Kayla Orlinsky

Algebra Exam Spring 2013

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

Solution. Let G be a group of order $2p^2$. Then by Sylow, $n_p \equiv 1 \mod p$ and $n_p | 2$ so because $p > 2$, $n_p = 1$. Thus, G has a normal Sylow p-subgroup.

$\boxed{\text{Abelian}}$ If G also has a normal Sylow 2-subgroup, then G is abelian and

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$$

or

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_p$$

depending on whether or not P_p the Sylow p-subgroup of G is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Now, if P_2 is a non-normal Sylow 2-subgroup of G, then by the recognizing of semi-direct products theorem, G is a semi-direct product of its Sylow 2 and Sylow p-subgroups.

$\boxed{P_p \cong \mathbb{Z}_{p^2}}$ If P_p is cyclic, then we can let $\varphi : P_2 \to \text{Aut}(\mathbb{Z}_{p^2}) \cong \mathbb{Z}_{p^2}^\times \cong \mathbb{Z}_{p^2-p}$ be a homomorphism.

Let $P_2 = \langle a \rangle$ and $P_p = \langle b \rangle$.

Then because $\mathbb{Z}_{p^2-p}$ is of even order, there is a nontrivial homomorphism φ which will give a semi-direct product structure to G.

Since $\mathbb{Z}_{p^2-p}$ is cyclic, its Sylow 2-subgroup is also cyclic and so can only have one element of order 2. This is because if the Sylow p-subgroup is $\langle x \rangle$ where x has order 2^n, then if $i < 2^{n-1}$, $2i < 2^n$ so x^i does not have order 2, and if $i > 2^{n-1}$, then $i = 2^{n-1} + r$ for $0 < r < 2^{n-1}$ so $(x^i)^2 = x^{2i} = x^{2^n+2r} = x^{2r}$ and $2r < 2^n$ so again, x^i does not have order 2.

Thus, the only element of order 2 is $x^{2^{n-1}}$.

Thus, we have one possible homorphism $\varphi(a) = \sigma$ where $\sigma : P_p \to P_p$ is defined by $\sigma(b) = b^{-1}$, this defined multipliation on G by $bab^{-1} = \varphi(a)(b) = b^{-1}$.

This gives a structure for G as

$$G \cong \langle a, b \,|\, a^2 = b^{p^2} = 1, ab = b^{-1}a \rangle \cong D_{2p^2}$$

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

$\boxed{P_p \cong \mathbb{Z}_p \times \mathbb{Z}_p}$. Then if $\varphi : P_2 \to \text{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p) \cong GL_2(\mathbb{F}_p)$ we have that $|GL_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p)$ and since $p^2 - p$ is even, again there exists a nontrivial homomorphism φ.

Let $P_p \cong \langle b\rangle \times \langle c\rangle$.

Since $\varphi(a)$ will have order 2 and P_2 can either act trivially on one or neither of the copies of $\mathbb{Z}_p$ inside P_p, we have two possible homomorphisms which generate different semi-direct products,

$\varphi_1(a)(b) = b^{-1}$ and $\varphi_1(a)(c) = c$, $\varphi_2(a)(b) = b^{-1}$ and $\varphi_2(a)(c) = c^{-1}$.

***Note that the swap function $P_p \to P_p$ where $(b, c) \mapsto (c, b)$ is an automorphism, and so $\varphi_3(a)(b) = b$ and $\varphi_3(a)(c) = c^{-1}$ is conjugate to $\varphi_1(a)$, namely, φ_1 and φ_3 generate isomorphic semi-direct products.

This gives two possible structures for G.

$$G \cong \langle a, b, c \,|\, a^2 = b^p = c^p = 1, bc = cb, ab = b^{-1}a, ac = ca\rangle \cong D_{2p} \times \mathbb{Z}_p$$

$$G \cong \langle a, b, c \,|\, a^2 = b^p = c^p = 1, bc = cb, ab = b^{-1}a, ac = c^{-1}a\rangle \cong \mathbb{Z}_2 \rtimes_{\varphi_2} \mathbb{Z}_p^2$$

Thus, there are 5 possible structures for G.

$$\mathbb{Z}_2 \times \mathbb{Z}_{p^2}$$

$$\mathbb{Z}_2 \times \mathbb{Z}_p \times \mathbb{Z}_p$$

$$D_{2p^2}$$

$$D_{2p} \times \mathbb{Z}_p$$

$$\langle a, b, c \,|\, a^2 = b^p = c^p = 1, bc = cb, ab = b^{-1}a, ac = c^{-1}a\rangle \cong \mathbb{Z}_2 \rtimes_{\varphi_2} \mathbb{Z}_p^2$$

✌

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).

Solution. Let S be the set of proper ideals of R which are not products of finitely many prime ideals.

Assume S is nonempty. Because R is noetherian, S contains a maximal element I.

Since I is not prime, there exists a product of elements $ab \in I$ such that $a \notin I$ and $b \notin I$ (if no such ab existed then I would be prime).

Then $(a)(b) \in I$ since sums of products of $ab \in I$ but $(a) \not\subset I$ and $(b) \not\subset I$.

Now, if $I+(a) = R$, then $1 = x+ra$ where $x \in I$ and $r \in R$. However, then $1-ar = x \in I$ so $b - rab = xb \in I$ because I is an ideal, and $rab \in I$ since $ab \in I$, so $b \in I$, which is a contradiction because $I \in S$.

However, $I \subset I + (a) \neq R$ and so $I + (a)$ cannot be in S by maximality of I.

Thus, there exists a finite set of prime ideals $P_1, ..., P_n$ such that $I + (a) = P_1P_2 \cdots P_n$.

Similarly, there exists $Q_1, ..., Q_m$ so $I + (b) = Q_1Q_2 \cdots Q_m$.

However, then

$$(Q_1Q_2 \cdots Q_m)(P_1P_2 \cdots P_n) = (I + (a))(I + (b)) = I.$$

This contradicts that I is in S, so S must in fact 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

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

Solution. By Nullsetellensatz, if $I = ((x-y)^3, (y-z)^5, (x+y+z-3)^7)$, and $g(x, y, z) \in R$ is such that $g(a, b, c) = 0$ for all $(a, b, c) \in V(I)$, then $g \in \sqrt{I}$ and so there exists an integer m such that $g^m \in I$.

Thus, we need only check that $g(x, y, z) = x^{16}y^{25}z^{81} - x^7z^{15} - yz^9 + x^5$ is satisfied by every point in $V(I)$.

The points in $V(I)$ correspond exactly to the zeros of the generators of I. Namely, we have that $(x - y)^3 = 0, (y - z)^5 = 0, (x + y + z - 3)^7 = 0$ simultaneously.

Thus, $x = y, y = z, x + y + z = 3$, so $x + x + x = 3$ so $x = 1$, so the only point in $V(I)$ is $(1, 1, 1)$ which is clearly satisfied by g since $1 \cdot 1 \cdot 1 - 1 \cdot 1 - 1 + 1 = 0$.

Thus, there exists an m so $g^m \in I$. ✌

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

Solution.

***As written, this problem is not quite correct. Let $R = \{0, a, b\}$ where addition is defined by $a + a = 0$, $b + b = 0$, $a + b = b + a = 0$, and 0 behaves as usual. And multiplication is given by $a^2 = a$, $b^2 = b$, $ab = b$, $ba = a$, and 0 behaves as usual.

- R is nonempty and has a 0 element.
- Addition in R is associative and commutative.
- R has additive inverses.
- Distributivity is immediate since the sum of any two elements in R is zero so multiplication trivially distributes.
- For multiplicative associativity, we check each case:

$$\begin{array}{cc} (ab)a = ba = a & a(ba) = aa = a \\ (ba)b = ab = b & b(ab) = bb = b \\ (ab)b = bb = b & a(bb) = ab = b \\ (ba)a = aa = a & b(aa) = ba = a \\ (aa)b = ab = b & a(ab) = ab = b \\ (bb)a = ba = a & b(ba) = ba = a \\ aaa = aa = a & bbb = bb = b \end{array}$$

Finally, R is a finite nonzero ring, $aba = a$ and $bab = b$ so for a and b, there is an element in R satisfying the hypothesis of the problem. However, R does not contain a multiplicative identity element 1, since $ab \neq ba$.
The issue here, is that the y satisfying $aya = a$ is not unique. $aba = a$ and $aaa = a$, where $a \neq b$ by assumption. Thus R need not contain an identity at all in this case.

Assume that R is a nonzero ring such that for each $x \in R$, there exists a *unique* $y \in R$ so $xyx = x$.

Let $x \in R$ be nonzero. Assume that there exists some $a \in R$ with $xa = 0$. Then

$$x(y + a)x = xyx + xax = xyx = x.$$

Now, because y is unique, we have that $y + a = y$ and so $a = 0$.

Thus, $xa = 0$ implies $a = 0$. Similarly $ax = 0$ also implies $a = 0$.

This shows that R contains no zero divisors.

Now, define

$$\begin{aligned}\varphi_x : R &\to R \\ y &\mapsto xy\end{aligned}$$

If φ_x is injective, then it is surjective (because R is finite) and so namely, every $y \in R$ can be written as xy. Namely, x is a left identity for R.

If φ_x is not injective, $\ker \varphi_x$ is not trivial. However, then $xa = 0$ for some $0 \neq a \in R$ which is a contradiction by the above.

Therefore, φ_x is injective and so it is an isomorphism. Namely, x is a left identity of R via the isomorphic association $y \sim_\varphi xy$.

Similarly, we can show that x is also a right identity and namely, we may call $x = 1 \in R$.

Now, assume that $ab = 1 \in R$.

We have already seen that R has no zero divisors, namely,

$$bab = b \implies bab - b = 0 \implies (ba - 1)b = 0$$

and so $ba = 1$ since b is not a zero divisor.

***Note that since R has no zero divisors, $xyx = x$ actually implies that $x(yx - 1) = 0$ and so $yx = 1$. Similarly, $(xy - 1)x = 0$ so $xy = 1$. Namely, every element of R is invertible and so R is a finite field.

✌

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

Solution.

(a) Let ξ be a primitive 15^{th} root of unity. Then, the roots of $f(x)$ are exactly $\xi^i \sqrt[15]{2}$. Namely, f is separbale and so $L/\mathbb{Q}$ is Galois.

Clearly $L = \mathbb{Q}(\xi, \sqrt[15]{2})$. Now, if $\varphi(n)$ denotes the Euler totient function, then

$$\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$$

and so there are 8 primitive 15^{th} roots of unity.

Therefore,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}] = [L : \mathbb{Q}(\xi)]8$$

and

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[15]{2})][\mathbb{Q}(\sqrt[15]{2}) : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[15]{2})]15$$

and so $[L : \mathbb{Q}] \geq 15 \cdot 8$. However, $[L : \mathbb{Q}] \leq 15 \cdot 8$, so we have that

$$[L : \mathbb{Q}] = 2^3 \cdot 3 \cdot 5.$$

(b) We have already found that $F = \mathbb{Q}(\xi)$ has degree 8 over $\mathbb{Q}$. Furthermore, this extension is Galois, since F is the splitting field of the seprable minimal polynomial of ξ, which has degree 8.

(c) We already know that $L/\mathbb{Q}$ is Galois. Let $G = \mathrm{Gal}(L/\mathbb{Q})$.

By the fundamental theorem of Galois theory, subfields of L $\mathbb{Q} \subset F \subset L$ correspond exactly to subgroups H of G satisfying $|H| = |\mathrm{Gal}(L/F)| = [L : F]$.

A subfield F of L is Galois over $\mathbb{Q}$ if and only if it corresponds to a subgroup H which is normal in G. Then $G/H = \mathrm{Gal}(F/\mathbb{Q})$ and $[G : H] = [F : \mathbb{Q}] = 8$.

Now, because any $\sigma \in G/H$, must permute the roots of the minimal polynomial of ξ, which are the primitive powers of ξ, we have that G/H will be abelian and namely cyclic.

Thus, $G/H \cong \mathbb{Z}_8$.

(d) This is a direct result of the fundamental theorem of Galois theory, which states that $G/H \cong \text{Gal}(F/\mathbb{Q})$ where $H = \text{Gal}(L/F)$.

However, since H is normal in G, HP_2 is a subgroup of G, where P_2 denotes a Sylow 2-subgroup of G.

Thus, because

$$|HP_2| = \frac{|H||P_2|}{|H \cap P_2|} = \frac{15 \cdot 8}{1} = 15 \cdot 8 = |G|,$$

by the isomorphism theorems, $G = HP_2$.

Thus, $G/H \cong P_2$ which is a subgroup of G.

***Note that it was not asked, but after (c), we actually have enough information to determine G.
Since, $H = \text{Gal}(L/F)$ is a normal subgroup of G of index 8, so $|H| = 15$.
By the Sylow theorems, $n_5 \equiv 1 \mod 5$ and $n_5|3$, and $n_3 \equiv 1 \mod 3$, and $n_3|5$, so $n_5 = n_3 = 1$ and so H has only normal Sylow subgroups and so it is abelian and isomoprhic to $\mathbb{Z}_{15}$.
However, normal Sylow subgroups of normal subgroups are normal (see **Fall 2011: Problem 5 Claim 3**), and so G has a normal Sylow 3 and a normal Sylow 5 subgroup.
Thus, G is abelain and

$$G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8$$

✌

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.

Solution. Let ξ be a ninth root of unity. Then if φ is the Euler totient function, $\varphi(9) = 3^2 - 3 = 6$, so $\mathbb{Q} \subset \mathbb{Q}(\xi) \subset F$, and $[\mathbb{Q}(\xi) : \mathbb{Q}] = 6$.

Now, $K = \mathbb{Q}(\xi)$ is clearly Galois over $\mathbb{Q}$ since it is the splitting field of a separable polynomial over $\mathbb{Q}$.

Now, by the fundamental theorem of Galois theory, subfields $\mathbb{Q} \subset K \subset F$ correspond exactly to subgroups $H \subset G = \mathrm{Gal}(F/\mathbb{Q})$, and an extension $K/\mathbb{Q}$ is Galois if and only if $H = \mathrm{Gal}(F/K)$ is normal in G.

Therefore, $H = \mathrm{Gal}(F/K)$ is normal in G, and since $[G : H] = |\mathrm{Gal}(K/\mathbb{Q})| = 6$ so $|H| = 10$.

Since in H $n_5 \equiv 1 \mod 5$ and $n_5 | 2$, $n_5 = 1$ so H has a normal Sylow 5-subgroup P_5.

Now, since any $\sigma \in G/H = \mathrm{Gal}(K/\mathbb{Q})$ permutes the 9^{th} roots of unity, it will be abelian.

Therefore, we obtain a subnormal series for G of

$$\{e\} \trianglelefteq P_5 \trianglelefteq H \trianglelefteq G$$

where $P_5 \cong \mathbb{Z}_5$ is abelian, $H/P_5 \cong \mathbb{Z}_2$ is abelian, and $G/H = \mathrm{Gal}(K/\mathbb{Q})$ is abelian.

So G is solvable.

✌

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

Solution. Write $x^n + 1 = (x - \xi)(x - \xi^2) \cdots (x - \xi^{n-1}) \in \mathbb{C}[x]$ where ξ is a primitive n^{th} root of unity.

Then, consider $f(x, y) = f(y) \in \mathbb{C}[x][y]$. Since $\mathbb{C}$ is a field, it is a UFD, so $\mathbb{C}[x]$ is a UFD and therefore, $\mathbb{C}[x][y]$ is a UFD.

Thus, we can apply Eisensten's with $p = x - \xi$. This is irreducible in $\mathbb{C}[x]$ since it is linear, and so it is prime because irreducible and prime are equivalent in a UFD.

Since p divides every coefficient of $f(y)$ except the leading coefficient, and p^2 does not divide the constant term of $f(y)$. So by Eisenstein, $f(x, y) = f(y)$ is irreducible in $\mathbb{C}[x][y] = \mathbb{C}[x, y]$. ✌