Spring 2013: Algebra Graduate Exam

Problem 1.

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

Proof. Next, note that the number of Sylow p groups must divide the order of the group, and be congruent to 1 mod p. Therefore there must be exactly one Sylow p group, and since it is unique it is normal. Call the Sylow p-subgroup N and the Sylow 2-subgroup K. Thus $G \cong N \rtimes_{\varphi} K$ where $\varphi \colon K \to \mathrm{Aut}(N)$ is a homomorphism.
Note that all groups of order p^2 are abelian, so in particular $N \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ or $N \cong \mathbb{Z}_{p^2}$.

Case 1. Assume $N \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, so that $\mathrm{Aut}(N) \cong GL_2(p)$, the general linear group over the field of integers modulo p. Then there are four homomorphisms which give three distinct groups up to isomorphism: the identity, the map $(x, y) \mapsto (x^{-1}, y)$, and the map $(x, y) \mapsto (x^{-1}, y^{-1})$. (Note: I'm not sure what these are the only homomorphisms)

(i) $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_2$,

(ii) $G \cong (\mathbb{Z}_p \oplus \mathbb{Z}_p) \times \mathbb{Z}_2$ with operation $((x_1, y_1), a) \cdot ((x_2, y_2), b) = \begin{cases} ((x_1x_2, y_1y_2), a + b) & a = 0 \\ ((x_1x_2^{-1}, y_1y_2), a + b) & a = 1 \end{cases}$, or

(iii) $G \cong (\mathbb{Z}_p \oplus \mathbb{Z}_p) \times \mathbb{Z}_2$ with operation $((x_1, y_1), a) \cdot ((x_2, y_2), b) = \begin{cases} ((x_1x_2, y_1y_2), a + b) & a = 0 \\ ((x_1x_2^{-1}, y_1y_2^{-1}), a + b) & a = 1 \end{cases}$.

Case 2. Assume $N \cong \mathbb{Z}_{p^2}$ so that $\mathrm{Aut}(N)$ is of order $\phi(p^2) = p(p - 1)$. Since p^2 is a power of a prime, $\mathrm{Aut}(N) \cong \mathbb{Z}_{p(p-1)}$. Since φ is a homomorphism, it must map $\overline{0} \mapsto \mathrm{id}$, and $\overline{1}$ to an automorphism of order 1 or 2. The only two such automorphisms are the identity and the map $1 \mapsto -1$.

(iv) $G \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_2$, or

(v) $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_2$ with operation $(x_1, a) \cdot (x_2, b) = \begin{cases} (x_1x_2, a + b) & a = 0 \\ (x_1x_2^{-1}, a + b) & a = 1 \end{cases}$.

This is the dihedral group of order $2p^2$.

□

Problem 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

Proof. (From Nicolle.) Let S be the set of ideals that are not the product of finitely many prime ideals of R. We intend to show that S is empty.

First assume that S is nonempty. Since R is Noetherian, by Zorn's Lemma there must exist a maximal element $M \in S$. Now consider the quotient R/M. If $I + M \in R/M$, then $I \notin S$ and so I is the product of finitely many ideals.

Notice that R/M must be prime. If it is not prime, there exists $I + M, J + M \neq 0$ such that $IJ + M = 0$ in R/M, that is $IJ = M$. However, this is a contradiction. Since I and J are both finite products of prime ideals, $IJ = M$ is too—a contradiction to the construction that $M \in S$. Thus R/M is prime.

Since R is commutative, R/M is commutative too. Recall that a commutative ring is prime if and only if its zero ideal is a prime ideal. Thus M is a prime ideal in R. This is a contradiction since this means that M is the product of a finite number of prime ideals (namely, one prime ideal, itself). Since $M \in S$, by construction, S must be empty. □

Problem 3.

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

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

Proof. Firstly, let

$$I = ((x-y)^3, (y-z)^5, (x+y+z-3)^7).$$

It is sufficient to show that $p(x, y, z)$ vanishes on $\mathrm{Var}(I)$; by Hilbert's Nullstellensatz, this implies that $p(x, y, z)^m \in I$ for some $m \in \mathbb{N}$.

By definition the variety of I is the points where all polynomials vanish:

$$\mathrm{Var}(I) = \{(x, y, z) : (x-y)^3 = (y-z)^5 = (x+y+z-3)^7 = 0\}$$

Ignoring multiplicity and looking the system of equations

$$\begin{aligned} x-y \quad\quad &= 0 \\ y-z \quad &= 0 \\ x+y+z-3 &= 0 \end{aligned}$$

yields $x = y = z = 1$.

Evaluating $p(x, y, z)$ at $(1, 1, 1)$ yields

$$p(1,1,1) = \underbrace{1^{16}1^{25}1^{81}}_{1}\underbrace{-1^71^{15}}_{-1}\underbrace{-1\cdot 1^9}_{-1}\underbrace{+1^5}_{+1} = 0,$$

so $p(x, y, z)$ vanishes on $\mathrm{Var}(I)$ and $p(x, y, z)^m \in I$ for some $m \in \mathbb{N}$ by Nullstellensatz. □

Problem 4.

Let $R \neq (0)$ be a finite ring such that for any element $x \in R$ there is $y \in R$ with $xyx = x$. Show that

(a) R contains an identity element and

(b) that for $a, b \in R$ if $ab = 1$ then $ba = 1$.

Note. It may be worth considering the counterexample to the claim that $xyx = x$ implies $xy = 1$. Let $x = 3 \in \mathbb{Z}_3$, then $x = 1, 3, 5$ and $\underbrace{3 \cdot 3 \cdot 3 = 3}_{xyx=x}$, but $xy = 3 \neq 1$.

Proof. This question is answered here `https://math.stackexchange.com/q/1417859/121988`.

(a)

(b) Consider the map (not necessarily a homomorphism) $f_y \colon R \to R$ which sends $z \mapsto yz$. The function f_y is an injection (and thus a bijection) since

$$\begin{aligned} f_y(t) = f_y(s) &\implies yt = ys \\ &\implies y(t-s) = 0 \\ &\implies \underbrace{xy}_{1}(t-s) = x \cdot 0 \\ t = s&. \end{aligned}$$

Since f_y is a bijection, $f_y^{-1}(1) = z$ is well-defined with $f_y(z) = yz = 1$. Then

$$x = x(yz) = (xy)z = z$$

so $f_y(x) = yx = 1$, as desired.

□

Problem 5.

Let $f(x) = x^{15} - 2$, and let L be the splitting field of $f(x)$ over $\mathbb{Q}$.

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

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

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

(d) Show that there is a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ that is isomorphic to $\mathrm{Gal}(F/\mathbb{Q})$.

Proof. Let ω be a fifteenth root of unity. Then $L = \mathbb{Q}[\omega, \sqrt[15]{2}]$.

(a) Since the extension of $\mathbb{Q}[\sqrt[15]{2}]]$ by a fifteenth root of unity is degree $\phi(15) = 8$,

$$[L : \mathbb{Q}] = \underbrace{[L : \mathbb{Q}[\omega]]}_{15}\underbrace{[\mathbb{Q}[\omega] : \mathbb{Q}]}_{\varphi(15)=8} = 8 \cdot 15 = 120.$$

(b) Let $F = \mathbb{Q}[\omega]$. As shown above, $[F : \mathbb{Q}] = \phi(15) = 8$. Note that F is Galois because every extension of $\mathbb{Q}$ by a root of unity is normal and thus Galois.

(c) An automorphism of F which fixes $\mathbb{Q}$ is of the form $\omega \mapsto \omega^k$ where $k \in \mathbb{Z}_{15}^\times$, the multiplicative group of $\mathbb{Z}_{15}$, which as a set consists of $\{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$. and is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

(d) This follows from the fundamental theorem of Galois theory. Since $\mathbb{Q}[\sqrt[15]{2}]$ is an intermediate field ($\mathbb{Q} \subset \mathbb{Q}[\sqrt[15]{2}] \subset L$), then there exists an (order reversing) bijection which sends intermediate fields to subgroups of $\mathrm{Gal}(L/\mathbb{Q})$. In particular, this map sends $\mathbb{Q}[\sqrt[15]{2}] \mapsto \mathrm{Gal}(L/\mathbb{Q}[\sqrt[15]{2}])$, the group of automorphisms of L that fix $\mathbb{Q}[\sqrt[15]{2}]$. This is isomorphic to $\mathrm{Gal}(F/\mathbb{Q})$, the group of automorphisms of F that fix $\mathbb{Q}$.

□

Problem 6.

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

Proof. First, let ω denote the ninth root of unity. Then

$$\underbrace{[F:\mathbb{Q}]}_{60} = [F:\mathbb{Q}[\omega]]\,\underbrace{[\mathbb{Q}[\omega]:\mathbb{Q}]}_{\varphi(9)=6},$$

so $[F:\mathbb{Q}[\omega]] = 10$.
Now the automorphism group of $\mathbb{Q}[\omega]$ is isomorphic to the cyclic group of order 6 with generator $\varphi\colon \omega \mapsto \omega^2$. In particular,

$$\omega \overset{\varphi}{\longmapsto} \omega^2 \overset{\varphi}{\longmapsto} \omega^4 \overset{\varphi}{\longmapsto} \omega^8 \overset{\varphi}{\longmapsto} \omega^7 \overset{\varphi}{\longmapsto} \omega^5 \overset{\varphi}{\longmapsto} \omega.$$

□

Problem 7.

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

Proof. □