

# MA553 Past Qualifying Examinations

Carlos Salinas

December 31, 2015

# 1 Heinzer MA 553 Problems

Past Heinzer and Włodarczyk problems with proofs to the theorems, corollaries, and lemmas where I believe they would benefit me.

## 1.1 Groups

**Problem 1.1.** Does the symmetric group  $S_5$  have a subgroup of order 10? Justify your answer.

*Proof.* Yes. In fact, the following more general result holds.

**Lemma 1.** *The group  $D_{2n}$  acts transitively on the set  $A$  consisting of the vertices of a regular  $n$ -gon.*

*Proof of lemma.* Labeling these vertices  $0, \dots, n-1$  in a clockwise fashion, let  $r$  be the rotation of the  $n$ -polygon clockwise by  $2\pi/n$  radians and let  $s$  be the reflection of the regular  $n$ -gon by any line which passes through the center of the  $n$ -gon. This defines an action on  $A$  since for any vertex  $a \in A$  and we have  $r \cdot a \in A$  (that is,  $r \cdot a \mapsto a+1 \pmod n$ ) and  $s \cdot a \in A$  (that is,  $s \cdot a \mapsto n-1-a \pmod n$  or something like that) and  $r, s$  are generators for  $D_{2n}$ .

Next, it is easy to see that the action is transitive for  $r^k \cdot a \mapsto a+k \pmod n$  traverses (goes through every element of) the set  $A$ .

Lastly, we claim that this action is faithful. That is, we claim that the stabilizer of  $A$  consists of the identity subgroup. First  $\langle e \rangle \subset \text{Stab}_{D_{2n}}(A)$  (this is always true). Let  $g \in \text{Stab}_{D_{2n}}(A)$ . Then,  $g \cdot a = a \pmod n$  for all  $a \in A$ . This cannot be an element of the form  $sr^k$  or  $r^k$  since  $r^k$  does not fix any vertices. Thus, it can only be an element of the form  $s$  or  $e$ . But likewise  $s$  only fixes at most two vertices (vertices which intersect the line we are reflecting about). Thus,  $g = e$  and we see that the action is indeed faithful.

Thus, there is an induced homomorphism  $\varphi: D_{2n} \hookrightarrow S_n$  with kernel  $\langle e \rangle$  the identity element, i.e.,  $\varphi$  is a monomorphism so  $D_{2n} \cong \varphi(D_{2n}) < S_n$ . This shows that  $S_n$  always contains a subgroup of order  $2n$ , namely, a subgroup isomorphic to the dihedral group  $D_{2n}$ . ♣

From the lemma above, we see that  $D_{10} \hookrightarrow S_5$  so that  $S_5$  has a subgroup of order 10. ■

**Problem 1.2.** Let  $G$  be a subgroup generated by the 5-cycles in  $S_5$ . Find the order of  $N_{S_5}(G)$ .

*Proof.* This is a thinly disguised Sylow's theorem problem. The 5-cycles of  $S_5$  are order the order 5 permutations of  $S_5$  hence, are contained in some Sylow 5-subgroup  $P$ . Since  $G$  is the largest subgroup containing these 5-cycles and  $P$  is a maximal subgroup of  $S_5$  then  $G = P$ . First, let us factor the order of  $S_5$  into primes,  $|S_5| = 5! = 2^3 \cdot 3 \cdot 5$ . By Sylow's theorem, we have that the index of the normalizer of  $G$  in  $S_5$  is  $n_5 = [S_5 : N_{S_5}(G)]$  and  $n_5 \equiv 1 \pmod 5$  and  $n_5 \mid 2^3 \cdot 3$ . Running through all of the possibilities, we see that  $n_5 = 1$  or  $n_5 = 6$ .

If  $n_5 = 1$  then  $G$  is the unique Sylow 5-subgroup of  $G$  and hence, a normal subgroup of  $S_5$ . Moreover, since all of the 5-cycles are even permutations  $G < A_5$ . Since  $G$  is a characteristic subgroup of  $S_5$  this would imply that  $G \triangleleft A_5$ , but  $A_5$  is simple. Thus,  $n_5 = 6$ .

Hence,  $n_5 = 6$  and we have that

$$|N_{S_5}(G)| = \frac{5!}{6} = \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5}{6} = 4 \cdot 5 = 20. \quad \blacksquare$$

**Problem 1.3.** Show that for any element  $\sigma$  of order 2 in the alternating group  $A_n$ , there exists  $\tau \in S_n$  such that  $\tau^2 = \sigma$ .

*Proof.* Consider the unique representation of  $\sigma$  as a product of disjoint cycles

$$\sigma = (a_1^1 \cdots a_{k_1}^1) \cdots (a_1^\ell \cdots a_{k_\ell}^\ell).$$

since disjoint cycles commute,  $|\sigma|$  is the least common multiple of the order of each of the cycles in the representation above. Since every  $n$ -cycle has order  $n$  and  $|\sigma| = 2$ , it follows that  $\sigma$  must be a product of disjoint transposition, i.e., disjoint 2-cycles.

Now, since  $\sigma \in A_n$ ,  $\sigma$  is an even permutation so consists of an even number of disjoint transpositions, say

$$\sigma = (a_1 b_1) \cdots (a_{2k} b_{2k})$$

for some positive integer  $k$ . Now, note that the product of transpositions

$$(a b)(c d) = (a c b d)^2$$

so that

$$\sigma = (a_1 a_2 b_1 b_2)^2 \cdots (a_{2k-1} a_{2k} b_{2k-1} b_{2k})^2.$$

Since each of these cycles are disjoint from one another, they commute so that

$$\sigma = [(a_1 a_2 b_1 b_2) \cdots (a_{2k-1} a_{2k} b_{2k-1} b_{2k})]^2.$$

Define

$$\tau := (a_1 a_2 b_1 b_2) \cdots (a_{2k-1} a_{2k} b_{2k-1} b_{2k}).$$

Then  $\tau^2 = \sigma$  as desired. ■

**Problem 1.4.** Let  $G$  be a finite group,  $p > 0$  a prime number. Show that a subgroup  $H < G$  contains a Sylow  $p$ -subgroup of  $G$  if and only if  $p$  does not divide  $[G : H]$ .

*Proof.*  $\implies$  Put  $|G| = p^\alpha m$  for positive integer  $m$  and  $\alpha$ , where  $m$  is not divisible by  $p$ . Suppose that  $P \in \text{Syl}_p(G)$  is contained in  $H$ . Then, by Lagrange's theorem, we have  $p^\alpha \mid |H|$  and  $|H| \mid p^\alpha m |G|$ . Thus,  $|H| = p^\alpha n$  for some  $n \mid m$  not divisible by  $p$ . Hence,

$$[G : H] = \frac{p^\alpha m}{p^\alpha n} = \frac{m}{n}$$

which is not divisible by  $p$  since  $m$  and  $n$  are not divisible by  $p$ .

$\Leftarrow$  Conversely, suppose that  $p \nmid [G : H]$ . Then  $|H| = p^\alpha m / [G : H]$ . Since  $p \nmid [G : H]$ ,  $[G : H] \mid m$ . Put  $|H| = p^\alpha n$ . Let  $P \in \text{Syl}_p(H)$ . Then  $P$  is a  $p$ -subgroup of  $G$  hence, must be contained in a Sylow  $p$ -subgroup  $Q$  of  $G$ . Thus,  $P < Q$ , but  $|P| = p^\alpha = |Q|$ . Hence,  $P = Q$ , i.e.,  $H$  contains a Sylow  $p$ -subgroup of  $G$ . ■

**Problem 1.5.** Let  $G$  be a finite group,  $p > 0$  a prime number, and  $H$  a normal subgroup of  $G$ . Prove the following assertions.

- (a) Any Sylow  $p$ -subgroup of  $H$  is the intersection  $P \cap H$  of a Sylow  $p$ -subgroup of  $G$  and  $H$ .
- (b) Any Sylow  $p$ -subgroup of  $G/H$  is the quotient  $PH/H$ , where  $P$  is a Sylow  $p$ -subgroup of  $G$ .

*Proof.* (a) Let  $Q \in \text{Syl}_p(H)$ . Then  $Q$  is a  $p$ -subgroup of  $G$  hence, it is contained in a Sylow  $p$ -subgroup  $P$  of  $G$ . Hence,  $Q < P \cap H$ . Conversely, since  $P \cap H < P$ ,  $P \cap H$  is a  $p$ -subgroup of  $H$  hence, it is contained in a Sylow  $p$ -subgroup  $R$  of  $H$ . Thus,  $Q < P \cap H < R$ . But since  $|Q| = |R|$  and  $|Q| \mid |P \cap H|$  and  $|P \cap H| \mid |R|$ , we must have that  $Q = P \cap H$ .

(b) We will begin by showing that if  $P \in \text{Syl}_p(G)$  then  $PH/H \in \text{Syl}_p(G/H)$ . Put  $|G| = p^\alpha m$  and  $|H| = p^\beta n$  where  $p \nmid m$  and  $p \nmid n$  and  $n \mid m$  (where the last necessarily true by Lagrange's theorem, since  $H$  is a subgroup of  $G$ ). By the 2nd isomorphism theorem, since  $H \triangleleft G$ , we have  $PH/H \cong P/P \cap H$  so that

$$|PH/H| = |P/P \cap H| = |P|/|P \cap H| = p^{\alpha-\beta};$$

this is by part (a) since  $P \cap H$  is a Sylow  $p$ -subgroup of  $H$  hence,  $|P \cap H| = p^\beta$ . Since  $|G/H| = p^{\alpha-\beta}n/m$ , it follows that if  $Q \in \text{Syl}_p(G/H)$ , then  $|Q| = p^{\alpha-\beta}$ . Thus, by a simple order argument, it must be that  $PH/H \in \text{Syl}_p(G/H)$  ( $PH/H$  is a  $p$ -group hence, it is contained in a Sylow  $p$ -subgroup  $Q$  of  $G/H$ , but  $|PH/H| = |Q| = p^{\alpha-\beta}$  thus,  $PH/H = Q$ ).

Now, suppose that  $Q \in \text{Syl}_p(G/H)$ . By Sylow's theorem,  $Q$  is conjugate to a subgroup of the form  $RH/H$  where  $R \in \text{Syl}_p(G)$ . By the 4th isomorphism theorem, there exists a subgroup  $K > H$  such that  $K/H = Q$ . Moreover, since  $Q$  is conjugate to  $RH/H$ ,  $K$  is conjugate to  $RH$ . Thus,  $K = gRHg^{-1}$  for some  $g \in G$ . But since  $H \triangleleft G$  for any  $h \in H$ ,  $r \in R$ , we have  $grhg^{-1} = grg^{-1}(ghg^{-1}) = grg^{-1}h'$  for some  $h' \in H$ . Hence,  $K = gRg^{-1}H$ . But  $R \in \text{Syl}_p(G)$  thus,  $gRg^{-1} = P$  for some Sylow  $p$ -subgroup  $P$  of  $G$ . Thus,  $K/H = PH/H = Q$ . ■

**Problem 1.6.** Let  $H$  be a normal subgroup of a finite group  $G$ , and let  $N < H$  be a normal Sylow subgroup of  $H$ . Prove that  $N$  is a normal subgroup of  $G$ .

*Proof.* This is an important result, what it says is that normal Sylow  $p$ -subgroups are *characteristic subgroups*, i.e., if  $K$  is characteristic in  $H$  and  $K \triangleleft G$  then  $K \triangleleft H$  and  $K \triangleleft G$ .

Suppose  $N$  is a normal Sylow  $p$ -subgroup of  $H$ . Then  $N$  is the unique Sylow  $p$ -subgroup of  $H$ . Since  $H \triangleleft G$ , for every  $g \in G$ ,  $gHg^{-1} = H$ . In particular,  $gNg^{-1} < H$ . Since conjugation preserves order,  $|gNg^{-1}| = |N|$  hence,  $gNg^{-1} = N$ . Thus,  $N \triangleleft G$ . ■

**Problem 1.7.** Let  $G$  be a finite group,  $p > 0$  a prime number, and  $H$  a normal  $p$ -subgroup of  $G$ . Prove the following assertions.

(a)  $H$  is contained in each Sylow  $p$ -subgroup of  $G$ .

(b) If  $K$  is any normal  $p$ -subgroup of  $G$ , then  $HK$  is a normal  $p$ -subgroup of  $G$ .

*Proof.* (a) Suppose that  $H$  is a normal  $p$ -subgroup of  $G$ . Then  $H$  is contained in some Sylow  $p$ -subgroup  $P$  of  $H$ . Moreover, since  $gHg^{-1} = H < gPg^{-1}$  for all  $g \in G$ , and since every Sylow  $p$ -subgroup of  $G$  is conjugate,  $H < Q$  for every  $Q \in \text{Syl}_p(G)$ .

(b) First, note that since  $H$  and  $K$  are normal subgroups of  $G$ ,  $HK < G$ . Moreover,  $|HK| = |H||K|/|H \cap K|$ . If  $|H \cap K| \neq 1$  then  $H \cap K$  is not the identity subgroup hence, must contain at least one element of order  $p^\alpha$  for  $\alpha \geq 1$ . By Lagrange's theorem,  $p \mid |H \cap K|$  and  $|H \cap K| \mid |H|, |K|$  so  $|H \cap K| = p^\beta$  for some  $\beta \geq 1$ . It follows that  $|HK| = p^\gamma$  for some  $\gamma \geq 1$ , i.e.,  $HK$  is a  $p$ -subgroup of  $G$ .

Lastly, we need to show that  $HK \triangleleft G$ . Let  $g \in G$ . Then for any  $h \in H$ ,  $k \in K$  we have  $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) = h'k'$  where  $h' \in H$  and  $k' \in K$  since  $H \triangleleft G$  and  $K \triangleleft G$ . Thus,  $HK \triangleleft G$ . Note that the latter is true regardless of whether  $H$  and  $K$  are  $p$ -subgroups of  $G$ . ■

**Problem 1.8.** Prove that the order of the automorphism group  $(\mathbb{Z}/3\mathbb{Z})^4$  is  $80 \times 78 \times 72 \times 54$ .

*Proof.* This is from an early section of Dummit and Foote. The idea is that  $\text{Aut}(\mathbb{Z}/3\mathbb{Z})^4 \cong \text{GL}_4(\mathbb{Z}/3\mathbb{Z})$  which has  $(3^4 - 1)(3^4 - 3)(3^4 - 9)(3^4 - 27) = 80 \cdot 78 \cdot 72 \cdot 54$  elements. ■

**Problem 1.9.** Prove, for fixed  $n$ , that the following conditions are equivalent:

- (a) Every abelian group of order  $n$  is cyclic.
- (b)  $n$  is square free (i.e., not divisible by any square integer  $> 1$ ).

*Proof.* (a)  $\implies$  (b) Suppose that every Abelian group of order  $n$  is cyclic. Let  $G$  be an Abelian group of order  $n$ . Then  $G = \langle x \rangle \cong Z_n$  for some element  $x \in G$  of order  $n$ . By the fundamental theorem of finitely generated Abelian groups, we have

$$G \cong Z_{n_1} \times \cdots \times Z_{n_r} \cong Z_n$$

where  $n_i$  are elementary divisors. Seeking a contradiction, suppose that  $n$  is not square free, i.e.,  $n = k^2m$ . Then, we have

$$Z_n \cong Z_k \times Z_{km},$$

but the group on the left is cyclic, whereas the group on the right is not (suppose  $(z_1, z_2) \in Z_k \times Z_{km}$  is a generator for  $Z_k \times Z_{km}$ ; then  $|(z_1, z_2)| = k^2m$ , but  $z_1^k = 1$  and  $z_2^{km} = 1$  hence  $(z_1, z_2)^{km} = (z_1^{km}, z_2^{km}) = (1, 1)$ ; i.e., the order of every element  $(z_1, z_2)$  is at most  $\text{lcm}(k, km) = km$ ). This contradicts the assumption that  $G$  is cyclic. Thus,  $n$  must be square free.

(b)  $\implies$  (a) Conversely, suppose that  $n$  is square free. Then, by the fundamental theorem of finitely generated abelian groups, we have

$$G \cong Z_{n_1} \times \cdots \times Z_{n_r}$$

where  $n = n_1 \cdots n_r$  and each  $n_i$  is an elementary divisor of  $n$ , i.e.,  $n_{i+1} \mid n_i$  which implies that  $n_1 = n_2k$  for some positive integer  $k \mid n$ . Thus,  $n = n_1^2kn_3 \cdots n_s$ . But  $n$  is square free thus,  $n_1 = 1$ . Proceeding in this manner, we see that  $n_i = 1$  for all  $i \neq s$  and  $n_s = n$ . Thus,

$$G \cong 1 \times \cdots 1 \times Z_n \cong Z_n$$

is cyclic. ■

**Problem 1.10.** Prove that there is no simple group of order 4125.

*Proof.* Suppose  $G$  is a group of order  $4125 = 3 \cdot 5^3 \cdot 11$ . We need to show that  $G$  contains at least one nontrivial normal subgroup. We shall proceed by Sylow's theorem. By Sylow's theorem,  $n_3 \equiv 1 \pmod{3}$  and  $n_3 \mid 5^3 \cdot 11$  thus,  $n_3 = 1, 25$ , and  $55$ . Similarly  $n_5 = 1$  and  $11$  and  $n_{11} = 1$  and  $375$ .

Forget that. Let us do something tricky. Suppose  $G$  is simple. Then  $G$  has no nontrivial normal subgroup. By Sylow's theorem,  $n_5 = 1$  or  $11$  so  $n_5 = 11$  for otherwise  $G$  has a unique hence, normal Sylow 5-subgroup. Also by Sylow's theorem, recall that  $[G : N_G(P)] = 11$  for any  $P \in \text{Syl}_5(G)$ . Let  $A$  denote the collection of left cosets of  $N_G$ . By Lagrange's theorem,  $|A| = [G : N_G(P)] = 11$ . Let

$G$  act on  $A$  by left multiplication. This action is transitive and hence, induces a homomorphism  $\varphi: G \rightarrow S_{11}$ . Moreover, since  $\ker \varphi \triangleleft G$  and  $G$  is simple,  $\ker \varphi$  is the identity subgroup. Thus, by the 1st isomorphism theorem,  $G \cong \varphi(G)$  so, by Lagrange's theorem,  $3 \cdot 5^3 \cdot 11 \mid 11!$ . However, the highest power of 5 to divide  $11!$  is  $5^2$ . This leads to a contradiction. Thus,  $G$  is not simple. ■

**Problem 1.11.** Show that  $P$  is abelian whenever  $\text{Aut}(P)$  is cyclic.

*Proof.* The problem follows quickly from the following results

**Lemma 2.** Any subgroup of a cyclic group is cyclic.

*Proof.* Suppose that  $G$  is cyclic, i.e.,  $G = \langle x \rangle$  for some element  $x \in G$ . Let  $H < G$ . If  $H$  is the identity subgroup then  $H = \langle e_G \rangle$ . Suppose  $H$  is nontrivial. Since every element of  $G$  is some power of  $x$ , every element of  $H$  is of the form  $x^k$  for some positive integer  $k$ . Put  $y := x^k$  where  $k$  is the smallest power of  $x$  such that  $x^k \in H$ . We show that  $\langle y \rangle = H$ .

First, it is immediate that  $\langle x \rangle < H$ . To see the reverse, let  $z \in H$ . Then  $z = x^\ell$  for some positive integer  $\ell$ . By our previous assumption, we have  $k < \ell$  so by the Euclidean algorithm, there exists positive integers  $q$  and  $r$  such that  $\ell = qk + r$  where  $r < k$  so

$$z = x^\ell = x^{qk+r} = (x^k)^q x^r = y^q x^r.$$

But since  $H$  is a group, we have  $y^{-q}z = x^r \in H$ . But we made the assumption that  $k$  is the smallest integer such that  $x^k \in H$ . Thus,  $r = 0$  and we have  $z = y^q$ . It follows that  $H = \langle y \rangle$ , i.e.,  $H$  is cyclic. ♣

**Lemma 3.** If  $G/Z(G)$  is cyclic, then  $G$  is Abelian.

*Proof.* Suppose  $G/Z(G)$  is cyclic. Then  $G/Z(G) = \langle \bar{x} \rangle$  for some  $x \in G$ . Thus, for every element  $g \in G$ ,  $g = x^k z$  for some  $z \in Z(G)$  for some positive integer  $k$ . Let  $x^{k_1} z_1, x^{k_2} z_2 \in G$ . Then

$$(x^{k_1} z_1)(x^{k_2} z_2) = x^{k_1} x^{k_2} z_1 z_2 = x^{k_1+k_2} z_2 z_1 = x^{k_2+k_1} z_2 z_1 = (x^{k_2} z_2)(x^{k_1} z_1).$$

Thus,  $G$  is Abelian. ♣

Suppose  $\text{Aut}(P)$  is cyclic. Then  $\text{Inn}(P) < \text{Aut}(P)$  is cyclic. But since,  $G/Z(G) \cong \text{Inn}(P)$ , we have that  $G$  is Abelian. ■

**Problem 1.12.** Let  $G$  be a finite group of order  $pqr$ , where  $p > q > r$  are prime.

- (a) If  $G$  fails to have a normal subgroup of order  $p$ , determine the number of elements in  $G$  of order  $p$ .
- (b) If  $G$  fails to have a normal subgroup of order  $q$ , prove that  $G$  has at least  $q^2$  elements of order  $q$ .
- (c) Prove that  $G$  has a nontrivial normal subgroup.

*Proof.* (a) By Sylow's theorem,  $n_p \equiv 1 \pmod{p}$  and  $n_p \mid qr$  so either  $n_p = 1$  or  $n_p = qr$ . Since we are assuming that  $G$  does not have a normal subgroup of order  $p$ ,  $n_p = qr$ . Since every subgroup of order  $p$  is cyclic, for every pair  $P, Q \in \text{Syl}_p(G)$ ,  $P \cap Q = \{e_G\}$ . Thus, the number of elements of order  $p$  must be  $qr(p-1)$ .

(b) Again, by Sylow's theorem,  $n_q \equiv 1 \pmod{q}$  and  $n_q \mid pr$  so either  $n_q = 1$ ,  $p$ , or  $pr$ . Since we are assuming that  $G$  does not have a normal subgroup of order  $p$ ,  $n_q = p$  or  $n_q = pr$ . Thus, we may assume that  $n_q = p$ . Now since every subgroup of order  $q$  is cyclic, the Sylow  $q$ -subgroups of  $G$  intersect pairwise at the identity subgroup. Thus, there are at most  $p(q-1)$  elements of order  $q$ . Now, since  $p > r > q$ ,  $p > q+2$  so  $(q+2)(q-1) = q^2 + q - 1 > q^2$  since  $q > 1$ . Thus,  $G$  has at least  $q^2$  elements of order  $q$ .

(c) Lastly we will show that  $G$  has at least one nontrivial normal subgroup. Seeking a contradiction, suppose that  $G$  does not have a normal Sylow  $r$ -subgroup or a Sylow  $q$ -subgroup. By Sylow's theorem,  $n_r \equiv 1$  and  $n_r \mid pq$  thus,  $n_r = 1, q, p$  or  $pq$ . Since we are assuming that  $G$  does not have a normal Sylow  $r$ -subgroup, then  $n_r$  is at least  $q$ . Thus, there are  $q(r-1)$  elements of order  $r$ . By parts (a) and (b) we have a total of

$$qr(p-1) + q^2 + q(r-1) + 1 = pqr - qr + q^2 + qr - q + 1 = pqr + q(q-1) + 1$$

elements of order  $p$ ,  $q$ , and  $r$  together with the identity element  $e$ . But  $q(q-1) + 1 > 0$  so we have  $pqr + q(q-1) + 1 > pqr = |G|$ . This is a contradiction. Thus, at least one of  $n_p$ ,  $n_q$  or  $n_r$  must equal 1 and hence, at least one of the  $p$ ,  $q$ , or  $r$  Sylow subgroups is normal in  $G$ . ■

**Problem 1.13.** Find all abelian groups of order 60. Find the number of elements of order 6 in each group.

*Proof.* Suppose  $G$  is an Abelian group of order  $|G| = 2^2 \cdot 3 \cdot 5$ . By the fundamental theorem of finitely generated abelian groups, we have that  $G$  is isomorphic to one of

$$Z_{2 \cdot 3 \cdot 5} \times Z_2 = Z_{30} \times Z_2 \quad \text{or} \quad Z_{2^2 \cdot 3 \cdot 5} = Z_{60}.$$

For  $G \cong Z_{60}$ , recall that since  $G$  is Abelian,  $G$  has a subgroup of order  $m$  for every positive integer  $n$  dividing  $m$ . Thus,  $G$  has a subgroup of order 6. Moreover, since  $Z_{60}$  is cyclic, this subgroup too is cyclic. Therefore, by Euler's totient theorem, this subgroup contains a total of  $\varphi(6) = \varphi(3)\varphi(2) = (3-1)(2-1) = 2$  elements of order 6.

For  $G \cong Z_{30} \times Z_2$ , if  $(z_1, z_2) \in G$  is an element of order 6 then  $z_1$  must be an element of order 3 or order 6 and  $z_2$  must be an (the only) element of order 2 (since  $|(z_1, z_2)| = \text{lcm}(|z_1|, |z_2|)$ ). Therefore, it suffices to count the elements of order 3 and 6 in  $Z_{30}$  and pair them up with an element of order 2 and an element of order 1 or 2, respectively. For the same reasons as above,  $G$  must contain a subgroup of order 3 and a subgroup of order 6. By Euler's totient theorem,  $\varphi(3) = 2$  and  $\varphi(6) = 2$ . Thus, there are  $2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 = 6$  elements of order 6 in  $G \cong Z_{30} \times Z_2$ . ■

**Problem 1.14.** Show that any group  $G$  of order 80 is solvable.

*Proof.* Suppose  $G$  is a group of order  $80 = 2^4 \cdot 5$ . By Sylow's theorem,  $n_5 \equiv 1 \pmod{5}$  and  $n_5 \mid 2^4$ . Thus,  $n_5 = 1, 16$ . Similarly,  $n_2 = 1$  or  $n_2 = 5$ .

If  $n_5 = 1$  we are done since  $P_5 \in \text{Syl}_5(G)$  is the unique Sylow 5-subgroup of  $G$  hence,  $P_5 \triangleleft G$  and  $G/P_5$  is a group of order  $2^4$ , i.e., a  $p$ -group hence,  $P_5$  and  $G/P_5$  are solvable. Thus,  $G$  is solvable.

Suppose  $n_5 \neq 1$ , then we must show that  $n_2 = 1$ . Since  $n_5 \neq 1$ , we have  $n_5 = 16$  and we have  $16(5 - 1) = 16 \cdot 4 = 64$  elements of order 5 which leaves  $80 - 64 - 1 = 15$  elements unaccounted for. Thus,  $n_2 = 1$  so  $P_2 \in \text{Syl}_2(G)$  is a normal subgroup of  $G$ . Thus,  $P_2 \triangleleft G$  and  $|P_2| = 2^4$  is a  $p$ -group hence, solvable. Moreover,  $|G/P_2| = 5$  hence, is Abelian thus, solvable. Therefore,  $G$  is solvable. ■

**Problem 1.15.** Let  $G$  be a finite group and suppose that  $\text{Aut}(G)$  is solvable. Show that  $G$  is solvable.

*Proof.* Suppose that  $\text{Aut}(G)$  is solvable. Then  $\text{Inn}(G) < \text{Aut}(G)$  is solvable. But  $\text{Inn}(G) \cong G/Z(G)$ . Thus,  $G/Z(G)$  is solvable. Since  $Z(G) \triangleleft G$  is Abelian,  $Z(G)$  is solvable. Thus,  $G$  is solvable. ■



## 1.2 Rings

**Problem 1.16.** Let  $R$  be a commutative ring with  $1 \neq 0$  and let  $\mathfrak{p}$  be a prime ideal of  $R$ . Let  $I$  and  $J$  be ideals of  $R$  such that  $I \cap J \subset \mathfrak{p}$ , prove that either  $I \subset \mathfrak{p}$  or  $J \subset \mathfrak{p}$ .

*Proof.* Without loss of generality, suppose that  $I \not\subset \mathfrak{p}$ . We show that  $J \subset \mathfrak{p}$ . Let  $x \in I$ . Then  $x \notin \mathfrak{p}$ . But for any  $y \in J$ ,  $xy \in I \cap J$ . Thus,  $xy \in \mathfrak{p}$ . Since  $\mathfrak{p}$  is prime,  $x \in \mathfrak{p}$  or  $y \in \mathfrak{p}$ . But  $x \notin \mathfrak{p}$  hence,  $y \in \mathfrak{p}$ . This is true for any  $y \in J$ . Thus,  $J \subset \mathfrak{p}$ . ■

**Problem 1.17.** Prove that a finite integral domain is a field.

*Proof.* Let  $a \in R$  be a nonzero element. Define the map  $\varphi_a: R \rightarrow R$  by  $\varphi_a(x) := ax$ . Then  $\varphi_a$  defines a group homomorphism on  $R$  viewed as an additive Abelian group: Let  $x, y \in R$  then

$$\begin{aligned}\varphi_a(x + y) &= a(x + y) \\ &= ax + ay \\ &= \varphi_a(x) + \varphi_a(y).\end{aligned}$$

Now, let  $x \in \ker \varphi$ . Then  $\varphi_a(x) = ax = 0$ . Since  $R$  is a domain and  $a \neq 0$ ,  $x = 0$ . Thus,  $\varphi$  is injective. Since  $R$  is finite and  $\varphi_a: R \rightarrow R$  is injective,  $\varphi_a$  is surjective (by the pigeonhole principle). Thus, there exists an element  $b \in R$  such that  $\varphi_a(b) = ab = 1$ . Thus,  $a$  is a unit. Since  $\varphi_a$  chosen arbitrarily, it follows that every nonzero element  $a \in R$  is a unit. Thus,  $R$  is a field. ■

**Problem 1.18.** An element  $x$  of a ring  $R$  is called nilpotent if some power of  $x$  is zero. Prove that if  $x$  is nilpotent, then  $1 + x$  is a unit in  $R$ .

*Proof.* First we will prove the following:

**Lemma 4.** If  $x$  is nilpotent, then  $-x$  is nilpotent.

*Proof.* Suppose that  $x$  is nilpotent. Then  $x^n = 0$  for some positive integer  $n$ . Then

$$(-x)^n = (-1)^n \cdot x^n = (-1)^n \cdot 0 = 0.$$

Thus,  $-x$  is nilpotent. ♣

Now, since  $x$  is nilpotent, by the preceding lemma,  $-x$  is nilpotent. Thus

$$(-x)^n - 1 = (-x - 1)((-x)^{n-1} + \cdots + 1).$$

Since  $x^n = 0$ , we have

$$-1 = ((-x) - 1)((-x)^{n-1} + \cdots + 1)$$

or

$$1 = (1 + x)((-x)^{n-1} + \cdots + 1).$$

Thus,  $1 + x$  is a unit. ■

**Problem 1.19.** Let  $R$  be a nonzero commutative ring with 1. Show that if  $I$  is an ideal of  $R$  such that  $1 + a$  is a unit in  $R$  for all  $a \in I$ , then  $I$  is contained in every maximal ideal of  $R$ .

*Proof.* Seeking a contradiction, assume otherwise. Then there exists a maximal ideal  $\mathfrak{m}$  such that  $\mathfrak{m} \not\supset I$ , i.e., for some  $a \in I$ ,  $a \notin \mathfrak{m}$ . Consider the ideal generated by  $(a)$ . Since  $a \in I$ ,  $(a) \neq R$  since  $I$  is a proper ideal of  $R$ , in particular, since  $a$  is a nonunit. Consider the ideal  $\mathfrak{m} + (a)$ . Since  $a \notin \mathfrak{m}$ ,  $\mathfrak{m} \subset \mathfrak{m} + (a)$ . But since  $\mathfrak{m}$  is maximal, it follows that  $\mathfrak{m} + (a) = R$ . Hence, there exists an element  $m \in \mathfrak{m}$  such that  $m + ra = 1$  for some  $r \in R$ . Then we have  $m = 1 - ra$ . Since  $-r \in R$  and  $a \in I$ , we have  $-ra \in I$  so  $m = 1 + (-ra)$  is a unit thus,  $\mathfrak{m} = R$ . This contradicts that  $\mathfrak{m}$  is a maximal ideal. Thus,  $I$  is contained in every maximal ideal of  $R$ . ■

**Problem 1.20.** Let  $R$  be an integral domain and  $F$  be its field of fractions. Let  $\mathfrak{p}$  be a prime ideal in  $R$  and

$$R_{\mathfrak{p}} := \left\{ \frac{a}{b} \mid a, b \in R, b \notin \mathfrak{p} \right\} \subset F.$$

Show that  $R_{\mathfrak{p}}$  has a unique maximal ideal.

*Proof.* We will show that

$$\mathfrak{p}R_{\mathfrak{p}} := \left\{ \frac{a}{b} \mid a \in \mathfrak{p}, b \notin \mathfrak{p} \right\}$$

is the unique maximal ideal of  $R_{\mathfrak{p}}$ . We will show that  $a/b \in R_{\mathfrak{p}}$  is a unit if and only if  $a/b \notin \mathfrak{p}R_{\mathfrak{p}}$ .

⇒ Suppose that  $a/b$  is a unit. Then there exists an element  $a'/b'$  such that

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd} = \frac{1}{1}.$$

That is, there exists an element  $s \in R \setminus \mathfrak{p}$  such that  $s(ac - bd) = 0$ . Since  $R$  is an integral domain,  $s \neq 0$  so  $ac - bd = 0$  implies  $ac = bd$ . Since  $b, d \notin \mathfrak{p}$ ,  $bd \notin \mathfrak{p}$  (since  $\mathfrak{p}$  is prime) and, in particular,  $ac \notin \mathfrak{p}$  so  $a/b \notin \mathfrak{p}R_{\mathfrak{p}}$ .

⇐ Conversely, suppose that  $a/b \notin \mathfrak{p}R_{\mathfrak{p}}$ . Then  $a \notin \mathfrak{p}$ . Thus,  $b/a \in R_{\mathfrak{p}}$  and

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{ab}{ba} = \frac{1}{1}.$$

Thus,  $a/b$  is a unit in  $R_{\mathfrak{p}}$ .

Now, since  $\mathfrak{p}R_{\mathfrak{p}}$  does not contain any units, it is a proper ideal of  $R_{\mathfrak{p}}$ . Moreover, for every  $a/b \notin \mathfrak{p}R_{\mathfrak{p}}$ ,  $\mathfrak{p}R_{\mathfrak{p}} + (a/b) = R_{\mathfrak{p}}$  so  $\mathfrak{p}R_{\mathfrak{p}}$  is a maximal ideal, i.e., is not contained in any proper ideal of  $R_{\mathfrak{p}}$ . Any other ideal must contain a unit or is strictly contained in  $\mathfrak{p}R_{\mathfrak{p}}$ . Thus,  $\mathfrak{p}R_{\mathfrak{p}}$  is the unique maximal ideal of  $R_{\mathfrak{p}}$ . ■

**Problem 1.21.** Let  $m$  and  $n$  be relatively prime integers. Show that there is an isomorphism  $Z_{mn}^{\times} \cong Z_m^{\times} \times Z_n^{\times}$ .

*Proof.* Suppose  $m$  and  $n$  are relatively prime. Then  $(m) + (n) = \mathbb{Z}$ , i.e.,  $(m)$  and  $(n)$  are comaximal. By the Chinese remainder theorem there is a ring isomorphism

$$Z_{mn} \cong Z_m \times Z_n.$$

which gives an isomorphism of the group of units

$$Z_{mn}^{\times} \cong (Z_m \times Z_n)^{\times}.$$

Thus, it suffices to show that  $(Z_m \times Z_n)^{\times} = Z_m^{\times} \times Z_n^{\times}$ .

Suppose  $(a, b) \in (Z_m \times Z_n)^\times$ . Then  $(a, b)$  is a unit in  $Z_m \times Z_n$ , i.e., there exists  $(c, d)$  such that  $(a, b)(c, d) = (1, 1)$ . But  $(a, b)(c, d) = (1, 1)$  if and only if  $ac = 1$  and  $bd = 1$ . Thus,  $a \in Z_m^\times$  and  $b \in Z_n^\times$  so  $(a, b) \in Z_m^\times \times Z_n^\times$ . Conversely, if  $(a, b) \in Z_m^\times \times Z_n^\times$  then  $a$  is a unit in  $Z_m$  and  $b$  is a unit in  $Z_n$ . Thus, there exists elements  $c \in Z_m$  and  $d \in Z_n$  such that  $ac = 1$  and  $bd = 1$  so  $(a, b)(c, d) = (ac, bd) = (1, 1)$ . Thus,  $(a, b) \in (Z_m \times Z_n)^\times$ . ■

**Problem 1.22.** Show that if  $x$  is non-nilpotent in  $R$  then a maximal ideal  $\mathfrak{p}$  of  $R$ , which does not contain  $x^n$  for  $n = 1, 2, \dots$ , is prime.

*Proof.* I think what the professor had in mind was to prove this: “Show that if  $x$  is non-nilpotent in  $R$  then the ideal  $\mathfrak{p}$ , which is maximal with respect to not containing  $x^n$  for any  $n \in \mathbb{Z}$ , is prime.”

This looks like a standard commutative algebra problem. Let  $S := \{x^k \mid k \geq 1\}$ , i.e., the multiplicative set generated by  $x$  and suppose that  $\mathfrak{p}$  is an ideal maximal with respect to  $\mathfrak{p} \cap S = \emptyset$ . Seeking a contradiction suppose  $a, b \in R$  with  $ab \in \mathfrak{p}$  but  $a, b \notin \mathfrak{p}$ . Then, the ideals  $\mathfrak{p} + (a)$  and  $\mathfrak{p} + (b)$  contain  $\mathfrak{p}$  and therefore must contain a power of  $x$ , say  $x^m$  and  $x^n$ , respectively. Thus, we have

$$x^m x^n = x^{m+n} \in (\mathfrak{p} + (a))(\mathfrak{p} + (b)) \subset \mathfrak{p} + (ab) \subset \mathfrak{p}.$$

But  $\mathfrak{p}$  is maximal with respect to not containing any power of  $x$ . This is a contradiction. Thus, we must have  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$  which implies  $\mathfrak{p}$  is prime. ■

**Problem 1.23.** Let  $\mathbb{Q}$  be the field of rational numbers and  $D = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ .

- (a) Show that  $D$  is a principal ideal domain.
- (b) Show that  $\sqrt{3}$  is not an element of  $D$ .

*Proof.* (a) First we define a Euclidean norm  $d: D \rightarrow \mathbb{Z}_{\geq 0}$  via  $d(a + b\sqrt{2}) := a^2 + 2b^2$ . Let  $I \subset D$  be a proper ideal. Let  $x = a + b\sqrt{2} \in I$  be minimal with respect to the Euclidean norm, i.e.,  $d(x) \leq d(y)$  for all  $y \in I$ .

(b) ■

**Problem 1.24.** Show that if  $p$  is a prime such that  $p \equiv 1 \pmod{4}$ , then  $x^2 + 1$  is not irreducible in  $\mathbb{Z}_p[x]$ .

*Proof.* ■

**Problem 1.25.** Show that if  $p$  is a prime such that  $p \equiv 3 \pmod{4}$ , then  $x^2 + 1$  is irreducible in  $\mathbb{Z}_p[x]$ .

*Proof.* ■

**Problem 1.26.** Find a simpler description for each of the following rings:

0.  $\mathbb{Z}[x]/(x^2 - 3, 2x + 4);$

0.  $\mathbb{Z}[i]/(2 + i) \ (i^2 = -1).$

*Proof.* ■

**Problem 1.27.** Show that  $\mathbb{Z}[\sqrt{-13}]$  is not a principal ideal domain. ■

*Proof.*

**Problem 1.28.** Let  $D$  be a principal ideal domain. Prove that every nonzero prime ideal of  $D$  is a maximal ideal. ■

*Proof.*

**Problem 1.29.** Prove or disprove that a nonzero prime ideal  $P$  of a principal ideal domain  $R$  is a maximal ideal. ■

*Proof.*

**Problem 1.30.** Consider the polynomial  $f(x) = x^4 + 1$ .

(a) Use the Eisenstein Criterion to show that  $f(x)$  is irreducible in  $\mathbb{Z}[x]$ .

(b) Prove that  $f(x)$  is reducible in  $\mathbf{F}_p[x]$  for every prime  $p$ .

*Proof.* ■

**Problem 1.31.** Assume that  $f(x)$  and  $g(x)$  are polynomials in  $\mathbb{Q}[x]$  and that  $f(x)g(x) \in \mathbb{Z}[x]$ . Prove that the product of any coefficient of  $f(x)$  with any coefficient of  $g(x)$  is an integer.

*Proof.* ■

**Problem 1.32.** Let  $k$  be a field,  $x, y$ , indeterminates. Let  $f(x)$  and  $g(x)$  be relatively prime polynomials in  $k[x]$ . Show that in the polynomial ring  $k(y)[x]$ ,  $f(x) - yg(x)$  is irreducible.

*Proof.* ■

### 1.3 Fields

**Problem 1.33.** Let  $F$  be a field with prime characteristic  $\text{ch}(F) = p$ . Let  $L/F$  be a finite extension such that  $p$  does not divide  $[L : F]$ . Show that  $L/F$  is a separable extension.

*Proof.* ■

**Problem 1.34.** Let  $\zeta_5$  be a primitive 5-th root of unity, and denote  $\theta = \zeta_5 + \zeta_5^{-1}$  as an element of the cyclotomic field  $\mathbb{Q}(\zeta_5)$ . Show that the minimal polynomial of  $\theta$  over  $\mathbb{Q}$  is  $m_{\theta, \mathbb{Q}}(x) = x^2 + x - 1$ .

*Proof.* ■

**Problem 1.35.** Prove or disprove the following: If  $f(x), g(x) \in \mathbb{Q}[x]$  are irreducible polynomials that have the same splitting field, then  $\deg f = \deg g$ .

*Proof.* ■

**Problem 1.36.** Prove or disprove that every finite algebraic extension field of  $\mathbb{F}_{p^n}$  is Galois.

*Proof.* ■

**Problem 1.37.** If  $[K : \mathbb{F}_p]$  divides  $[L : \mathbb{F}_p]$ , does it follow that  $K$  is isomorphic to a subfield of  $L$ .

*Proof.* ■

**Problem 1.38.** Let  $\mathbb{F}_p$  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  $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = a$  is the least positive integer such that  $p^a \equiv 1 \pmod{n}$ . [*Hint:* the Galois group of the extension of  $\mathbb{F}_p$  is generated by the Frobenius automorphism.]

*Proof.* ■

**Problem 1.39.** Fix a prime  $p$ , and consider the polynomial  $f(x) = x^p - x - 1$ . Let  $\mathbb{F}_p(f)$  be the splitting field of  $f(x)$  over  $\mathbb{F}_p$ . Let  $a \in \mathbb{F}_p(f)$  be a root of  $f$ .

- (a) Show that  $a \mapsto a + 1$  defines an automorphism of  $\mathbb{F}_p(f)$ .

*Proof.* Let ■

- (b) Show that  $\text{Gal}(\mathbb{F}_p(f)/\mathbb{F}_p) \cong \mathbb{Z}_p$ .

*Proof.* ■

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

*Proof.* ■

$\mathbb{F}_p(f)/\mathbb{F}_p$  is called an Artin–Schreier Extension.

**Problem 1.40.** Let  $x$  and  $y$  be indeterminates over the field  $\mathbb{F}_2$ . Prove that there exists infinitely many subfields of  $L = \mathbb{F}_2(x, y)$  that contain the field  $K = \mathbb{F}_2(x^2, y^2)$ .

*Proof.* ■

**Problem 1.41.** Let  $K/F$  be an algebraic field extension. If  $K = F(a)$  for some  $a \in K$ , prove that there are only finitely many subfields of  $K$  that contain  $F$ .

*Proof.* ■

**Problem 1.42.** Let  $p$  be a prime integer. Recall that a field extension  $K/F$  is called a  $p$ -extension if  $K/F$  is Galois and  $[K : F]$  is a power of  $p$ . If  $K/F$  and  $L/K$  are  $p$ -extensions, prove that the Galois closure of  $L/F$  is a  $p$ -extension.

*Proof.* ■

**Problem 1.43.** Give an example where  $K/F$  and  $L/K$  are  $p$ -extensions, but  $L/F$  is not Galois.

*Proof.* ■

**Problem 1.44.** Let  $L/\mathbb{Q}$  be the splitting field of the polynomial  $x^6 - 2 \in \mathbb{Q}[x]$ .

- (a) If  $a$  is one root of  $x^6 - 2$ , draw the subfield lattice of the extension  $\mathbb{Q}(a)$  over  $\mathbb{Q}$ .
- (b) Give generators for each subfield  $K$  of  $L$  for which  $[K : \mathbb{Q}] = 2$ . How many are there?
- (c) Give generators for each subfield  $K$  of  $L$  for which  $[K : \mathbb{Q}] = 3$ . How many are there?
- (d) Give generators for each subfield  $K$  of  $L$  for which  $[K : \mathbb{Q}] = 4$ . How many are there?
- (e) How many subfields  $K$  of  $L$  have index  $[L : K] = 2$ ?

**Problem 1.45.** Give an example of a field  $F$  having characteristic  $p > 0$  and irreducible monic polynomial  $f(x) \in F[x]$  that has a multiple root.

*Proof.* ■

**Problem 1.46.** Let  $f$  be an irreducible polynomial of degree  $k$  over  $\mathbb{F}_p$ . Find the splitting field of  $f$  and its Galois group.

*Proof.* ■

**Problem 1.47.** Let  $n$  be a positive integer and  $d$  a positive integer that divides  $n$ . Suppose  $a \in \mathbb{R}$  is a root of the polynomial  $x^n - 2 \in \mathbb{Q}[x]$ . Prove that there is precisely one subfield  $F$  of  $\mathbb{Q}(a)$  with  $[F : \mathbb{Q}] = d$ .

*Proof.* ■

**Problem 1.48.** Let  $a = \sqrt[3]{5 - \sqrt{7}}$ .

- (a) Find the minimal polynomial of  $a$ , and the conjugates of  $a$ .
- (b) Determine the Galois closure of  $F$  of  $\mathbb{Q}(a)$ .

(c) Show that  $F/\mathbb{Q}$  is an extension by radicals.

(d) Conclude that  $\text{Gal}(F/\mathbb{Q})$  is solvable.

*Proof.* ■

**Problem 1.49.** Let  $F$  be a field of characteristic  $p > 0$ . Fix an element  $c$  in  $F$ . Prove that  $f(x) = x^p - c$  is irreducible in  $F[x]$  if and only if  $f(x)$  has no roots in  $F$ .

*Proof.* ■

**Problem 1.50.** Determine the Galois group of the splitting field over  $\mathbb{Q}$  and all its subfields for

(a)  $f(x) = x^3 - 2$

(b)  $f(x) = x^4 + 2$

(c)  $f(x) = x^4 + 4$

(d)  $f(x) = x^4 + 4x + 2$

*Proof.* ■

**Problem 1.51.** Show that  $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ , where  $\zeta_3^2 + \zeta_3 + 1 = 0$ .

*Proof.* ■

**Problem 1.52.** 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.,  $F \subseteq E \subseteq L$  and  $[E : F] = 2$ .

(b) Does there exist a unique subfield  $K$  of index 2, i.e.,  $F \subseteq E \subseteq L$  and  $[E : F] = 2$ .

*Proof.* ■

**Problem 1.53.** Let  $L/F$  be a Galois extension of degree  $[L : F] = p^2$  for some prime  $p$ . Let  $K$  be a subfield satisfying  $F \subset K \subset L$ . Must  $K/F$  be a normal extension?

*Proof.* ■

**Problem 1.54.** Let  $L/F$  be the Galois closure of the separable algebraic field extension  $F(\theta)/F$ . Let  $p$  be a prime that divides  $[L : F]$ . Prove that there exists a subfield  $K$  of  $L$  such that  $[L : K] = p$  and  $L = K(\theta)$ .

*Proof.* Since  $p$  divides  $[L : K]$ ,  $[L : K] = pn$  for some positive integer  $n$ . ■

**Problem 1.55.** Suppose  $L/\mathbb{Q}$  is a finite field extension with  $[L : \mathbb{Q}] = 4$ . Is it possible that there exist precisely two subfields  $K_1$  and  $K_2$  of  $L$  for which  $[L : K_i] = 2$ ? Justify your answer.

*Proof.* ■

## 2 January 2007

**Problem 2.1.** 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 5.** 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 2.2.** 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 2.3.** 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 2.4.** 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 2.5.** 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 2.6.** 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 2.7.** 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 2.8.** 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 2.9.** 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 2.10.** 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.* ■

### 3 Spring 2008

**Problem 3.1.** 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 3.2.** 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 3.3.** 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 3.4.** 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 3.5.** 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 3.6.** 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 3.7.** 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 3.8.** 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 3.9.** 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 3.10.** Determine the Galois group of the splitting field over  $\mathbb{Q}$  of  $f(x) = x^4 + 4$ .

*Proof.*

■

**4 August, 2015**

**Problem 4.1.**

*Proof.*



## 4.1 August 2010