MA553 Past Qualifying Examinations

Carlos Salinas

December 27, 2015

1 January 2007

Problem 1.1. Let $(G, \cdot)$ be a group. Show that G is Abelian whenever $\operatorname{Aut}(G)$ is a cyclic group under composition.

Proof. Suppose that $\operatorname{Aut}(G)$ is cyclic. Then $\operatorname{Inn}(G) < \operatorname{Aut}(G)$ is cyclic. But $\operatorname{Inn}(G) \cong G/Z(G)$. Thus, G is Abelian by the following lemma.

Lemma 1. *Let $(G, \cdot)$ be a group. If $G/Z(G)$ is cyclic, then G is Abelian.*

Proof of lemma. Suppose that $G/Z(G)$ is cyclic. Then $G/Z(G) = \langle \bar{x} \rangle$ for some representative $x \in G$. This means that for any $g \in G$, we can write $g = x^k z$ for some positive integer k, for some $z \in Z(G)$. Let $g_1, g_2 \in G$. Then, by the following obvious algebraic manipulations

$$g_1 g_2 = x^{k_1} z_1 x^{k_2} z_2 = z_1 x^{k_1+k_2} z_2 = z_2 x^{k_2+k_1} z_1 = z_2 x^{k_2} x^{k_1} z_1 = (x^{k_2} z_2)(x^{k_1} z_1) = g_2 g_1,$$

we see that G is Abelian. ♣

■

Problem 1.2. Let $(G, \cdot)$ be an Abelian group. The *torsion subgroup of* G is defined as the collection of elements of finite order:

$$\operatorname{Tor}(G) := \{ g \in G \mid g^m = e \text{ for some integer } m > 0 \}.$$

(a) Show that the quotient group $G/\operatorname{Tor}(G)$ is *torsion free*, i.e., it contains no nontrivial elements of finite order.
(b) Show that $\operatorname{Tor}(G)$ is finite whenever G is finitely generated. (Do not assume that G is finite.)

Proof. (a) (Presumably the torsion subgroup is a normal subgroup of G.) Define $T := \operatorname{Tor}(G/\operatorname{Tor}(G))$. We will show that $T = \bar{e}$. It is clear that $\langle \bar{e} \rangle \subset T$ thus, we need only show that $T \subset \langle \bar{e} \rangle$, i.e., if $t \in T$ then $g = \bar{e}$. Let $\bar{g} \in T$. Then $\bar{g} \in G/\operatorname{Tor}(G)$ and $\bar{g}^m = \bar{e}$ for some positive integer m. But $\bar{g}^m = \bar{e}$ implies that $g^m \operatorname{Tor}(G) = \operatorname{Tor}(G)$, i.e., $g^m \in \operatorname{Tor}(G)$. Thus, $(g^m)^n = g^{mn} e$ for some positive integer n. Thus, $g \in \operatorname{Tor}(G)$ so we must have $\bar{g} = \bar{e}$.

(b) Suppose that G is finitely generated. By the fundamental theorem of finitely generated Abelian groups, $G \cong \mathbb{Z}^r \times Z_{s_1} \times \cdots \times Z_{s_n}$ for positive integers $r, s_1, ..., s_n$. It suffices to show that $\mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n} = \operatorname{Tor}(G)$ (once we have demonstrated this, note that $|\mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n}| = s_1 \cdots s_n < \infty$). It is clear that $\mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n} \subset \operatorname{Tor}(G)$ since every element of $\mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n}$ has finite order, i.e., for any $(\mathbf{1}, z_1, ..., z_n) \in \mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n}$, we have $z = (\mathbf{1}, z_1, ..., z_n)^{s_1 \cdots s_n} = (\mathbf{1}, 1, ..., 1)$ (as a consequence of Lagrange's theorem). Now, suppose $z := (\mathbf{z}, z_1, ..., z_n) \in \operatorname{Tor}(G)$. Then $z^m = (\mathbf{1}, 1, ..., 1)$ for some positive integer m. Since every non-identity element of $\mathbb{Z}^r$ has infinite order, $\mathbf{z} = \mathbf{1}$ and $s_i \mid k$ for all i. Thus $z \in \mathbf{1} \times Z_{s_1} \times \cdots Z_{s_n}$. Thus, $|\operatorname{Tor}(G)| = s_1 \cdots s_n$ so $\operatorname{Tor}(G)$ is indeed finite. ■

Problem 1.3. Let $(G, \cdot)$ be a group of order $|G| = 351$. Show that G is solvable.

Proof. The best plan of attack is to use Sylow's theorem. First, let us factor the order of G into powers of primes, $|G| = 351 = 3^3 \cdot 13$. In light of this factorization, it suffices to show that either $|\operatorname{Syl}_{13}(G)| = 1$ or $|\operatorname{Syl}_3(G)| = 1$ and hence, the unique Sylow-13 (or Sylow-3) subgroup will be a normal subgroup of G. By Sylow's theorem, $n_{13} \equiv 1 \pmod{13}$ and $n_{13} \mid 3^3$. Thus, $n_{13} = 1$ or 27. Suppose $n_{13} = 27$. Then G contains $12 \times 27 = 324$ elements of order 13 so there are $351 - 324 - 1 = 26$ elements remaining. This implies that $n_3 = 1$. Thus, $P_3 \in \operatorname{Syl}_3(G)$ is the unique Sylow-3 subgroup of G hence, is normal. Thus, $G \rhd P_3$ so G/P_3 is a group. Incidentally, $G/P_3 \cong Z_{13}$ hence, solvable and P_3 is a p-group, hence solvable. Thus, G is solvable.

On the other hand, if $n_{13} = 1$ then $P_{13} \in \operatorname{Syl}_{13}(G)$ is the unique Sylow-13 subgroup of G hence, normal in G. Since P_{13} is a p-group, it is solvable. Moreover, G/P_{13} is a group of order 3^3, i.e., a p-group, hence, solvable. Thus, G is solvable.

In either case, we have shown that G must be solvable. ■

Problem 1.4. Let $(G, \cdot)$ be a group, and $H < G$ a subgroup of finite index. Show that there exists a normal subgroup $N \lhd G$ contained in H which is also of finite index. (Do not assume that G is finite.)

Proof. Suppose $H < G$ is a subgroup of finite index, i.e., H partitions G into a finite number of cosets, say $G/H \coloneqq \{H, g_1H, ..., g_{k-1}H\}$. Define a homomorphism $\varphi\colon G \to S_{G/H}$ by $g \mapsto gH$ (this is clearly a homomorphism: take $g_1, g_2 \in G$ then $\varphi(g_1g_2) = g_1g_2H = (g_1H)(g_2H) = \varphi(g_1)\varphi(g_2)$). Thus, $\ker\varphi \lhd G$ of finite index (in particular, by the 1st isomorphism theorem and Lagrange's theorem $|G : \ker\varphi| \mid |S_{G/H}| = |S_k| = k!$). Thus, it suffices to show that $\ker\varphi < H$. But this is clear since, if $g \in \ker\varphi$ then $gH = H$ hence, $g \in H$. ■

Problem 1.5. Let $(G, \cdot)$ be a finite group, and $\varphi\colon G \to G$ be a group homomorphism. Show that for all normal Sylow p-subgroups $P \lhd G$ we have $\varphi(P) < P$.

Proof. Suppose $|G| < \infty$ and let $P \in \operatorname{Syl}_p(G)$ be normal in G. Then P is unique of order p^α for some α. By the 1st isomorphism theorem, $\varphi(P) \mid p^\alpha$ so $\varphi(P)$ must be contained in a Sylow p-subgroup of G. Since P is the unique Sylow p-subgroup of G, $\varphi(P) < P$. ■

Problem 1.6. Let $(R, +, \cdot)$ be a commutative ring with $1 \neq 0$.

(a) Show that R is an integral domain if and only if (0) is a prime ideal.
(b) Show that R is a field if and only if (0) is a maximal ideal.

Proof. (a) $\Longleftarrow$ Suppose that (0) is a prime ideal. Then $R/(0)$ is a domain. But $R/(0) \cong R$ (canonically i.e., the map $\bar{r} \mapsto r$ is a bijective homomorphism) hence, R is a domain.

$\Longleftarrow$ Conversely, suppose that R is a domain.

(b) ■

Problem 1.7. let $(R, +, \cdot)$ be a unique factorization domain. Choose an irreducible element $p \in R$, and define the *localization at p* as the ring of fractions $R_p = D^{-1}R$ with respect to the multiplicative set $D = R - (p)$. Show that R_p is a principal ideal domain.

Proof. ■

Problem 1.8. Let $(F, +, \cdot)$ be a field, and $F(\theta)/F$ be a finite, separable extension. Let L be the splitting field of the minimal polynomial $m_{\theta,F}(x) \in F[x]$. Prove that for every prime p dividing the degree $[L : F]$, there exists a field K such that $F \subset K \subset L$, $[L : K] = p$, and $L = K(\theta)$.

Proof. ■

Problem 1.9. Let $(\mathbb{F}_p, +, \cdot)$ be a finite field whose Cardinality p is prime. Fix a positive integer n which is not divisible by p, and let ζ_n be a primitive nth root of unity. Show that $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = \alpha$ is the least positive integer such that $p^\alpha \equiv 1 \pmod{n}$.

Proof. ■

Problem 1.10. Prove that the Galois group of the splitting field over $\mathbb{Q}$ of $f(x) = x^4 + 4x^2 + 2$ is a cyclic group.

Proof. ■

2 Spring 2008

Problem 2.1. Let $(G, \cdot)$ be a group, $(H, +)$ be an Abelian group, and $\varphi\colon G \to H$ be a group homomorphism. If N is a subgroup such that $\ker\varphi < N < G$, show that $N \lhd G$ is a normal subgroup.

Proof. Let N be a subgroup of G containing $\ker\varphi$. Then we must show that for any $g \in G$, $gNg^{-1} \subset N$. First we observe that, since $\ker\varphi \lhd G$, then $\ker\varphi \lhd N$ since for any $g \in N$, g is also in G so that $g(\ker\varphi)g^{-1} = \ker\varphi \subset N$. Thus, $\ker\varphi \lhd N$. By the first isomorphism theorem[1], $G/\ker\varphi \cong H$ hence, $G/\ker\varphi$ is Abelian. Moreover, $N/\ker\varphi < G/\ker\varphi$ hence, $N/\ker\varphi \lhd G/\ker\varphi$. It follows immediately from the lattice isomorphism theorem[2] (this is essentially the UMP of the quotient by a group) that $N \lhd G$. ■

Problem 2.2. Let $(G, \cdot)$ be a finite Abelian group of even order, i.e., $|G| = 2k$ for some $k \in \mathbb{N}$.

(a) For k odd, show that G has exactly one element of order 2.
(b) Does the same happen for k even? Prove or give a counterexample.

Proof. (a) This problem is most easily proven using Cauchy's theorem[3]. Suppose that k is odd. If $k = 1$, $G \cong Z_2$ and we are done (Z_2 contains only one nontrivial element and its order is 2). Otherwise $k > 2$. Then by Cauchy's theorem we are guaranteed that there exists an element $g \in G$ of order 2. Suppose h is another element (distinct from g) of order 2. Since 2 is the smallest prime number dividing the order of G, by a corollary to Cayley's theorem[4], $\langle g\rangle$ is a normal subgroup of G so $G/\langle g\rangle$ is a group. Moreover, since $h \neq g$, then $\bar{h} \neq \bar{e}$ and $2 \geq |\bar{h}| > 1$ implies that $|\bar{h}| = 2$. But $2 \nmid k = |G/\langle g\rangle|$ contradicting Lagrange's theorem. It follows that G must have exactly one element of order 2.

(b) No. Here is the simplest counterexample: Consider the direct product $Z_2 \times Z_2$. The elements $(1, 0)$ and $(0, 1)$ are elements of order 2, but are not equivalent. ■

Problem 2.3. Let $(G, \cdot)$ be a finite group of odd order, and $H \lhd G$ be a normal subgroup of prime order $|H| = 17$. Show that $H < Z(G)$.

Proof. Let G act on H by conjugation, i.e., the map $\varphi\colon G \times H \to H$ defined by the rule $\varphi(g, h) := ghg^{-1}$ determines a group action on H. First, we verify that φ indeed defines a group action on H: First, observe that for $e_G \in G$ the identity element, $\varphi(e_G, h) = e_G h e_G^{-1} = h$; next, if $g_1, g_2 \in G$ then

$$\varphi(g_1, \varphi(g_2, h)) = \varphi(g_1, g_2hg^{-1}) = g_1g_2hg_2^{-1}g_1 = g_1g_2h(g_1g_2)^{-1} = \varphi(g_1g_2, h).$$

Lastly, φ is clearly well-defined in the sense $\varphi(g, h) \in H$ for all $g \in G$, $h \in H$. Thus, φ is a group action. Now, let us ask what the kernel of this action is. Thus group action φ, induces a group homomorphism $\varphi'\colon G \to \operatorname{Aut}(H)$ given by $\varphi'(g) := \operatorname{Eval}(\varphi, g)$. Now, since $|H| = 17$, $H \cong Z_{17}$, hence is cyclic. Thus, $\operatorname{Aut}(H) \cong (\mathbb{Z}/17\mathbb{Z})^\times \cong Z_{16}$. Now, since $|\varphi'(G)| \mid |G|$, $|\varphi'(G)|$ is odd. But $\varphi'(G) < \operatorname{Aut}(H)$ so, by Lagrange's theorem, $|\varphi'(G)| \mid 16$. Thus, $|\varphi'(G)| = 1$, i.e., φ' is the trivial homomorphism, i.e., $\varphi(g, h) = ghg^{-1} = h = \varphi(1, h)$. Thus, $H < Z(G)$. ■

[1] Theorem 16 of Dummit and Foote §3, p. 99.
[2] Theorem 20 of Dummit and Foote §3, p. 99.
[3] Theorem 11 of Dummit and Foote §3, p. 93
[4] Corollary 5 of Dummit and Foote §4, p. 121

Problem 2.4. Let $(G, \cdot)$ be a finite group. Show that there exists a positive integer n such that G is isomorphic to a subgroup of A_n, the alternating group on n letters. [*Hint:* Show that A_n contains a copy of S_{n-1} when $n \geq 3$.]

Proof. Let $n - 2 \coloneqq |G|$. If $n - 2 = 1$ or 2, $G \cong 0$ (the trivial group) or $G \cong Z_2$, both of which are exactly A_1 and A_2. Suppose $n - 2 \geq 3$. By Cayley's theorem, G imbeds into S_{n-1}. Now, define a homomorphism

$$\varphi(\sigma) \coloneqq \begin{cases} \sigma & \text{if } \sigma \text{ is even} \\ \sigma(n+1\ n+2) & \text{if } \sigma \text{ is odd} \end{cases}.$$

We check that this is in fact a homomorphism. Let $\sigma, \tau \in G$. Then

$$\varphi(\sigma\tau) = \begin{cases} \sigma\tau & \text{if } \sigma\tau \text{ is even} \\ \sigma\tau(n+1\ n+2) & \text{if } \sigma\tau \text{ is odd} \end{cases}.$$

But $\sigma\tau$ is odd if and only if σ or τ is odd and $\sigma\tau$ is even if and only if τ is even. ■

Problem 2.5. Let $(G, \cdot)$ be a group of order $|G| = 200$.

(a) Show that G is solvable.
(b) Show that G is the semidirect product of two p-subgroups.

Proof. (a) First we factor the order of the group G, $|G| = 200 = 2^3 \cdot 5^2$. Now we will make use of Sylow's theorem to show that G has at least one normal p-subgroup.

(b) ■

Problem 2.6. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be commutative rings with $1 \neq 0$, and let $\varphi\colon R \to S$ be a surjective ring homomorphism. Assuming that R is local, i.e., it has a unique maximal ideal, show that S is also local.

Proof. ■

Problem 2.7. Let $(R, +, \cdot)$ be a principal ideal domain.

(a) Show that every maximal ideal in R is a prime ideal.
(b) Must every prime ideal in R be a maximal ideal? Prove or give a counterexample.

Proof. ■

Problem 2.8. Let L/F be a Galois extension of degree $[L : F] = 2p$ where p is an odd prime.

(a) Show that there exists a unique quadratic subfield E, i.e., $F \subset E \subset L$ and $[E : F] = 2$.
(b) Does there exist a unique subfield K of index 2, i.e., $F \subset K \subset L$ and $[L : K] = 2$? Prove or give a counterexample.

Proof. ■

Problem 2.9. Fix a prime p, and consider the Artin–Schreier polynomial $f(x) = x^p - x - 1$.

(a) Let $\mathbb{F}_p(f)$ be the splitting field of $f(x)$ over $\mathbb{F}_p$. Show that $\text{Gal}(\mathbb{F}_p(f)/\mathbb{F}_p) \cong Z_p$.

(b) Prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. ∎

Problem 2.10. Determine the Galois group of the splitting field over $\mathbb{Q}$ of $f(x) = x^4 + 4$.

Proof. ∎

3 August, 2015

Problem 3.1.

Proof. ∎

3.1 August 2010