ALGEBRA QUALIFYING EXAM   MAY, 2000

Partial credit is given for partial solutions.

1. Up to isomorphism describe all groups of order 595 (5·7·17).

Fix → 2. Let M be a finitely generated module over a PID R. If $M \otimes_R M \cong M$ determine the structure of M.

3. Let $\rho \in \mathbb{C}$ be a primitive p^{th} root of 1 for an odd prime p and set $L = \mathbb{Q}(\rho)$. What is Gal(L/Q)? If m is the number of different positive integer divisors of $p - 1$, how many fields F satisfy $\mathbb{Q} \subseteq F \subseteq L$ and how many of these are Galois extensions of Q? What are the Gal(F/Q)? Show that $[L: \mathbb{R} \cap L)] = 2$. Show that $N_{L/\mathbb{Q}}(1 - \rho^j) = p$ for any $1 \leq j \leq p-1$.

Hilb. basis thm

4. Let R be a commutative Noetherian ring with 1 and let $\varphi: R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]$ be a surjective ring homomorphism. Show that φ is an automorphism.

5. Let I be an ideal in $\mathbb{C}[x_1, \ldots, x_n]$.
   i) Show that there is $k > 0$ so that $(\sqrt{I})^k \subseteq I$.
   → ii) Prove that if I is maximal then I/I^k is a finite dimensional C-vector space for all $k \geq 0$.
   iii) Show that $\mathbb{C}[x_1, \ldots, x_n]/I$ is finite dimensional over C $\Leftrightarrow$ $\{\alpha \in \mathbb{C}^n \mid f(\alpha) = 0, \text{ all } f \in I\}$ is finite.

6. If R is a finite ring with 1 and $x, y \in R$ satisfy $xy = 1$, show that $yx = 1$.   var(I)

↳ R finite ⇒ R noetherian

Let $\varphi: R \to R$ by $a \mapsto xa$; then $\varphi(y) = 1$, hence surjective.

Now consider the chain $\ker\varphi \subseteq \ker\varphi^2 \subseteq \cdots \subseteq \ker\varphi^n = \ker\varphi^{n+1}$

Since φ is surjective, so is φ^n; now choose $x \in \ker\varphi$.

then $\exists\, y$ s.t. $x = \varphi^n(y) \Rightarrow 0 = \varphi(x) = \varphi^{n+1}(y) \Rightarrow y \in \ker\varphi^{n+1} = \ker\varphi^n$

hence $x = \varphi^n(y) = 0 \Rightarrow \ker\varphi = 0 \Rightarrow \varphi$ injective

So now consider $1 - yx$; $\varphi(1-yx) = x(1-yx) = x - xyx = x - x = 0$

hence $1 - yx \in \ker\varphi = 0 \Rightarrow 1 - yx = 0 \Rightarrow 1 = yx$

Algebra: May 2000:

(1) $|G| = 595 = 5 \cdot 7 \cdot 17$:

Sylow: $r_{17} \equiv 1 \pmod{17}$ & $r_{17} \mid 5\cdot 7 \Rightarrow r_{17} = 1, \cancel{5}, \cancel{7}, 5\cdot 7$

$r_7 \equiv 1 \pmod{7}$ & $r_7 \mid 5\cdot 17 \Rightarrow r_7 = 1, \cancel{5}, \cancel{17}, 5\cdot 17$

$r_5 \equiv 1 \pmod{5}$ & $r_5 \mid 7\cdot 17 \Rightarrow r_5 = 1, 7, \cancel{17}, \cancel{7\cdot 17}$

$\begin{array}{r} 35 \\ \times 17 \\ \hline 18 \end{array}$ $\begin{array}{r} 17 \\ \times 5 \\ \hline 85 \end{array}$

$16 = 2^4$
$6 = 2 \cdot 3$

Suppose $r_{17} = 5\cdot 7$: $35 \cdot 16$ elements order 17

$(5\cdot 7\cdot 17) - (5\cdot 7 \cdot 16) = 5\cdot 7(1) = 35$ elements of other order.

Therefore if $r_7 = 5\cdot 17 = 85$, there are 84 elts order 7; so contradiction and thus $r_7 = 1$, hence getting a normal Sylow 7-sg Q.

On the other hand, $r_{17} = 1$: Sylow 17-sg N is normal.

Therefore NQ index 5 subgroup in either case.

Now consider the repn on cosets: $\varphi: G \to S_5$ w/ $NQ \supseteq \ker\varphi$.

See that $|G/\ker\varphi| \mid 5!$ and $|G/\ker\varphi| \mid 5\cdot 7\cdot 17$,

hence $|G/\ker\varphi| \mid \gcd(5!, 5\cdot 7\cdot 17) = 5 \Rightarrow |G/\ker\varphi| = 5 \Rightarrow |\ker\varphi| = 57$

$\Rightarrow NQ = \ker\varphi \Rightarrow NQ$ normal subgroup

Now, let S be a Sylow 5-subgroup & $S \cap NQ = \{0\}$ since orders coprime, hence $SNQ = G$ and so $G = NQ \rtimes S$. Hence hom:

$\varphi: S \to Aut(NQ) \cong Aut(\mathbb{Z}_{17} \oplus \mathbb{Z}_7) \cong \mathbb{Z}_{16} \oplus \mathbb{Z}_6$

$\langle s \rangle \mapsto \sigma_s(n) = sns^{-1}$

So σ_s must be order 1 or 5, but $Aut(NQ)$ has no order 5 elements

hence, $\sigma_s = id$, hence abelian, hence $G \cong \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{17}$

② M fin-gen module over PID R.
If $M \otimes_R M \cong M$, determine the structure of M

Fundamental Theorem of Modules/PID: $M \cong R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$
where $a_1 | a_2 | \cdots | a_m$.

So now see that:

$$M \otimes_R M \cong (R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)) \otimes (R^k \oplus R/(a_1) \oplus \cdots \oplus R/(a_m))$$
$$\cong (R^k \otimes R^k) \oplus \left(R^k \otimes \left(\bigoplus_i (R/(a_i))\right)\right) \oplus \left(\left(\bigoplus_i (R/(a_i))\right) \otimes R^k\right)$$
$$\oplus \left(\bigoplus_{1 \le i,j \le m} \left(R/(a_i) \otimes R/(a_j)\right)\right)$$

See that

- $R^k \otimes \left(\bigoplus_i R/(a_i)\right) \cong \bigoplus_i \left(R^k \otimes R/(a_i)\right)$, and then

$$(R^k \otimes R/(a_i)) \cong (R \oplus \cdots \oplus R) \otimes R/(a_i) \cong \left(R \otimes_R R/(a_i)\right)^k$$
$$\xrightarrow{\text{since } R \otimes_R M \cong M} \cong \left(R/(a_i)\right)^k$$

- similarly, $\left(\bigoplus_i R/(a_i)\right) \otimes R^k \cong \bigoplus \left(R/(a_i) \otimes R^k\right)$

& $\left(R/a_i \otimes R^k\right) \cong \left(R/(a_i)\right)^k$

- $R^k \otimes R^k \cong (R \otimes R^k)^k \cong (R^k)^k \cong R^{k^2}$

- $R/(a_i) \otimes R/(a_j) \cong R/(\gcd(a_i, a_j)) \cong R/(a_{\min(i,j)})$ since $a_i | a_j$, $i \le j$

So $M \otimes M \cong R^{k^2} \oplus \left(\bigoplus_i \left(R/(a_i)\right)^k\right) \oplus \left(\bigoplus_i \left(R/(a_i)\right)^k\right) \oplus \bigoplus_{1 \le i,j \le m} \left(R/(a_{\min(i,j)})\right)$

$\cong$

$M \cong R^k \oplus \left(\bigoplus_i \left(R/(a_i)\right)\right) \Rightarrow k = k^2$

For either $k = 1$ ~~1~~, there are unequal copies of the torsion part, hence torsion must be zero, so in this case $M = R$.

③ $\rho \in \mathbb{C}$ primitive p^{th} root of 1 for odd p, let $L = \mathbb{Q}(\rho)$

(a) $\underline{Gal(L/\mathbb{Q})}$? If p is prime the ρ is a root of $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$ where the deg $p-1$ poly is irreducible. Therefore it is minimal for ρ, hence $|Gal(L/\mathbb{Q})| = p-1$. The element $\sigma \in Gal(L/\mathbb{Q})$ is an has automorphism, so sends primitive p^{th} root to primitive p^{th} root, hence, get $\sigma: \rho \mapsto \rho^k$ with $\gcd(p,k)$; and therefore $\sigma^{p-1}(\rho) = \rho^{k^{p-1}} = \rho$ since ~~since~~ $\gcd(p,k) \Rightarrow k^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem.

So σ has order $p-1$, hence $\underline{Gal(L/\mathbb{Q}) \cong \mathbb{Z}_{p-1}}$

(b) Let m be the number of divisors of $p-1$; How many fields $\underline{F \text{ w/ } \mathbb{Q} \subseteq F \subseteq L}$ and how many $F/\mathbb{Q}$ are Galois?

Intermediate fields correspond to subgroups of $Gal(L/\mathbb{Q})$ and Galois subextensions correspond to normal subgroups.

Recall that every subgroup of $\mathbb{Z}_{p-1}$ is normal since it is abelian; therefore all subextensions are Galois.

Also, there is a subgroup of $\mathbb{Z}_{p-1}$ for every divisor, hence there are m intermediate fields (or $m-2$ excluding L and $\mathbb{Q}$).

(c) $\underline{\text{What are the } Gal(F/\mathbb{Q})}$? $\mathbb{Z}_k$, k ranges over divisors of $p-1$.

(d) $\underline{\text{Show that } [L : \mathbb{R} \cap L] = 2}$:

Consider the element $\tau \in Gal(L/\mathbb{Q})$ with $\tau : x \mapsto \bar{x}$.

Then $\langle \tau \rangle \leqslant Gal(L/\mathbb{Q}) \cong \mathbb{Z}_{p-1}$ an order 2 sg., hence index $\frac{p-1}{2}$.

So: $\frac{p-1}{2} = [Gal(L/\mathbb{Q}) : \langle \tau \rangle] = [L^{\langle \tau \rangle} : \mathbb{Q}] = [L \cap \mathbb{R} : \mathbb{Q}]$

Therefore, by tower law, $\underline{[L : \mathbb{R} \cap L] = 2}$

(e) $N_{L/\mathbb{Q}}(1-\rho^j) = p$ for all $1 \le j \le p-1$.

$x^{p-1} + x^{p-2} + \dots + x + 1 = \dfrac{x^p - 1}{x-1}$ min poly of ρ, hence irred.

But then $\dfrac{(x+1)^p - 1}{x}$ is also irreducible with $\rho - 1$ a root, and clearly $\rho^i - 1$ are all the roots for $i = 1, \dots, p-1$.

See that $\dfrac{(x+1)^p - 1}{x} = x^{p-1} + p x^{p-2} + \dots + p x + p$.

$$
\begin{aligned}
\text{hence } N(1-\rho^i) = \underbrace{(-1)^{p-1}}_{1 \text{ since } p \text{ odd}} N(1-\rho^i) &= \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma(1-\rho^i) \\
&= \prod_{\sigma \in \mathrm{Gal}} (1 - \sigma(\rho)^i) \\
&= \text{product of roots of } (*) \\
&= p.
\end{aligned}
$$

④ R commutative, noetherian, $\varphi : R[X_1,\dots,X_n] \to R[X_1,\dots,X_n]$ a surjective ring homomorphism. Show that φ is an automorphism.

By Hilbert Basis theorem, $R[X_1,\dots,X_n]$ is also noetherian.

Now consider the chain of ideals $\ker\varphi \subseteq \ker\varphi^2 \subseteq \dots \subseteq \ker\varphi^n = \ker\varphi^{n+1}$, which terminates for some n since $R[X_1,\dots,X_n]$ noetherian.

Choose $x \in \ker\varphi$; now, since φ is surjective, so is φ^n, hence $\exists\, y$ s.t. $\varphi^n(y) = x$, hence $\varphi^{n+1}(y) = \varphi(x) = 0$ since $x \in \ker\varphi$.

But now $y \in \ker\varphi^{n+1} = \ker\varphi^n \Rightarrow x = \varphi^n(y) = 0 \Rightarrow x = 0$

$\Rightarrow \ker\varphi = 0$ injective

⑤ $I \subseteq \mathbb{C}[X_1,\dots,X_n]$ ideal.

(i) Show $\exists\, k > 0$ s.t. $(\sqrt{I})^k \subseteq I$.

Hilbert Basis $\Rightarrow \mathbb{C}[X_1,\dots,X_n]$ noeth $\Rightarrow I$ finitely generated, hence $\sqrt{I} = \langle f_1,\dots,f_m\rangle$. For each f_i, $\exists\, t_i$ s.t. $f_i^{t_i} \in I$; let $t = \max_i\{t_i\}$

Then for any $f \in \sqrt{I}$, $f = \sum_{i=1}^{m} g_i f_i$, hence let $k = tm$ and we get $f^k = f^{tm} = \left(\sum_{i=1}^{m} g_i f_i\right)^{tm}$; each term has total degree tm, hence there is a factor of f_i^t for at least one i in each, hence every factor is in I, hence $f^k \in I$.

Therefore, $(\sqrt{I})^{tm} \subseteq I$

(ii) Show that if I maximal, then I/I^k fin-dim $\mathbb{C}$-v.s. $\forall\, k \geq 0$.

I maximal, so $I = (x_1 - a_1, \dots, x_n - a_n)$ by weak Nullstellensatz.

Therefore, $Var(I^k) = Var(I)$, hence $\sqrt{I^k} = Id(Var(I^k))$

$= Id(Var(I)) = \sqrt{I} = I$ $\quad$ I max $\Rightarrow$ I prime $\Rightarrow$ I radical

So $I/I^k = \sqrt{I^k}/I^k$; by part (i), $\exists\, m$ s.t. $(\sqrt{I^k})^m \subseteq I^k$, hence the ideal is nilpotent; recall that $\mathbb{C}[X_1,\dots,X_n]$ noeth, hence $I/I^k = \langle a_1,\dots,a_e\rangle$, where the generators are all nilpotent

i.e., $a_i^m = 0$ for every i.
Since all are nilpotent, there are only finitely many powers of each x_i in I/I_1^k, hence let those be a finite $\mathbb{C}$-basis.

(iii) Show $\mathbb{C}[x_1,\dots,x_n]/I$ fin-dim $/\mathbb{C} \iff Var(I)$ finite.

($\Rightarrow$) $\mathbb{C}[x_1,\dots,x_n]/I$ fin-dim'l $\Rightarrow \mathbb{C}[x_1,\dots,x_n]/I$ artinian
$\Rightarrow$ has finitely many max ideals $\Rightarrow$ there are finitely many max ideals of $\mathbb{C}[x_1,\dots,x_n]$ containing I. Let $\{M_i\}_{i=1}^m$ be those ideals. Recall that $M_i = (x_1 - a_1^{(i)}, \dots, x_n - a_n^{(i)})$ by weak nullstellensatz. Hence the various permutations of $(a_1^{j_1}, \dots, a_n^{j_n})$, $1 \le j_\ell \le m$, will be the shared zeroes in I, hence $|Var(I)| < \infty$.
($\Rightarrow$) Suppose $Var(I)$ finite.
We then know that $\mathbb{C}^{|Var\,I|} = \mathbb{C}[x_1,\dots,x_n]/\sqrt{I}$?