Algebra Qualifying Exam Solutions

MGSA

August 19, 2019

In order to make changes to this document, submit a pull request to `https://github.com/mgsa-usc/QualifyingExams` or email mgsa@usc.edu for help.

Contents

Fall 2012: Algebra Graduate Exam

Problem 1.

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

Proof. Sylow's theorems tell us that any group G must have

$$\begin{aligned} r_5 &\text{ Sylow 5-subgroups,} \\ r_7 &\text{ Sylow 7-subgroups, and} \\ r_{23} &\text{ Sylow 23-subgroups} \end{aligned}$$

where r_5, r_7, and r_{23} divide $5 \cdot 7 \cdot 23$, and $r_p \equiv 1 \bmod p$.

$$r_p = 1, 5, 7, 5 \cdot 7, 23, 5 \cdot 23, 7 \cdot 23, \text{ or } 5 \cdot 7 \cdot 23$$

considering the restriction on modulus, $r_5 \in \{1, 7 \cdot 23\}$, $r_7 = 1$, and $r_{23} = 1$. Let P and Q be the unique Sylow 23-subgroup and Sylow 7-subgroup respectively. Since $P \cap Q = 1$, $PQ \cong P \times Q$. Let R be a Sylow 5-subgroup.

Since $R \trianglelefteq G$ (why?), and R has a complement $P \times Q$, G is a semidirect product of R by $P \times Q$, that is $G = R \ltimes (P \times Q)$.

By Rotman Lemma 7.21, there is a homomorphism

$$\theta\colon \underbrace{R \to \mathrm{Aut}(P \times Q)}_{\mathbb{Z}_5 \to \mathbb{Z}_{22} \times \mathbb{Z}_6}.$$

But since $\gcd(5, 22) = \gcd(5, 6) = 1$, the only homomorphism is trivial. Therefore there is only one group of order $5 \cdot 7 \cdot 23$, the abelian group

$$G \cong \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{23}.$$

$\square$

Problem 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.

Proof. (From Nicolle)
R is a PID since F is a field, so by the *structure theorem for finitely generated modules over a PID*,

$$\begin{aligned} A &\cong T(A) \oplus R^n \\ B &\cong T(B) \oplus R^m \\ C &\cong R^t, \end{aligned}$$

were $T(M)$ denotes the torsion submodule of M. Since $A \otimes_R C \cong B \otimes_R C$, it follows that

$$(T(A) \oplus R^n) \otimes_R R^t \cong (T(B) \oplus R^m) \otimes_R R^t$$
$$(T(A) \otimes_R R^t) \oplus (R^n \otimes_R R^t) \cong (T(B) \otimes_R R^t) \oplus (R^m \otimes_R R^t)$$

Thus the free part of $A \otimes_R C$ is isomorphic to the free part of $B \otimes_R C$:

$$R^n \otimes_R R^t \cong R^m \otimes_R R^t,$$

so $n = m$. Similarly, the torsion submodules of $A \otimes_R C$ and $B \otimes_R C$ are isomorphic:

$$(T(A) \otimes_R R^t) \cong (T(B) \otimes_R R^t),$$

so $T(A) = T(B)$. Therefore,

$$A \cong T(A) \oplus R^n \cong T(B) \oplus R^m \cong B,$$

as desired.

As a counterexample, consider $A = B \oplus \mathrm{Ann}(C)$. Then

$$A \otimes_R C \cong B \otimes_R C \oplus \underbrace{\mathrm{Ann}(C) \otimes_R C}_{0} \cong B \otimes_R C,$$

but $A \ncong B$. □

Problem 3.

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

Note. This is identical to the Problem 5 in the 2014 fall exam.

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

First note that $y^3+xy = y(y^2+x)$ vanishes when $y=0$ or $x=-y^2$.
Case 1. Assume $y=0$. Then x^3+y^2 vanishes at $(0,0)$.
Case 2. Assume $x=-y^2$. Substituting this yields $(-y^2)^3+y^2 = y^2(-y^4+1)$, so the polynomial vanishes at $(0,0),(-1,1),(-1,-1),(1,i),(1,-i)$ Checking these:

$$\begin{aligned}
0^3+0^2 &= 0^3+0\cdot 0 &&= 0\\
(-1)^3+1^2 &= 1^3+(-1)\cdot 1 &&= 0\\
(-1)^3+(-1)^2 &= (-1)^3+(-1)(-1) &&= 0\\
1^3+i^2 &= i^3+1\cdot i &&= 0\\
1^3+(-i)^2 &= (-i)^3+1(-i) &&= 0.
\end{aligned}$$

Now it is enough to check that $f(x,y)$ vanishes on $\mathrm{Var}(I) = \{(0,0),(-1,1),(-1,-1),(1,i),(1,-i)\}$:

$$\begin{aligned}
f(0,0) &= \underbrace{(0+0)}_{0}(0^2+0^4-2) = 0\\
f(-1,1) &= \underbrace{(-1+1)}_{0}((-1)^2+1^4-2)\\
f(-1,-1) &= (-1+(-1))\underbrace{((-1)^2+(-1)^4-2)}_{0}\\
f(1,i) &= (1+i)\underbrace{(1^2+i^4-2)}_{0}\\
f(1,-i) &= (1+(-i))\underbrace{(1^2+(-i)^4-2)}_{0}.
\end{aligned}$$

Thus by Hilbert's Nullstellensatz, since f vanishes on $\mathrm{Var}(I)$, a power of f is in I. □

Problem 4.

For integers $n, m > 1$, let $A \subseteq M_n(\mathbb{Z}_m)$ 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?

Proof. The idea here it to show that A is semisimple, and so by Artin-Wedderburn can be written as

$$A \cong M_{n_1}(\Delta_1) \times \ldots \times M_{n_m}(\Delta_m)$$

where Δ_i is a field because it is finite and $n_i = 1$.

The converse is false. Let A be the ring generated by a single element with $n = m = 2$:

$$A = \left\langle \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

Then A is commutative, but $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ while $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. ☐

Problem 5.

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

Proof. Firstly, $F = \mathbb{Q}[\sqrt[3]{2}, \omega]$ where ω is a sixth root of unity. Then

$$\begin{aligned}
&[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 6, \text{ and} \\
&[F : \mathbb{Q}[\sqrt[3]{2}]] = \varphi(6) = 2,
\end{aligned}$$

so $[F : \mathbb{Q}] = [F : \mathbb{Q}[\sqrt[3]{2}]] \cdot [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 12$ and $\mathrm{Gal}(F/\mathbb{Q}) = 12$. Now consider the automorphisms

$$\tau : \begin{cases} \omega \mapsto \overline{\omega} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases} \quad \text{and} \quad \sigma : \begin{cases} \omega \mapsto \omega \\ \sqrt[3]{2} \mapsto \omega \sqrt[3]{2} \end{cases} .$$

Now τ is of order 2 and σ is of order 6, and the dihedral relation is satisfied:

$$\begin{aligned}
\sigma\tau\sigma\tau(\omega) &= \sigma\tau\sigma(\overline{\omega}) &&= \sigma\tau(\overline{\omega}) &&= \sigma(\omega) &&= \omega \\
\sigma\tau\sigma\tau(\sqrt[3]{2}) &= \sigma\tau\sigma(\sqrt[3]{2}) &&= \sigma\tau(\omega\sqrt[3]{2}) &&= \sigma(\overline{\omega}\sqrt[3]{2}) &&= \underbrace{\overline{\omega}\omega}_{1}\sqrt[3]{2} = \sqrt[3]{2}.
\end{aligned}$$

$\square$

Problem 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.

Proof. Let r_p denote the number of Sylow p-subgroups of G. Sylows theorems state that r_p divides $2^2 \cdot 3 \cdot 7^2$, so

$$\begin{aligned}
r_2 &\in \{1, 3, 7, 3 \cdot 7, 7^2, 3 \cdot 7^2\} \\
r_3 &\in \{1, 2, 2^2, 7, 2 \cdot 7, 2^2 \cdot 7, 7^2, 2 \cdot 7^2, 2^2 \cdot 7^2\} \\
r_7 &\in \{1, 2, 2^2, 3, 2 \cdot 3, 2^2 \cdot 3\}
\end{aligned}$$

also $r_p \equiv 1 \bmod p$, so

$$\begin{aligned}
r_2 &\in \{1, 3, 7, 3 \cdot 7, 7^2, 3 \cdot 7^2\} \\
r_3 &\in \{1, 2^2, 7, 2^2 \cdot 7, 7^2, 2^2 \cdot 7^2\} \\
r_7 &= 1
\end{aligned}$$

This means that there is a unique—and thus normal—Sylow 7-subgroup, call it $N \cong \mathbb{Z}_7$. Therefore $G \cong N \rtimes K$ where K is a subgroup of order 12.

Now a group is solvable if it has a normal series whose factor groups are cyclic of prime order. Since K is solvable, it has a normal series

$$K = K_0 \leq K_1 \leq K_2 \leq \ldots \leq K_n = 1.$$

where K_i/K_{i+1} is a cyclic group of prime order. Moreover, since N is normal, NK_{i+1} is a subgroup of NK_i. Thus

$$G = NK_0 \leq NK_1 \leq NK_2 \leq \ldots \leq \underbrace{NK_n}_{N} \leq 1$$

is a normal series of G where $NK_i/NK_{i+1} \cong K_i/K_{i+1}$ is a cyclic group of prime order for $i \in \{0, 1, ..., n-1\}$, and $N/1 \cong N \cong \mathbb{Z}_7$ is a cyclic group of prime order. Therefore G is solvable. $\square$

Spring 2012: Algebra Graduate Exam

Problem 1.

Let I be an ideal of $R = \mathbb{C}[x_1, \ldots, x_n]$. Show that $\dim_{\mathbb{C}}(R/I)$ is finite if and only if I is contained in only finitely many maximal ideals of R.

Proof. $\square$

Problem 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.

Proof. We'll start by using Sylow's theorems. Firstly, let r_p denote the number of Sylow p-subgroups. Since p divides $|G|$,

$$\begin{aligned} r_{19} &\in \{1, 7, 7^2, 11, 11 \cdot 7, 11 \cdot 7^2, 11^2, 11^2 \cdot 7, 11^2 \cdot 7^2\}, \\ r_{11} &\in \{1, 7, 7^2, 19, 19 \cdot 7, 19 \cdot 7^2\}, \\ r_7 &\in \{1, 11, 11^2, 19, 19 \cdot 11, 19 \cdot 11^2\}. \end{aligned}$$

Since $r_p \cong 1 \bmod p$, we can further refine this to

$$\begin{aligned} r_{19} &= 1, \\ r_{11} &\in \{1, 19 \cdot 7\}, \\ r_7 &= 1. \end{aligned}$$

This means that we have unique subgroups H_{19} and H_7 of orders 19 and 7 respectively. Since H_7 and H_{19} are unique and thus normal, the product of H_7 and H_{19} forms a normal subgroup, call it N. Since $H_7 \cap H_{19} = \{e\}$, $H_7 H_{19} \cong H_7 \times H_{19}$, where H_{19} is abelian because it is cyclic, and H_7 is abelian because all groups of order p^2 are abelian. Thus $N \cong \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19}$ or $N \cong \mathbb{Z}_{49} \times \mathbb{Z}_{19}$.

Since N and H_{11} are complementary, that is $N \cap H_{11} = \{e\}$ and $|N||H_{11}| = |G|$, G can be realized as the semidirect product of N and H_{11}

$$G = N \rtimes H_{11}.$$

Thus it is enough to consider the possible structures of the semidirect product.

Case 1. Assume $N \cong \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19}$. Consider homomorphisms $\varphi \colon H_{11} \to \mathrm{Aut}(N)$, noting that

$$\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19}) \cong \mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7) \times \mathrm{Aut}(\mathbb{Z}_{19}) \cong \underbrace{\mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7)}_{\text{order } 48 \cdot 42} \times \mathbb{Z}_{18}.$$

Since $\gcd(11, 48 \cdot 42 \cdot 18) = 1$, the only homomorphism is trivial. So the semidirect product is direct

$$G \cong \mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{19} \times H_{11}$$

Case 2. Assume $N \cong \mathbb{Z}_{49} \times \mathbb{Z}_{19}$. Consider homomorphisms $\varphi \colon H_{11} \to \mathrm{Aut}(N)$, noting that

$$\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}_{49} \times \mathbb{Z}_{19}) \cong \mathrm{Aut}(\mathbb{Z}_{49}) \times \mathrm{Aut}(\mathbb{Z}_{19}) \cong \underbrace{\mathrm{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_7)}_{\text{order } 7 \cdot 6} \times \mathbb{Z}_{18}.$$

Since $\gcd(11, 7 \cdot 6 \cdot 18) = 1$, the only homomorphism is trivial. So the semidirect product is direct

$$G \cong \mathbb{Z}_{49} \times \mathbb{Z}_{19} \times H_{11}$$

Since $|H_{11}| = 11^2$, it is abelian, so by the fundamental theorem of abelian groups, G is isomorphic to

$$\begin{aligned} &\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \times \mathbb{Z}_{19}, \\ &\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_{121} \times \mathbb{Z}_{19}, \\ &\mathbb{Z}_{49} \times \mathbb{Z}_{11} \times \mathbb{Z}_{11} \times \mathbb{Z}_{19}, \qquad \text{or} \\ &\mathbb{Z}_{49} \times \mathbb{Z}_{121} \times \mathbb{Z}_{19}. \end{aligned}$$

$\square$

Problem 3.

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

Note: Since x is not a zero left divisor, if $xy = 0$ for $y \in F[G]$ then $y = 0$.

Proof. Since $\operatorname{char} F$ does not divide $|G|$, by Mashke's Theorem, $F[G]$ is semisimple, so by the Artin-Wedderburn theorem,

$$F[G] \cong M_{n_1}(D_1) \times M_{n_2}(D_2) \times \ldots \times M_{n_k}(D_k)$$

where $M_{n_i}(D_i)$ is an n_i-by-n_i matrix ring over a division ring D_i.

Thus any $\alpha = \sum_{g \in G} a_g g \in F[G]$ maps under the isomorphism to

$$\varphi(\alpha) = (a_1, a_2, \ldots, a_k) \in M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k).$$

Now suppose for the sake of contradiction that some a_i is not invertible for some i; without loss of generality, say that $i = 1$. Then there exists some $b \neq 0 \in M_{n_1}(D_1)$ such that $a_1 b = 0$ (why?), and

$$(a_1, a_2, \ldots, a_k) \cdot (b, 0, 0, \ldots, 0) = (\underbrace{a_1 b}_{0}, 0, 0, \ldots, 0).$$

Therefore $\varphi^{-1}(a_1, a_2, \ldots, a_k) = x$ is a left divisor.

Thus in order for x not to be a left divisor, all a_i must be invertible. Thus $x^{-1} = \varphi^{-1}(a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1})$. $\square$

Problem 4.

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

Proof. Let $q(y) = y^4 + 2y^3 + 3y^2 + 2y + 1$ so that $q(x^2) = p(x)$. Since $\deg(q) = 4$, q is solvable by radicals with roots $\{a_1, a_2, a_3, a_4\}$ expressible as radicals. Thus p is also solvable by radicals with roots $\{\pm\sqrt{a_1}, \pm\sqrt{a_2}, \pm\sqrt{a_3}, \pm\sqrt{a_4}\}$. $\square$

Problem 5.

Let R be a commutative ring with 1 and let $x_1, \ldots, x_n \in R$ so that $x_1 y_1 + \ldots + x_n y_n = 1$ for some $y_j \in R$. Let $A = \{(r_1, r_2, \ldots, r_n) \in R^n \mid x_1 r_1 + \ldots + x_n r_n = 0\}$. Show that

(i) $R^n \cong_R A \oplus R$,

(ii) A has n generators, and

(iii) when $R = F[x]$ for F a field, then A_R is free of rank $n-1$.

Proof. First consider the map $\varphi\colon R^n \to R$ that sends $(r_1, \ldots, r_n) \mapsto x_1 r_1 + \ldots + x_n r_n$ so that $\varphi(y_1, \ldots, y_n) = 1$ and thus is surjective. Notice also that $\ker(\varphi) = A$. So the short exact sequence splits:

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

(i) Since R, as a module over itself, is free and thus projective, so $R^n \cong_R A \oplus R$.

(ii) (?)

(iii) If $R = F[x]$, then R is a PID. Thus by the structure theorem for finitely generated modules over a PID,

$$A \cong T(A) \oplus R^k$$

and since $R^n \cong A \oplus R = T(A) \oplus R^{k+1}$, $T(A) \cong 0$ and $k = n-1$, so $\text{rank}(A) = \text{rank}(R^{n-1}) = n-1$.

□

Problem 6.

For p a prime, let F_p be the field of p elements and K and extension field of F_p of dimension 72.

(i) Describe the possible structures of $\mathrm{Gal}(K/F_p)$.

(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?

Proof. □

Fall 2013: Algebra Graduate Exam

Problem 1.

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

Proof. First note that the only normal subgroup of S_5 is A_5, which has order 60.

Case 1. Assume $|H| = 15$. Then H must have both a Sylow 5-subgroup and a Sylow 3-subgroup, and thus H must contain a 5-cycle and a 3-cycle. Since neither of the subgroups generated by these elements is normal in S_5, their product is not a subgroup. Therefore any subgroup of S_5 containing a 5-cycle and a 3-cycle has more than 15 elements.

Case 2. Assume $|H| = 20$. Of course, H must have both a Sylow 5-subgroup and a Sylow 2-subgroup, so

Case 2a. Assume the Sylow 2-subgroup contains a transposition. Then a 5-cycle and a transposition generates S_5, so $|H| = 120$, a contradiction.

Case 2b. If the Sylow 2-subgroup does not contain a transposition, it must contain element of the form $(s_1 s_2)(s_3 s_4)$. (...?)

Case 3. Assume $|H| = 30$. Thus H has a Sylow 5-subgroup, a Sylow 3-subgroup, and a Sylow 2-subgroup. Based on Case 2a, if H has a Sylow 2-subgroup, it must be of the form $(s_1 s_2)(s_3 s_4)$ (...?)

□

Problem 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.

Proof. □

Problem 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 $\alpha \in \mathrm{Var}(I)$, $A(\alpha) = 0_{n\times n}$, show that for some integer m, $A^m \in M_n(I)$.

Proof. □

Problem 4.

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

Proof. $\square$

Problem 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 $i \in \mathbb{Z}/p\mathbb{Z}$.

Proof. $\square$

Problem 6.

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 $\mathrm{Gal}(L/K)$.

Proof. $\square$

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 $\varphi\colon K \to \operatorname{Aut}(N)$ 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 $\operatorname{Aut}(N) \cong GL_2(p)$, 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 $\operatorname{Aut}(N)$ is of order $\phi(p^2) = p(p-1)$. Since p^2 is a power of a prime, $\operatorname{Aut}(N) \cong \mathbb{Z}_{p(p-1)}$. 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 $2p^2$.

$\square$

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. $\square$

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

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

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

$$p(1,1,1) = \underbrace{1^{16}1^{25}1^{81}}_{1} \underbrace{-1^7 1^{15}}_{-1} \underbrace{-1 \cdot 1^9}_{-1} \underbrace{+1^5}_{+1} = 0,$$

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. $\square$

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 R contains an identity element and that for $a, b \in R$ if $ab = 1$ then $ba = 1$.

Proof. $\square$

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 $\mathbb{Q}$.

$\square$

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,

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

$\square$

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. $\square$