z}_6$ & S_3

now $\mathbb{Q}(\alpha,\omega)=E$

$$\begin{array}{c} \mathbb{Q}(\alpha,\omega)=E \\ | \ \big) 3 \\ \mathbb{Q}(\omega) \\ | \ \big) 2 \\ \mathbb{Q} \end{array}$$

$\big)3 \rightsquigarrow \alpha^3 \in \mathbb{Q}(\omega)$

let $\sigma: \alpha \mapsto \omega^2\alpha$ ← third root of unity (recall $x^3-\alpha^3$ min poly over $\mathbb{Q}(\omega)$)
$\omega \mapsto \omega$

$\sigma^3 = id$

$\tau: \alpha \mapsto \alpha$
$\omega \mapsto \omega^5$ ← must send primitive to primitive

$\to \tau^2 = id$

so $\tau\sigma\tau^{-1}(\alpha) = \tau\sigma(\alpha) = \tau(\omega^2\alpha) = \omega^{10}\alpha = \omega^4\alpha = \sigma^2(\alpha) = \sigma^{-1}(\alpha)$ (with $\tau^{-1} = \tau$)

$\tau\sigma\tau(\omega) = \tau\sigma(\omega^5) = \tau(\omega^5) = \omega = \sigma^{-1}(\omega)$

so $\tau\sigma\tau^{-1} = \sigma^{-1} \Rightarrow$ $\underline{Gal(E/\mathbb{Q}) \cong S_3}$

(2) (a) $|G| = pqr$, $p<q<r$ prime. Show G has normal s.g. index p.

Sylow: $n_r \equiv 1 \pmod r$ & $n_r \mid pq \Rightarrow n_r = 1, p, q, pq$

Case $n_r = pq$: then there are $pq(r-1)$ distinct non-identity order r elements

$n_q \equiv 1 \pmod q$ & $n_q \mid pr \Rightarrow n_q = 1, p, r, pr$

If $n_q = r$, then $\exists\ r(q-1)$ distinct non-id order q elts

Then: $pq(r-1) + r(q-1) + 1 = pqr - pq + rq - r + 1$

$= pqr + r(q-1) - pq + 1$

$r \geq q$, $q-1 \geq p$

$\Rightarrow r(q-1) \geq qp$

hence $> pqr$.

Hence $n_q = 1$, and we get a normal Sylow q-s.g. Q.

Case $n_r = 1$: then R is a normal Sylow r-s.g.

Therefore, in either case we get subgroup RQ of order qr and index p.

By rep'n on cosets, $\exists\ \varphi: G \to S_p$ w/ $\ker\varphi \subseteq RQ$.

Now, $|G/\ker\varphi| \,\big|\, |S_p| = p!$ & $|G/\ker\varphi| \,\big|\, |G| = pqr$

$\Rightarrow |G/\ker\varphi| \,\big|\, \gcd(p!, pqr) = p$ ← since $p < q, r$

$\Rightarrow |G/\ker\varphi| = p \Rightarrow |\ker\varphi| = rq \Rightarrow \ker\varphi \cong RQ$

$\Rightarrow RQ$ normal.

③ R comm, noeth, $I \subseteq R$ irred if $I = J \cap K \Rightarrow I = J$ or $I = K$.

(a) Every ideal in R is finite $\cap$ of irreducibles

Let $\mathcal{F}$ = {ideals not finite $\cap$ of irreducibles} & suppose $\mathcal{F} \neq \phi$.

R noeth, so every chain of ascending ideals terminates, hence apply Zorn's Lemma to $\mathcal{F}$ to get maximal M in $\mathcal{F}$.

Suppose $M = J \cap K$. M not irreducible since $M \in \mathcal{F}$, hence $M \neq J$ and $M \neq K$, but $M \subsetneq J$ & $M \subsetneq K$, hence $J, K \notin \mathcal{F}$ since M is maximal in $\mathcal{F}$.

therefore J, K are finite $\cap$ of irred, hence M is, therefore a contradiction and thus $\mathcal{F} = \phi$.

(b) Every irreducible ideal is primary

Let I be irreducible; consider R/I. Let $x, y \in R/I$ and suppose $xy = 0$ ($xy \in I$) and $y \neq 0$. Then we want to show $x^n = 0$ for some n ($x^n \in I$)

R noeth, so the sequence $Ann(x) \subseteq Ann(x^2) \subseteq \cdots \subseteq Ann(x^n) = Ann(x^{n+1})$ terminates

Now we'll show that $(x^n) \cap (y) = 0$:

Choose any elt from this intersection; $ax^n = by$

$\Rightarrow ax^{n+1} = byx = bxy = 0 \Rightarrow a \in Ann(x^{n+1}) = Ann(x^n)$

(R comm.) $\Rightarrow ax^n = 0$

Hence $(x^n) \cap (y) = 0$; but 0 irred, hence $(x^n) = 0$ or $(y) = 0$. We know that $y \neq 0$, so $(x^n) = 0$, hence $x^n = 0$, hence $x^n \in I$

and thus I primary

(b) $|G| = 3\cdot 7\cdot 13 \Rightarrow |N| = 7\cdot 13$.

We just showed $\exists$ normal sg. of index 3, so let $N \trianglelefteq G$, $[G:N]=3$. By Cauchy's thm $\exists$ $P \le G$ w/ $|P|=3$.

Orders coprime, so $P \cap N = \{1\} \Rightarrow PN = G$

So $G = N \rtimes P$, getting $\varphi: P \to Aut(\mathbb{Z}_7 \oplus \mathbb{Z}_{13}) \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{12}$ (with $N = \mathbb{Z}_7 \oplus \mathbb{Z}_{13}$)

$P = \langle a \rangle \mapsto h_a(x) = axa^{-1}$

$|P| = 3 \Rightarrow h_a$ has order 3 or 1.

Case order 1: $axa^{-1} = h_a(x) = x \Rightarrow$ abelian $\Rightarrow$ $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{13}$.

Case order 3:

$\mathbb{Z}_6 = \langle b \rangle$, $\mathbb{Z}_{12} = \langle c \rangle$

① $(b^2, 1)$, $(b^4, 1)$ ③ $(1, c^4)$, $(1, c^8)$

② (b^2, c^4), (b^4, c^8) ④ (b^4, c^4), (b^2, c^8)

} 8 order 3 elts in $Aut(\mathbb{Z}_7 \oplus \mathbb{Z}_{13})$

$N = \mathbb{Z}_7 \oplus \mathbb{Z}_{13} = \langle \alpha \rangle \oplus \langle \beta \rangle$; $\theta_i \in Aut(N)$

$\theta_1(\alpha, \beta) = (\alpha^2, \beta)$ $\quad \theta_3(\alpha, \beta) = (\alpha, \beta^3)$

$\theta_2(\alpha, \beta) = (\alpha^2, \beta^3)$ $\quad \theta_4(\alpha, \beta) = (\alpha^4, \beta^3)$

(squares of each of these give the other 4)

$k^3 = 1 \pmod{13}$

$k^3 - 1 \equiv 0 \pmod{13}$

$\Downarrow$

$(k-1)(k^2+k+1) \equiv 0 \pmod{13}$

$\Downarrow$

$k^2 + k \equiv 12 \pmod{13}$

$\Downarrow$

$k(1+k) \equiv 12 \pmod{13}$

$\Downarrow$

$k = 3$ or 9

① $h_a(\alpha, \beta) = (\alpha^2, \beta) = (a\alpha a^{-1}, a\beta a^{-1})$

$\Rightarrow G \cong \langle a, \alpha, \beta : a^3 = \alpha^7 = \beta^{13} = 1,\ \alpha^2 = a\alpha a^{-1},\ \beta = a\beta a^{-1} \rangle$

② $h_a(\alpha, \beta) = (\alpha^2, \beta^3) = (a\alpha a^{-1}, a\beta a^{-1})$

$\Rightarrow G \cong \langle a, \alpha, \beta : a^3 = \alpha^7 = \beta^{13} = 1,\ \alpha^2 = a\alpha a^{-1},\ \beta^3 = a\beta a^{-1} \rangle$

③ $h_a(\alpha, \beta) = (\alpha, \beta^3) \Rightarrow G \cong \langle a, \alpha, \beta : a^3 = \alpha^7 = \beta^{13} = 1,\ \alpha = a\alpha a^{-1},\ \beta^3 = a\beta a^{-1} \rangle$

④ $h_a(\alpha, \beta) = (\alpha^4, \beta^3) \Rightarrow G \cong \langle a, \alpha, \beta : a^3 = \alpha^7 = \beta^{13} = 1,\ \alpha^4 = a\alpha a^{-1},\ \beta^3 = a\beta a^{-1} \rangle$

④ A fin-dim k-alg s.t. $a \in A$ has $a^7 = a$.
Show: A direct product of fields

A fin-dim k-alg $\Rightarrow$ A artinian $\Rightarrow$ $J(A)$ nilpotent

But $a^7 = a$, hence $\nexists$ nilpotent elts in A, hence $J(A) = 0$,

Therefore A art + Jac s.s. $\Rightarrow$ A s.s.

Apply Art-Wedd: $A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$

If $n_i > 1$ for any i, then $\exists$ nilpotent elements $\Rightarrow n_i = 1 \ \forall i$.

$\Rightarrow A \cong D_1 \oplus \cdots \oplus D_k$.

Now, every elt in A has an inverse ($a^6 a = a \Rightarrow a^6 = 1$
$\Rightarrow a^5 = a^{-1}$),
therefore the D_i are fields.

⑤ G, H fin-gen abelian groups s.t. $G \otimes_{\mathbb{Z}} H = 0$.
Show that G & H are finite & have relatively prime orders.

$H \cong \mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{e_n}}$

$G \cong \mathbb{Z}^l \oplus \mathbb{Z}_{q_1^{f_1}} \oplus \cdots \oplus \mathbb{Z}_{q_m^{f_m}}$

$$0 = H \otimes_{\mathbb{Z}} G \cong (\mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{e_n}}) \otimes_{\mathbb{Z}} (\mathbb{Z}^l \oplus \mathbb{Z}_{q_1^{f_1}} \oplus \cdots \oplus \mathbb{Z}_{q_m^{f_m}})$$

$$\cong \mathbb{Z}^k \otimes \mathbb{Z}^l \otimes (\mathbb{Z}^k \otimes \mathbb{Z}_{q_1^{f_1}}) \otimes \cdots$$

↗ Distribution of $\otimes$ over $\oplus$

$\mathbb{Z}^k \otimes \mathbb{Z}^l = \mathbb{Z}^{kl}$, hence $\mathbb{Z}^{kl} = 0 \Rightarrow k$ or $l = 0$

WLOG, suppose $k = 0$ & $l \neq 0$

consider other summands: $\mathbb{Z}^l \otimes_{\mathbb{Z}} \mathbb{Z}_{p_i^{e_i}} = (\mathbb{Z} \otimes \mathbb{Z}_{p_i^{e_i}})^l = (\mathbb{Z}_{p_i^{e_i}})^l \neq 0$

therefore $l = 0$ as well.; hence neither G or H have free part, hence finite.

- $\mathbb{Z}_{p_i^{e_i}} \otimes_{\mathbb{Z}} \mathbb{Z}_{q_j^{f_j}} = 0 \iff \gcd(p_i, q_j) = 1$,

therefore orders are coprime.