

# MA553 Past Qualifying Examinations

Carlos Salinas

January 5, 2016

# 1 January 2007

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

*Proof.* Suppose that  $\text{Aut}(G)$  is cyclic. Then  $\text{Inn}(G) < \text{Aut}(G)$  is cyclic. But  $\text{Inn}(G) \cong G/Z(G)$ . 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:

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

- (a) Show that the quotient group  $G/\text{Tor}(G)$  is *torsion free*, i.e., it contains no nontrivial elements of finite order.
- (b) Show that  $\text{Tor}(G)$  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  $T := \text{Tor}(G/\text{Tor}(G))$ . 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  $\bar{g} \in G/\text{Tor}(G)$  and  $\bar{g}^m = \bar{e}$  for some positive integer  $m$ . But  $\bar{g}^m = \bar{e}$  implies that  $g^m \text{Tor}(G) = \text{Tor}(G)$ , i.e.,  $g^m \in \text{Tor}(G)$ . Thus,  $(g^m)^n = g^{mn} e$  for some positive integer  $n$ . Thus,  $g \in \text{Tor}(G)$  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  $r, s_1, \dots, s_n$ . It suffices to show that  $\mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n} = \text{Tor}(G)$  (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  $\mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n} \subset \text{Tor}(G)$  since every element of  $\mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n}$  has finite order, i.e., for any  $(\mathbf{1}, z_1, \dots, z_n) \in \mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n}$ , we have  $z = (\mathbf{1}, z_1, \dots, z_n)^{s_1 \cdots s_n} = (\mathbf{1}, 1, \dots, 1)$  (as a consequence of Lagrange's theorem). Now, suppose  $z := (\mathbf{z}, z_1, \dots, z_n) \in \text{Tor}(G)$ . Then  $z^m = (\mathbf{1}, 1, \dots, 1)$  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  $z \in \mathbf{1} \times Z_{s_1} \times \cdots \times Z_{s_n}$ . Thus,  $|\text{Tor}(G)| = s_1 \cdots s_n$  so  $\text{Tor}(G)$  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  $|\text{Syl}_{13}(G)| = 1$  or  $|\text{Syl}_3(G)| = 1$  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,  $P_3 \in \text{Syl}_3(G)$  is the unique Sylow-3 subgroup of  $G$  hence, is normal. Thus,  $G \triangleright P_3$  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  $P_{13} \in \text{Syl}_{13}(G)$  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  $N \triangleleft G$  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  $G/H := \{H, g_1H, \dots, g_{k-1}H\}$ . Define a homomorphism  $\varphi: G \rightarrow S_{G/H}$  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,  $\ker \varphi \triangleleft G$  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  $\varphi: G \rightarrow G$  be a group homomorphism. Show that for all normal Sylow  $p$ -subgroups  $P \triangleleft G$  we have  $\varphi(P) < P$ .

*Proof.* Suppose  $|G| < \infty$  and let  $P \in \text{Syl}_p(G)$  be normal in  $G$ . Then  $P$  is unique of order  $p^\alpha$  for some  $\alpha$ . 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)  $\Leftarrow$  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.

$\Leftarrow$  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  $\zeta_n$  be a primitive  $n$ th 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  $\varphi: G \rightarrow H$  be a group homomorphism. If  $N$  is a subgroup such that  $\ker \varphi < N < G$ , show that  $N \triangleleft G$  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  $\ker \varphi \triangleleft G$ , then  $\ker \varphi \triangleleft N$  since for any  $g \in N$ ,  $g$  is also in  $G$  so that  $g(\ker \varphi)g^{-1} = \ker \varphi \subset N$ . Thus,  $\ker \varphi \triangleleft N$ . By the first isomorphism theorem<sup>1</sup>,  $G/\ker \varphi \cong H$  hence,  $G/\ker \varphi$  is Abelian. Moreover,  $N/\ker \varphi < G/\ker \varphi$  hence,  $N/\ker \varphi \triangleleft G/\ker \varphi$ . It follows immediately from the lattice isomorphism theorem<sup>2</sup> (this is essentially the UMP of the quotient by a group) that  $N \triangleleft G$ . ■

**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<sup>3</sup>. 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<sup>4</sup>,  $\langle g \rangle$  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  $H \triangleleft G$  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  $\varphi: G \times H \rightarrow H$  defined by the rule  $\varphi(g, h) := ghg^{-1}$  determines a group action on  $H$ . First, we verify that  $\varphi$  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

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

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

<sup>1</sup>Theorem 16 of Dummit and Foote §3, p. 99.

<sup>2</sup>Theorem 20 of Dummit and Foote §3, p. 99.

<sup>3</sup>Theorem 11 of Dummit and Foote §3, p. 93

<sup>4</sup>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  $n - 2 := |G|$ . 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

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

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  $\sigma$  or  $\tau$  is odd and  $\sigma\tau$  is even if and only if  $\tau$  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  $\varphi: R \rightarrow S$  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 MA 553: Midterm, Fall 2015

In full detail now:

**Problem 3.1.** (a) Show, for any abelian group, the map  $x \mapsto x^{-1}$  is an automorphism.

(b) Show, for any  $n$ , the dihedral group  $D_{2n}$  of order  $2n$ , satisfies  $D_{2n} \cong Z_2 \rtimes Z_n$ .

*Proof.* (a) Let  $G$  be an abelian group and define the map  $\varphi: G \rightarrow G$  by  $\varphi(x) := x^{-1}$ . Then, for any  $x, y \in G$ , we have

$$\begin{aligned}\varphi(xy) &= (xy)^{-1} \\ &= y^{-1}x^{-1} \\ &= x^{-1}y^{-1} \\ &= \varphi(x)\varphi(y).\end{aligned}$$

Hence,  $\varphi$  is a homomorphism.

Next, we will show that  $\varphi$  is in fact an automorphism. To that end, we must show that  $\varphi$  is one-to-one and onto.

First, we show  $\varphi$  is one-to-one. Let  $x \in \ker \varphi$ . Then  $\varphi(x) = x^{-1} = e$ . Then we have  $x^{-1}x = x$ . But  $x^{-1}x = e$  so  $x = e$ . Thus,  $\ker \varphi = \{e\}$  and  $\varphi$  must be injective.

To see that  $\varphi$  is onto, take  $x \in G$  then  $\varphi(x^{-1}) = (x^{-1})^{-1} = x$ . Thus,  $\varphi$  is surjective and we conclude that  $\varphi \in \text{Aut}(G)$ .

(b) Recall that the dihedral group of order  $2n$  is the group

$$G := D_{2n} = \langle r, s \mid r^n = s^2 = e \text{ and } srs^{-1} = r^{-1} \rangle.$$

Now, note that the subgroup generated by  $r$ ,  $K := \langle r \rangle$ , is order  $n$  hence,  $K \triangleleft G$  since  $[G : K] = 2$  is the smallest prime dividing the order of  $G$ . Let  $H := \langle s \rangle$ . This is a subgroup of order 2. Note that  $H \cap K = \{e\}$  and  $HK < G$  since  $K$  is normal in  $G$ . Moreover,  $|HK| = |H||K|/|H \cap K| = 2n = |G|$  so  $HK = G$  so we have  $G = H \rtimes K$ . Moreover, since  $H$  and  $K$  are cyclic of order 2 and  $n$ , respectively, we have  $H \cong Z_2$  and  $K \cong Z_n$  so  $G \cong Z_2 \rtimes Z_n$ . ■

**Problem 3.2.** Show that there is no simple group of order  $306 = 2 \cdot 3^2 \cdot 17$ .

*Proof.* Suppose  $G$  is a finite group of order  $306 = 2 \cdot 3^2 \cdot 17$ . We will show that one of  $n_2$ ,  $n_3$ , or  $n_{17}$  equals 1.

By Sylow's theorem,  $n_p \equiv 1 \pmod{p}$  and  $n_p \mid m$  where  $|G| = p^\alpha m$ . Thus, we have:

- $n_2 = 1, 3, 3^2, 17, 3 \cdot 17$ , or  $3^2 \cdot 17$ ;
- $n_3 = 1, 34$ ;
- $n_{17} = 1, 18$ .

Seeking a contradiction, suppose that none of  $n_2$ ,  $n_3$ , or  $n_{17}$  equal 1. Then, at least,  $n_2 = 3$ ,  $n_3 = 34$ , and  $n_{17} = 18$ . This means that there are  $1 + 3 + 16 \cdot 18 = 302$  elements of order 1, 2, and 17. But there are at least 8 elements of order 3 in the remaining Sylow 3-subgroups, pushing this total to 310 which is absurd. Thus, at least one of  $n_2$ ,  $n_3$ , or  $n_{17}$  equals 1. ■



**Problem 3.3.** Suppose  $R$  is a ring with identity, and  $I$ ,  $J$ , and  $K$  are (two-sided) ideals of  $R$  with  $K \subset I \cup J$ . Prove that either  $K \subset I$  or  $K \subset J$ .

*Proof.* We shall proceed by contradiction. Suppose that  $K \not\subset I$  and  $K \not\subset J$ . Then there exists elements  $a, b \in K$  such that  $a \notin I$  and  $b \notin J$ . Now, consider the element  $a - b \in K$ . Since  $K \subset I \cup J$ , then  $a - b \in I$  or  $a - b \in J$ . Without loss of generality, suppose that  $a - b \in I$ . Then  $(a - b) + b = a \in I$  since  $I$  is additively closed. This is a contradiction. Thus,  $K \subset I$  or  $K \subset J$ . ■

**Problem 3.4.** Let  $R$  and  $S$  be rings and suppose that  $\varphi: R \rightarrow S$  is a ring homomorphism. Let  $I$  be an ideal of  $R$  and  $J$  ideal of  $S$ .

- (a) Show that  $\varphi^{-1}(J) := \{r \in R \mid \varphi(r) \in J\}$  is an ideal in  $R$ .
- (b) Show that if  $\varphi$  is surjective, then  $\varphi(I) := \{\varphi(r) \mid r \in I\}$  is an ideal in  $S$ .
- (c) Given an example where  $\varphi$  is not surjective and  $\varphi(I)$  is not an ideal in  $S$ .

*Proof.* (a) We need to show two things: Let  $r \in R$  and  $a \in \varphi^{-1}(J)$  then  $\varphi(ra) = \varphi(r)\varphi(a)$ , but  $\varphi(a) \in J$  so  $\varphi(r)\varphi(a) \in J$ . Thus,  $ra \in \varphi^{-1}(J)$ . Lastly, we show  $\varphi^{-1}(J)$  is an additive subgroup, namely, for  $a_1, a_2 \in \varphi^{-1}(J)$ , we have  $\varphi(a_1), \varphi(a_2) \in J$  so  $\varphi(a_1) + \varphi(a_2) = \varphi(a_1 + a_2) \in J$ . Thus,  $a_1 + a_2 \in \varphi^{-1}(J)$ . Thus,  $\varphi^{-1}(J)$  is an ideal in  $R$ .

(b) Suppose  $\varphi$  is surjective. Then, for every element  $s \in S$ , there exist an element  $r \in R$  such that  $s = \varphi(r)$ . Now, let  $a \in \varphi(I)$  and  $s \in S$ . Then  $\varphi(b) = a$  for some  $b \in I$  and  $\varphi(r) = s$  for some  $r \in R$ . Thus,  $\varphi(rb) = sa \in \varphi(I)$ . Lastly, if  $a_1, a_2 \in \varphi(I)$  then  $\varphi(b_1) = a_1$  and  $\varphi(b_2) = a_2$  for  $b_1, b_2 \in I$  so  $b_1 + b_2 \in I$  implies that  $\varphi(b_1 + b_2) = \varphi(b_1) + \varphi(b_2) \in \varphi(I)$ . Thus,  $\varphi(I)$  is an ideal of  $S$ .

(c) Consider the map  $\varphi: Z_4 \rightarrow Z_2 \times Z_2$  given by the rule  $\varphi(s) = (s, s)$ . This map is a homomorphism since for any  $s_1, s_2 \in Z_4$ , we have

$$\begin{aligned} \varphi(s_1 + s_2) &= (s_1 + s_2, s_1 + s_2) & \varphi(s_1 s_2) &= (s_1 s_2, s_1 s_2) \\ &= (s_1, s_1) + (s_2, s_2) & &= (s_1, s_1)(s_2, s_2) \\ &= \varphi(s_1) + \varphi(s_2) & &= \varphi(s_1)\varphi(s_2). \end{aligned}$$

But note that  $\varphi$  is not surjective since  $\varphi(Z_4) = \{(0, 0), (1, 1)\}$ . Moreover, the latter is not an ideal since for  $(1, 0) \in Z_2 \times Z_2$ ,  $(1, 0)(1, 1) = (1, 0) \notin \varphi(Z_4)$ . ■

**Problem 3.5.** (a) Let  $R$  be a commutative ring with identity  $1 \neq 0$ . Suppose that, for every  $r \in R$ , there is some  $n = n_r \geq 2$  so that  $r^n = r$ . Prove that every prime ideal of  $R$  is maximal.

- (b) Suppose  $R$  is a unique factorization domain,  $p \in R$  is irreducible, and  $\mathfrak{p}$  is a prime ideal with  $0 \subsetneq \mathfrak{p} \subset (p)$ . Show  $\mathfrak{p} = (p)$ . (*Hint:* Prove that  $\mathfrak{p}$  can be generated by irreducible elements.)

*Proof.* (a) Let  $\mathfrak{p} \in \text{Spec}(R)$ . Then  $R/\mathfrak{p}$  is an integral domain. Now, let  $r \in R \setminus \mathfrak{p}$  and  $\pi: R \rightarrow R/\mathfrak{p}$  be the canonical projection. Put  $\bar{r} := \pi(r)$ . Then since  $r^n = r$  for some  $n \geq 2$  we have

$$\pi(r^n) = (\bar{r})^n(\bar{r})^n = \bar{r} = \pi(r).$$

Thus,  $\bar{r}(\bar{r}^{n-1} - \bar{1}) = 0$  implies  $\bar{r} = \bar{0}$  or  $\bar{r}^{n-1} = \bar{1}$ . But  $r \notin \mathfrak{p}$  so  $\bar{r} \neq \bar{0}$ . Thus,  $\bar{r}^{n-1} = \bar{1}$  and we see that  $\bar{r}$  is a unit. Thus,  $R/\mathfrak{p}$  is a field which implies that  $\mathfrak{p}$  is maximal.

(b) First note that if  $p$  is irreducible in  $R$  then it is prime. We will show that  $\mathfrak{p}$  contains a principal prime ideal. Let  $a \in \mathfrak{p}$ . Then, since  $R$  is a UFD, we may write  $a = p_1 \cdots p_n$  for  $p_1, \dots, p_n$  irreducible in  $R$ . Hence, each  $p_i$  is prime in  $R$  and  $(p_i)$  is a prime ideal. Moreover, since  $a = p_1 \cdots p_n \in \mathfrak{p}$ ,  $p_k \in \mathfrak{p}$  for some  $1 \leq k \leq n$ . Thus,  $(p_k) \subset \mathfrak{p}$ . Hence, we have  $(p_k) \subset \mathfrak{p} \subset (p)$ . But this implies  $p_k = rp$  for some  $r \in R$ . Since  $p_k$  is irreducible,  $r$  must be a unit so  $(p_k) = (p)$  which implies that  $\mathfrak{p} = (p)$ . ■

## 4 MA 553: Final, Fall 2015

**Problem 4.1.** Let  $G$  be a finite non-Abelian group, and let  $Z(G)$  be the center of  $G$ . Prove that  $|Z(G)| \leq |G|/4$ .

*Proof.* Seeking a contradiction, suppose  $4 > [G : Z(G)]$ . Since  $Z(G) \triangleleft G$ , we have  $G/Z(G)$  is a group of order 1, 2, or 3. Thus,  $G/Z(G) \cong Z_1, Z_2$ , or  $Z_3$  all of which are cyclic. This implies that  $G$  is Abelian. This is a contradiction. ■

**Problem 4.2.** Let

$$G = \text{SL}_2(\mathbf{Z}/(5)) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbf{Z}/(5), \text{ and } ad - bc \equiv 1 \pmod{5} \right\}.$$

- (a) Show  $|G| = 120$ .
- (b) Show  $N := \{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mid b \in \mathbf{Z}/(5) \}$  is a Sylow 5-subgroup of  $G$ .
- (c) Find the number of Sylow 5-subgroups of  $G$ .

*Proof.* (a) We'll do a case by case analysis. First, suppose that  $a = 0$ . Then  $bc \equiv 1 \pmod{5}$  and we have elements of the form

$$\begin{bmatrix} 0 & b \\ c & d \end{bmatrix}.$$

Hence, we have 5 choices for  $c$  and 4 choices for  $b$  ( $d$  is determined by the equivalence  $bd \equiv 1 \pmod{5}$ ). So there are  $5 \cdot 4 = 20$  elements with  $a = 0$ .

Now, suppose  $a \neq 0$ . Then  $d \equiv (1 + bc)a^{-1} \pmod{5}$ . Hence there are 4 choices for  $a$  and 5 choices for both  $b$  and  $c$ . Hence, there are  $4 \cdot 5 \cdot 5 = 100$  elements of the form

$$\begin{bmatrix} a & b \\ c & (1 + bc)a^{-1} \end{bmatrix}.$$

with  $a \neq 0$ . Tallying up this total, we have  $20 + 100 = 120$ , as was to be shown.

(b) First, note that  $|G| = 120 = 2^3 \cdot 3 \cdot 5$  and since 5 is the smallest power of 5 dividing  $|G|$ , it suffices to show that  $|N| = 5$ . Now, note that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^b = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$$

hence,  $N$  is generated by  $g := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ . Moreover,

$$g^5 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^5 = \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence,  $|N| = |g| = 5$  so  $N \in \text{Syl}_5(G)$ .

(c) By Sylow's theorem, there are  $n_5 = 1$  or  $6$ . We will show that  $N$  is not normal in  $\mathrm{SL}_2(\mathbf{Z}/(5))$  so that  $n_5 \neq 1$ . Let  $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbf{Z}/(5))$ . Then, for any matrix in  $N$  we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 1-ac & a^2 \\ -bc & 1+ba \end{bmatrix}$$

is in  $N$  if and only if  $ac = ba = 0$  and  $-bc = 0$ . But  $ad \equiv 1 + bc \pmod{5}$ . Implies  $bc = 0$  so  $b = 0$  or  $c = 0$  so either  $b = 0$  and  $c = 0$  or  $c = 0$ . The former implies that  $ad = 1 \equiv \pmod{5}$  so  $a = d = 1$ . This would imply that  $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ . Thus,  $N \not\triangleleft \mathrm{SL}_2(\mathbf{Z}/(5))$  so  $n_5 = 6$ . ■

**Problem 4.3.** Suppose  $R$  is a UFD and  $F$  is the quotient field of  $R$ . Let  $f(X) \in R[X]$  and suppose  $f(X)$  factors as a product of lower degree polynomials in  $F[X]$ . Show  $f(X)$  factors as a product of lower degree polynomials in  $R[X]$ .

*Proof.* This is an important result called *Gauß's lemma* and is proven in Dummit and Foote more or less as follows:

Suppose  $f(X)$  factors as  $f(X) = g(X)h(X)$  for polynomials  $g, h \in F[X]$  with  $\deg(g), \deg(h) < \deg(f)$ . Then each coefficient  $\{a_i\}, \{b_i\}$  of  $g$  and  $h$ , respectively, is in  $F$ . Thus, clearing denominators, we have  $df(X) = g'(X)h'(X)$  for  $g'(X), h'(X) \in R[X]$ . If  $d$  is a unit in  $R$  we are done since  $f(X) = d^{-1}df(X) = d^{-1}g'(X)h'(X)$ .

Suppose  $d$  is not a unit. Then, since  $R$  is a UFD, we may write  $d$  as the product  $d = d_1 \cdots d_n$  of irreducible elements  $d_i \in R$ . Since  $d_1$  is irreducible and  $R$  is a UFD, then  $d_1$  is prime so the ideal generated by  $d_1$  is prime. Thus,  $(R/(d_1))[X]$  is a domain and

$$\bar{0} = \overline{df(X)} = \bar{d} \cdot \overline{f(X)} = \overline{g'(X)h'(X)} = \overline{g'(X)} \cdot \overline{h'(X)}.$$

Thus, either  $\overline{g'(X)} = \bar{0}$  or  $\overline{h'(X)} = \bar{0}$  since  $(R/(d_1))[X]$  is a domain. Without loss of generality, suppose  $\overline{g'(X)} = \bar{0}$ . Then,  $(1/d_1)g'(X) \in R[X]$  so, dividing over  $F$ , we have  $(d_2 \cdots d_n)f(X) = ((1/d_1)g'(X))h'(X)$  in  $R[X]$ . Proceeding recursively in this fashion until, we may arrive at  $f(X) = G(X)H(X)$  where  $G(X), H(X) \in R[X]$ . Since we reduced by elements in the subring  $R$ ,  $\deg(G) = \deg(g)$  and  $\deg(H) = \deg(h)$  so that  $f(X)$  factors as a product of polynomials of lower degree in  $R[X]$ , as desired. ■

**Problem 4.4.** Let  $R$  be a commutative ring. Recall an element  $a \in R$  is *nilpotent* if  $r^n = 0$  for some  $n \geq 1$ . Let  $I = \{a \in R \mid a \text{ is nilpotent}\}$ .

(a) Show  $I$  is an ideal. (*Hint:* To show  $I$  is an additive subgroup, show if  $x, y \in I$  there is an  $N > 0$  so that  $(x - y)^N = 0$  using the binomial expansion of  $(x - y)^N$ .)

(b) Show  $I$  is contained in any prime ideal of  $R$ .

*Proof.* (a) In fact, one can show that  $I = \mathrm{Nil}(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$ , i.e.,  $I$  is the intersection of all prime ideals in  $R$  hence, an ideal.

First, we show that  $R$  is multiplicatively closed. Let  $r \in R$  and  $a \in I$ . Then  $(ar)^n = a^n r^n$  since  $R$  is commutative. But  $r^n = 0$ , so  $(ar)^n = a^n \cdot 0 = 0$ . Thus  $ar \in I$ .

Next, we show that it is additively closed. Suppose  $a, b \in I$ . Then  $a^m = 0$  and  $b^n = 0$  for some positive integer  $m$  and  $n$ . Suppose, without loss of generality, that  $n \geq m$ . Let  $N = n + m$ . Then

$$\begin{aligned}(a + b)^N &= (a + b)^{n+m} \\ &= \sum_{i=1}^{n+m} \binom{n+m}{i} a^i b^{n+m-i}.\end{aligned}$$

Now, note that if  $k \geq n$ ,  $x^k = 0$  so  $\binom{n+m}{k} a^k b^{n+m-k} = 0$ . On the other hand, if  $k < n$ ,  $n+m-k > m$  so  $b^{n+m-k} = 0$  so  $\binom{n+m}{k} a^k b^{n+m-k} = 0$ . In either case, we see that  $\binom{n+m}{k} a^k b^{n+m-k} = 0$  so  $(a+b)^N = 0$ . Thus,  $a + b \in I$ . Hence,  $I$  is an ideal.

(b) Let  $\mathfrak{p}$  be a maximal ideal of  $R$ . Now, since  $\mathfrak{p}$  is an ideal of  $R$ ,  $0 \in \mathfrak{p}$ . Moreover, for any  $a \in I$ ,  $a^n = 0$  for some positive integer  $n$ . Thus,  $a^n = 0 \in \mathfrak{p}$ . But  $\mathfrak{p}$  is a prime ideal. Thus,  $a \in \mathfrak{p}$  or  $a^{n-1} \in \mathfrak{p}$ . If the former, we are done. In the later,  $a^{n-1} \in \mathfrak{p}$  so  $a \in \mathfrak{p}$  or  $a^{n-2} \in \mathfrak{p}$ . Proceeding recursively in this manner, we have  $a \in \mathfrak{p}$ . Thus,  $I \subset \mathfrak{p}$ , as desired. ■

**Problem 4.5.** Let  $\alpha \in \mathbf{C}$  be algebraic over  $\mathbf{Q}$ , and let  $f(X) \in \mathbf{Q}[x]$  be its minimal polynomial. Let  $\sqrt{\alpha}$  be a square root of  $\alpha$ , and let  $g(X) \in \mathbf{Q}[X]$  be its minimal polynomial.

(a) Show  $\deg f(X)$  divides  $\deg g(X)$ .

(b) Show  $\sqrt{\alpha} \in \mathbf{Q}(\alpha)$  if and only if  $f(X^2)$  is reducible in  $\mathbf{Q}[X]$ .

*Proof.* (a) This follows directly from the tower of fields theorem. Let  $\mathbf{Q}(f)$  denote the splitting field of  $f$ . Then,  $\alpha \in \mathbf{Q}(f)$  so that  $\mathbf{Q}(g) \supset \mathbf{Q}(f)$ . Thus, we have

$$[\mathbf{Q}(g) : \mathbf{Q}] = [\mathbf{Q}(g) : \mathbf{Q}(f)][\mathbf{Q}(f) : \mathbf{Q}] = k \cdot \deg(f)$$

Thus,  $\deg(f) \mid \deg(g)$ .

(b)  $\implies$  Suppose that  $\sqrt{\alpha} \in \mathbf{Q}(\alpha)$ . Then  $f(\sqrt{\alpha}^2) = f(\alpha) = 0$  hence,  $f(X^2)$  has a root in  $\mathbf{Q}$  hence, is reducible.

$\Leftarrow$  Conversely, suppose that  $f(X^2)$  is reducible. Then, we may write  $f(X^2) = \prod_{i=1}^k f_i(X)$  where  $f_i \in \mathbf{Q}[X]$  is irreducible. Now, each of these factors,  $f_i$ , have degree less than  $2n$  where  $n := \deg(f(X^2))$ . Suppose

$$f_i(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_0$$

for  $a_{k-1}, \dots, a_0 \in \mathbf{Q}$ . Then

$$f_i(\sqrt{\alpha}) = \alpha^{k/2} + a_{k-1}\alpha^{(k-1)/2} + \cdots + a_0.$$

■

**Problem 4.6.** Let  $f(X) = X^6 + 3 \in \mathbf{Q}[X]$ .

(a) Let  $\alpha$  be a root of  $f(X)$ . Prove  $(\alpha^3 + 1)/2$  is a primitive 6th root of unity.

(b) Determine the Galois group of  $f(X)$  over  $\mathbf{Q}$ .

*Proof.* (a) To show that  $(\alpha^3 + 1)/2$  is a 6th root of unity, suffices to show that  $\Phi_6((\alpha^3 + 1)/2) = 0$  where  $\Phi_6$  is the 6th cyclotomic polynomial. Recall that we may derive the  $n$ th cyclotomic polynomial via the formula

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

so that

$$X^6 - 1 = \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_6(X) = (X - 1)(X + 1)(X^2 + X + 1)$$

and we have

$$\begin{aligned} \Phi_6(X) &= \frac{X^6 - 1}{(X - 1)(X + 1)(X^2 + X + 1)} \\ &= X^2 - X + 1. \end{aligned}$$

Thus,

$$\begin{aligned} \Phi_6((\alpha^3 + 1)/2) &= \frac{1}{4}(\alpha^3 + 1)^2 - \frac{1}{2}(\alpha^3 + 1) + 1 \\ &= \frac{1}{4}\alpha^6 + \frac{1}{2}\alpha^3 + \frac{1}{4} - \frac{1}{2}\alpha^3 - \frac{1}{2} + 1 \\ &= \frac{1}{4}\alpha^6 + \frac{3}{4} \\ &= \frac{1}{4}(\alpha^6 + 3) \\ &= 0. \end{aligned}$$

Thus,  $(\alpha^3 + 1)/2$  is 6th root of unity.

To show that  $(\alpha^3 + 1)/2$  is in fact a primitive root of unity, we need to show that 6 is the smallest integer such that  $((\alpha^3 + 1)/2)^6 = 1$ . And that is too much work.

(b) Put  $\zeta_6 := (\alpha^3 + 1)/2$ . The roots of the polynomial are  $\sqrt[6]{3}, \zeta_6 \sqrt[6]{3}, \dots, \zeta_6^5 \sqrt[6]{3}$ . Hence, the splitting field of  $f$  contains  $\sqrt[6]{3}$  and a primitive sixth root of unity  $(\alpha^3 + 1)/2$ . Since  $\deg(\Phi_6) = 2$ , and  $\sqrt{3} \in \mathbf{Q}(\Phi_6)$ , the minimal polynomial of  $\sqrt[6]{3}$  over  $\mathbf{Q}(\Phi_6)$  is  $X^3 - \sqrt{3}$ . Hence, the degree of the extension

$$[\mathbf{Q}(f) : \mathbf{Q}] = [\mathbf{Q}(f) : \mathbf{Q}(\Phi_6)][\mathbf{Q}(\Phi_6) : \mathbf{Q}] = 3 \cdot 2 = 6.$$

Thus, the Galois group of  $\mathbf{Q}(f)/\mathbf{Q}$  is order 6.

Moreover, the Galois group acts transitively on the roots of  $f$  so there are automorphism of the splitting field fixing the subfields  $\mathbf{Q}(\Phi_6)$  and  $\mathbf{Q}$ . These are the automorphism

$$\sigma: \alpha \mapsto -\alpha \quad \text{and} \quad \tau: \alpha \mapsto \zeta_6 \alpha.$$

Note that  $\sigma$  has order 2 and  $\tau$  has order 3 so that  $\text{Gal}(\mathbf{Q}(f)/\mathbf{Q}) \cong D_6$ . ■

**Problem 4.7.** Let  $R := (\mathbf{Z}/(3))[X]$ . Consider the ideals  $I_1 := (X^2 + 1)$ , and  $I_2 := (X^2 + X + 2)$ . For  $i = 1, 2$  we set  $F_i = R/I_i$ .

(a) Show  $F_1$  and  $F_2$  are fields.

(b) Are  $F_1$  and  $F_2$  isomorphic? If not, why not, and if so give an isomorphism from  $F_1$  to  $F_2$ .

*Proof.* (a) Recall by some theorem in chapter 13 that  $F[X]/(f)$  is a field if and only if  $f$  is irreducible. Therefore, it suffices to show that  $X^2 + 1$  and  $X^2 + X + 2$  are irreducible over  $\mathbf{Z}/(3)$ . To that end, since the degree of these polynomials is two, it suffices to show that they have no roots over  $\mathbf{Z}/(3)$ .

In the case of  $X^2 + 1$ , we have  $0^2 + 1 \neq 0$ ,  $1^2 + 1 = 1 \neq 0$ , and  $2^2 + 1 = 4 + 1 = 1 + 1 = 2 \neq 0$ . Thus,  $X^2 + 1$  is irreducible.

In the case of  $X^2 + X + 2$ , we have  $0^2 + 0 + 2 = 2 \neq 0$ ,  $1 + 1 + 2 = 1 \neq 0$ , and  $4 + 2 + 2 = 8 = 2 \neq 0$ .

Thus,  $F_1$  and  $F_2$  are fields.

(b) By the classification theorem for finite fields, both  $F_1$  and  $F_2$  are an extension over  $\mathbf{F}_3 = \mathbf{Z}/(3)$  of degree 2 hence, both are isomorphic to  $\mathbf{F}_{3^2}$ . In particular, they are isomorphic to each other. Let  $\alpha$  be a root of  $X^2 + 1$  and  $\beta$  be a root of  $X^2 + X + 2$ . Then the map  $\alpha \mapsto \beta$  which fixes  $\mathbf{F}_3$  is an isomorphism. It suffices to show that this is an injective homomorphism. First, this is a homomorphism since for any  $x, y \in F_1$ , if  $x, y \in \mathbf{F}_3$ ,  $\varphi(x + y) = x + y = \varphi(x) + \varphi(y)$ . If one of  $x$  or  $y$  not in  $\mathbf{F}_3$ , suppose  $x$ , then  $x = \alpha^k + x'$  for  $x' \in \mathbf{F}_3$  so

$$\varphi(\alpha^k + x' + y) = \beta^k + x' + y = \varphi(\alpha^k + x') + \varphi(y)$$

etc., thus this is an isomorphism.

To see that this map is injective, note that  $\ker \varphi = \{0\}$ . Thus,  $\varphi$  is an isomorphism. ■

**Problem 4.8.** Suppose  $F$  is a field,  $K = F(\alpha)$  is a Galois extension, with cyclic Galois group generated by  $\sigma(\alpha) := \alpha + 1$ . Show that  $\text{ch}(K) = p \neq 0$ , and  $\alpha^p - \alpha \in F$ .

*Proof.* Suppose that the Galois group of  $K$  is cyclic of order  $n > 1$ . Then,

$$\sigma^n(\alpha) = \alpha = \alpha + n.$$

Thus,  $0 = \alpha - \alpha = n \in F$  so  $\text{ch}(F)$  is prime since the order of a field is always prime.

Lastly, note that  $\alpha^p - \alpha = \alpha(\alpha^{p-1} - 1)$  since  $\alpha$  is the root of the polynomial  $x^p - x$ . ■

## 5 Qualifying Exam, January 2000

**Problem 5.1.** Find all groups of order  $7 \cdot 11^3$  which have a cyclic subgroup of order  $11^3$ .

*Proof.* Suppose  $G$  is a group of order  $7 \cdot 11^3$ . By Sylow's theorem,  $n_{11} \equiv 1 \pmod{11}$  and  $n_{11} \mid 7$ , thus  $n_{11} = 1$  and we see that  $G$  must have a unique, therefore normal, Sylow 11-subgroup  $P$  of order  $11^3$ . Also by Sylow's theorem, we see that  $n_7 = 1$  or  $11^3 = 1331$  (what an outrageous number!!!).

If  $n_7 = 1$ , again the Sylow 7-subgroup  $Q$  is unique hence, normal in  $G$  and we must have  $PQ = QP = G$  (since  $P \cap Q = \{e\}$  and  $|PQ| = |P||Q|/|P \cap Q| = 11^3 \cdot 7/1 = |G|$ ). Thus,  $G \cong Z_7 \times Z_{11^3}$ .

Otherwise,  $n_7 = 11^3$ . Thus, there are  $6 \cdot 11^3 + 1$  elements of order 7 plus the identity plus  $11^3 - 1$  elements in  $P$ . Thus, there are a total of  $6 \cdot 11^3 + 1 + 11^3 - 1 = 7 \cdot 11^3$  elements of order 7, in  $Q$ , plus the identity. No contradiction here. But we still have  $P \cap Q = \{e\}$  for any  $Q \in \text{Syl}_7(G)$ . Therefore, I suspect that the only other (nonabelian) group that has a cyclic subgroup of order  $11^3$  must be the semidirect product  $Z_7 \rtimes Z_{11^3}$ .

This is what 성준 had to say about the matter:

Suppose  $Q$  is a group of order 7 and  $P$  is a cyclic group of order  $11^3$ . If  $\varphi: Q \rightarrow \text{Aut}(P)$  is a homomorphism, then  $\varphi(Q) \mid 7$  so  $\varphi(Q) = 1$  or  $\varphi(Q) = 7$ . But if  $\psi \in \text{Aut}(P)$ , then  $\psi$  must send a generator  $g$  of  $P$  to another generator of  $P$ . Since there are only  $\varphi(11^3) = 11^3 - 11^2 = 1331 - 121 = 1220$  which is not divisible by 7. Thus  $\varphi$  can only be the trivial homomorphism and  $Q \rtimes_{\varphi} P \cong Z_7 \times Z_{11^3}$ . ■

**Problem 5.2.** Let  $R$  be a ring with identity 1 and consider the following two conditions:

- (i) If  $a, b \in R$  and  $ab = 0$ , then  $ba = 0$ ;
- (ii) If  $a, b \in R$  and  $ab = 1$ , then  $ba = 1$ ;
- (a) Show that (i) implies (ii).
- (b) Show by example that (ii) does not imply (i).

*Proof.* (i)  $\implies$  (ii) Let  $a, b \in R$  such that  $ab = 1$ . Consider the product of elements of  $R$

$$b(ab - 1)a = baba - ba = 0.$$

Then, by (i), we have  $ba(ba - 1) = 0$  so

$$a(ba - 1)b = (ba - 1)ab = ba - 1 = 0$$

so  $ba = 1$ .

(ii)  $\not\implies$  (i) Consider the ring of  $2 \times 2$  matrices over  $\mathbf{R}$ ,  $M(2, \mathbf{R})$ . Then, for any matrices  $A, B \in M(2, \mathbf{R})$  such that  $AB = 1$  we have  $BA = 1$ . However,

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

but

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \quad \blacksquare$$



**Problem 5.3.** Let  $F$  be a field. Suppose that  $E/F$  is a Galois extension, and that  $L/F$  is an algebraic extension with  $L \cap E = F$ . Let  $EL$  be the composite field, i.e., the subfield of an algebraic closer  $\bar{F}$  of  $F$  generated by  $E$  and  $L$ .

- (a) Show  $EL/L$  is a Galois extension.
- (b) Show that there is an injective homomorphism

$$\varphi: \text{Gal}(EL/L) \hookrightarrow \text{Gal}(E/F).$$

Find the fixed field of the image of  $\varphi$ .

- (c) Show that  $[EL : L] = [E : F]$ .
- (d) Give an example to show that the conclusion of (c) is false if we do not assume that  $E/F$  is Galois.

*Proof.* This is standard and is found in Dummit & Foote<sup>5</sup>

(a) Since  $E/F$  is Galois,  $E$  is the splitting field of some separable polynomial  $f \in F[X]$ . Hence,  $EL/L$  is the splitting field of  $f$  viewed as a polynomial in  $L[X]$  (since  $F \subset L$ , we can just look at the embedding  $F[X] \hookrightarrow L[X]$ ). Thus,  $EL/L$  is Galois.

(b) Define the map  $\varphi: \text{Gal}(EL/L) \rightarrow \text{Gal}(E/F)$  to be  $\varphi(\sigma) := \sigma|_E$ , i.e.,  $\varphi$  is the restriction of  $\sigma \in \text{Gal}(EL/L)$  to  $E$ . Since  $E/F$  is Galois, every embedding of  $E$  fixing  $F$  is an automorphism of  $E$  hence,  $\varphi$  is well defined and because of the properties of restriction, trivially  $\varphi$  is a homomorphism, i.e., for any  $\sigma_1, \sigma_2 \in \text{Gal}(EL/L)$  we have

$$\varphi(\sigma_1 \circ \sigma_2) = \sigma_1 \circ \sigma_2|_E = (\sigma_1|_E) \circ (\sigma_2|_E) = \varphi(\sigma_1) \circ \varphi(\sigma_2).$$

Now, let us show  $\varphi$  is injective. To that end, we will show that  $\ker \varphi = \{\text{id}_{EL}\}$ . Let  $\sigma \in \ker \varphi$ . Then  $\sigma|_E = \text{id}_E$ . But  $\sigma|_L = \text{id}_L$ . Thus,  $\sigma = \text{id}_{EL}$ . Hence,  $\varphi$  is injective.

(c)

(d) Consider the extensions  $E := \mathbf{Q}(\sqrt[3]{2})$  and  $L := \mathbf{Q}(\omega\sqrt[3]{2})$  where  $\omega$  is a primitive 3rd root of unity, i.e., satisfies  $\omega^2 + \omega + 1 = 0$ . Then, the minimal polynomial for both extensions over  $\mathbf{Q}$  is  $X^3 - 2$ . In particular,  $[E : F] = 3$ . However, the composite

$$EL = \mathbf{Q}(\omega, \sqrt[3]{2})$$

is a degree 2 extension over  $L$  (since the minimal polynomial for  $\omega$  over  $L$  is  $X^2 + X + 1$ ). Thus,  $[EL : L] = 2 \neq 3 = [E : F]$  since neither the extension  $E$  or  $L$  is Galois. ■

**Problem 5.4.** Let  $G$  be a finite group. Let  $p$  be a prime and suppose that  $|G| = p^k m$ , with  $k \geq 1$  and  $p \nmid m$ . Let  $X$  be the collection of all subsets of  $G$  of order  $p^k$ . Then  $G$  acts on  $X$  by left multiplication, i.e.,  $g \cdot A = \{ga \mid a \in A\}$ . For  $A \in X$  denote by  $H_A$  the stabilizer in  $G$  of  $A$ . Show that  $|H_A| \mid p^k$ .

---

<sup>5</sup>I'm not saying that I remembered how to do it, but I can start the proof at the very least.

*Proof.* ■

**Problem 5.5.** Let  $R = \mathbf{Z} + X\mathbf{Q}[X] \subset \mathbf{Q}[X]$  be the ring consisting of polynomials with rational coefficients whose constant term is an integer.

- (a) Prove that  $R$  is an integral domain, with units 1 and  $-1$ .
- (b) Show that  $X$  is not an irreducible element of  $R$ .
- (c) Let  $(X) := RX$  be the ideal of  $R$  generated by  $X$ . Describe  $R/(X)$  and show that  $R/(X)$  is not an integral domain. What can you conclude about  $X$ ?

*Proof.* (a) Let  $f, g \in R$  such that  $fg = 0$ . Then

$$f(X)g(X) = (a_n/b_n)X^n + (a_{n-1}/b_{n-1})X^{n-1} + \cdots + a_0b_0 = 0$$

where the coefficients  $a_i/b_i$  for  $1 \leq i \leq n$  are sums of products of coefficients of  $f$  and  $g$ . Since the right handside of the equation above has degree 0, each of the coefficients  $a_i/b_i = 0$  and since  $\mathbf{Z}$  is a Euclidean domain,  $a_0b_0 = 0$  implies that either  $a_0 = 0$  or  $b_0 = 0$ . Hence, either  $f = 0$  or  $g = 0$  (that is, WLOG, supposing  $b_0 = 0$  then the next smallest coefficient of  $g$ , say  $b'_1 = 0$  for otherwise  $b'_1a_0X \neq 0$  is in the product). Thus,  $R$  is an integral domain.

(b) Consider the decomposition  $X = 2((1/2)X)$ . Thus,  $X$  is not irreducible.

(c) Consider the ideal generated by  $X$ , i.e., the set  $(X)$  of all polynomials in  $\mathbf{Q}$  of degree  $\geq 1$  such that the coefficient of the degree 1 part of the polynomial is in  $\mathbf{Z}$ , i.e., all  $f$  of the form  $(a_n/b_n)X^n + \cdots + a_1X$  where  $a_i/b_i \in \mathbf{Q}$  and  $a_1 \in \mathbf{Z}$ .

Now, consider the quotient  $R/(X)$ . Under this quotient, every polynomial is of degree at most 1 with the coefficient being a number between 0 and 1. Let  $\bar{f}, \bar{g} \in R/(X)$  where the  $X$  coefficient of  $\bar{f}$  is  $1/2$  and the constant coefficient of  $\bar{g}$  is 2. Then  $\bar{f} \neq \bar{0}$  and  $\bar{g} \neq \bar{0}$ , but  $\bar{f}\bar{g} = \bar{0}$ . ■

## 6 Qualifying Exam, January 2011

**Problem 6.1.** Let

$$G = \mathrm{SL}_2(\mathbf{Z}/(5)) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbf{Z}/(5), \text{ and } ad - bc \equiv 1 \pmod{5} \right\}.$$

- (a) Show  $|G| = 120$ .
- (b) Show

$$N := \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \mid b \in \mathbf{Z}/(5) \right\}$$

is a Sylow 5-subgroup of  $G$ .

- (c) Find the number of Sylow 5-subgroups of  $G$ .

*Proof.* ■

**Problem 6.2.** (a) Let  $G$  be a group,  $H$  a subgroup of  $G$  with  $[G : H] = 2$ . Suppose  $K$  is a subgroup of  $G$  of odd order. Show  $K \subset H$ .

- (b) Let  $G$  be a finite group and suppose there is a sequence of subgroups

$$G_0 := G \supset G_1 \supset G_2 \supset \cdots \supset G_n := H,$$

with  $[G_i : G_{i+1}] = 2$  for  $i \in \{1, \dots, n-1\}$ . Suppose  $H$  has odd order. Show  $H \triangleleft G$ .

- (c) Suppose  $|G| = 2^n m$ , with  $m$  odd. Suppose  $G$  has a normal subgroup  $H$  of order  $m$ . Show there is a sequence of subgroups  $G_0 := G \supset G_1 \supset \cdots \supset G_n := H$ , with  $[G_i : G_{i+1}] = 2$ , for all  $i$ .

*Proof.* ■

**Problem 6.3.** Let  $R$  be a commutative ring with identity  $1 \neq 0$ , and let  $I$  be an ideal of  $R$ . Define  $\mathrm{rad}(I)$  to be the intersection of all maximal ideals containing  $I$ , with the convention  $\mathrm{rad}(R) = R$ . Let  $\sqrt{I} := \{r \in R \mid r^n \in I \text{ for some } n > 0\}$ .

- (a) Prove  $\mathrm{rad}(I)$  is an ideal of  $R$  containing  $I$ .
- (b) Prove  $\sqrt{I} \subset \mathrm{rad}(I)$ .
- (c) Let  $F$  be a field, set  $R = F[X]$ , and let  $I = (f)$ , for some nonzero polynomial  $f(X) \in R$ . Describe  $\mathrm{rad}(I)$  in this instance.

*Proof.* ■

**Problem 6.4.** Let  $S$  be the subring of  $\mathbf{C}[X] \times \mathbf{C}[Y]$  consisting of pairs  $(f, g)$  with  $f(0) = g(0)$ .

- (a) Let  $\varphi: \mathbf{C}[X, Y] \rightarrow S$  be defined by  $\varphi(h) = (f, g)$ , where  $f(X) = h(x, 0)$ , and  $g(Y) = h(0, Y)$ . Prove  $\varphi$  is a surjective homomorphism.
- (b) Prove  $\mathbf{C}[X, Y]/(X, Y) \cong S$ .

- (c) Use (b) to describe the prime ideals of  $S$ . Be sure to justify your answer.

*Proof.* ■

**Problem 6.5.** Let  $p$  be a prime, let  $F = \mathbf{F}_p$  be the field of  $p$  elements and  $K = \mathbf{F}_{p^{10}}$  be the unique extension of  $F$  with  $p^{10}$  elements.

- (a) Find all subfields of  $K$ . Make sure to justify your answer.
- (b) Find a formula for the number of monic irreducible polynomials of degree 10 in  $F[X]$ . Justify your answer.

*Proof.* ■

**Problem 6.6.** Let  $f(X) = (X^2 - 3)(X^3 - 7) \in \mathbf{Q}[X]$ . Let  $K$  be the splitting field of  $f(X)$  over  $\mathbf{Q}$ .

- (a) Find the degree of  $K$  over  $\mathbf{Q}$ .
- (b) Classify the Galois group  $\text{Gal}(K/\mathbf{Q})$ .
- (c) Find all subfields  $E$  of  $K$  so that  $E/\mathbf{Q}$  is a quadratic extension.

*Proof.* ■