MA553 Past Qualifying Examinations

Carlos Salinas

January 2, 2016

1 Heinzer MA 553 Problems

Past Heinzer and Włodarczyk problems with proofs to the theorems, corrolaries, 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 $0, ..., n-1$ 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, $r \cdot a \mapsto a + 1 \mod n$) and $s \cdot a \in A$ (that is, $s \cdot a \mapsto n - 1 \mod n$ or something like that) and r, s are generators for D_{2n}.

Next, it is easy to see that the action is transitive for $r^k \cdot a \mapsto a + k \mod n$ 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 $\langle e \rangle \subset \mathrm{Stab}_{D_{2n}}(A)$ (this is always true). Let $g \in \mathrm{Stab}_{D_{2n}}(A)$. Then, $g \cdot a = a \mod n$ 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 $\varphi\colon D_{2n} \hookrightarrow S_n$ with kernel $\langle e \rangle$ the identity element, i.e., φ 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 premutations of S_5 hence, are contained in some Sylow 5-subgroup P. Since G is the larges 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 $G \lhd A_5$, but A_5 is simple. Thus, $n_5 = 6$.

Hence, $n_5 = 6$ and we have that

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

Problem 1.3. Show that for any element σ 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 σ 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 σ must be a product of disjoint transposition, i.e., disjoint 2-cycles.

Now, since $\sigma \in A_n$, σ 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

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

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. $\Longrightarrow$ Put $|G| = p^\alpha m$ for positive integer m and α, where m is not divisible by p. Suppose that $P \in \mathrm{Syl}_p(G)$ 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.

$\Longleftarrow$ 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 $P \in \mathrm{Syl}_p(H)$. 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 $Q \in \mathrm{Syl}_p(H)$. 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 $P \in \mathrm{Syl}_p(G)$ then $PH/H \in \mathrm{Syl}_p(G/H)$. 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 $H \lhd G$, 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 $Q \in \mathrm{Syl}_p(G/H)$, then $|Q| = p^{\alpha-\beta}$. Thus, by a simple order argument, it must be that $PH/H \in \mathrm{Syl}_p(G/H)$ (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 $Q \in \mathrm{Syl}_p(G/H)$. By Sylow's theorem, Q is conjugate to a subgroup of the form RH/H where $R \in \mathrm{Syl}_p(G)$. 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 $H \lhd G$ 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 $R \in \mathrm{Syl}_p(G)$ 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 is says is that normal Sylow p-subgroups are *characteristic subgroups*, i.e., if K is characteristic in H and $K \lhd G$ then $K \lhd H$ and $K \lhd G$.

Suppose N is a normal Sylow p-subgroup of H. Then N is the unique Sylow p-subgroup of H. Since $H \lhd G$, 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, $N \lhd G$. ∎

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 $Q \in \mathrm{Syl}_p(G)$.

(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^α 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 $HK \lhd G$. 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 $H \lhd G$ and $K \lhd G$. Thus, $HK \lhd G$. 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 $\mathrm{Aut}\big((\mathbb{Z}/3\mathbb{Z})^4\big) \cong \mathrm{GL}_4(\mathbb{Z}/3\mathbb{Z})$ 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) $\Longrightarrow$ (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 $\mathrm{lcm}(k, km) = km$). This contradicts the assumption that G is cyclic. Thus, n must be square free.

(b) $\Longrightarrow$ (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, $n = n_1^2 k n_3 \cdots n_s$. But n is square free thus, $n_1 = 1$. Proceeding in this manner, we see than $n_i = 1$ 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 $P \in \mathrm{Syl}_5(G)$. 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 $\varphi\colon G \to S_{11}$. Moreover, since $\ker\varphi \lhd G$ 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 $\mathrm{Aut}(P)$ 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 $y \coloneqq x^k$ 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 ℓ. 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

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

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

$$(x^{k_1}z_1)(x^{k_2}z_2) = x^{k_1}x^{k_2}z_1z_2 = x^{k_1+k_2}z_2z_1 = x^{k_2+k_1}z_2z_1 = (x^{k_2}z_2)(x^{k_1}z_1).$$

Thus, G is Abelian. ♣

Suppose $\mathrm{Aut}(P)$ is cyclic. Then $\mathrm{Inn}(P) < \mathrm{Aut}(P)$ is cyclic. But since, $G/Z(G) \cong \mathrm{Inn}(P)$, 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 $P, Q \in \mathrm{Syl}_p(G)$, $P \cap Q = \{e_G\}$. 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 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

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

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 $|(z_1, z_2)| = \mathrm{lcm}(|z_1|, |z_2|)$). 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 $P_5 \in \mathrm{Syl}_5(G)$ is the unique Sylow 5-subgroup of G hence, $P_5 \lhd G$ 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 $P_2 \in \mathrm{Syl}_2(G)$ is a normal subgroup of G. Thus, $P_2 \lhd G$ 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 $\mathrm{Aut}(G)$ is solvable. Show that G is solvable.

Proof. Suppose that $\mathrm{Aut}(G)$ is solvable. Then $\mathrm{Inn}(G) < \mathrm{Aut}(G)$ is solvable. But $\mathrm{Inn}(G) \cong G/Z(G)$. Thus, $G/Z(G)$ is solvable. Since $Z(G) \lhd G$ 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 $I \subset P$ or $J \subset P$.

Proof. Without loss of generality, suppose that $I \not\subset J$. 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 $\varphi_a \colon R \to R$ by $\varphi_a(x) := ax$. Then φ_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, φ is injective. Since R is finite and $\varphi_a \colon R \to R$ is injective, φ_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 φ_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 ideals. 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

$$R_{\mathfrak{p}} \coloneqq \left\{ \tfrac{a}{b} \;\middle|\; a, b \in R,\, b \notin \mathfrak{p} \right\} \subset F.$$

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

Proof. We will show that

$$\mathfrak{p}R_{\mathfrak{p}} \coloneqq \left\{ \tfrac{a}{b} \;\middle|\; a \in \mathfrak{p},\, b \notin \mathfrak{p} \right\}$$

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

$\Longrightarrow$ 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 $a/b \notin \mathfrak{p}R_{\mathfrak{p}}$.

$\Longleftarrow$ 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 $R_{\mathfrak{p}}$. Morevore, for every $a/b \notin \mathfrak{p}R_{\mathfrak{p}}$, $\mathfrak{p}R_{\mathfrak{p}} + (a/b) = R_{\mathfrak{p}}$ so $\mathfrak{R}_{\mathfrak{p}}$ 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 $(Z_m \times Z_n)^{\times} = Z_m^{\times} \times Z_m^{\times}$.

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 $n = 1, 2, ...$, 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 $S := \left\{ x^k \mid k \geq 1 \right\}$, 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 $D = \left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \right\}$.

(a) Show that D is a principal ideal domain.

(b) Show that $\sqrt{3}$ is not an element of D.

Proof. (a) We prove the following stronger result (which is, incidentally, easier to prove than what we are asked to prove): D is a field (in fact, it is the extension $\mathbb{Q}(\sqrt{2})$). Let $a + b\sqrt{2} \in D$ be a nonzero element. To show that $a + b\sqrt{2}$ is a unit, it suffices to find an inverse for it. Hence, we have

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Note that $a^2 - 2b^2 \neq 0$ if and only if $a^2 = 2b^2$, but this implies that $a = \sqrt{2}b$ which is impossible since $\sqrt{2} \notin \mathbb{Q}$ so that the above is indeed in D. Now, we have

$$\begin{aligned}
(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right) &= \frac{1}{a^2 - 2b^2}\left(a^2 + ab\sqrt{2} - 2b^2 + -ba\sqrt{2}\right) \\
&= \frac{a^2 - 2b^2}{a^2 - 2b^2} \\
&= 1.
\end{aligned}$$

Thus, D is a field.

(b) We shall proceed by contradiction. Suppose that $\sqrt{3} \in D$. Then

$$\sqrt{3} = a + b\sqrt{2}$$

for some $a, b \in \mathbb{Q}$. Squaring both sides, we have

$$\begin{aligned} 3 &= a^2 + 2b^2 + 2ab\sqrt{2} \\ 3 - a^2 - 2b^2 &= 2ab\sqrt{2} \\ \sqrt{2} &= \frac{3 - a^2 - 2b^2}{2ab}. \end{aligned}$$

This implies that $\sqrt{2} \in \mathbb{Q}$, which is a contradiction. ■

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 $\mathbb{F}_p[x]$.

Proof. Since $p \equiv 1 \pmod 4$, $p = a^2 + b^2$ for some integers a and b. It follows that $b \not\equiv 0 \pmod p$ or else $a = \sqrt{p}$ or $a^2 + b^2 > p$, a contradiction. Thus b is a unit in $\mathbb{F}_p$. We claim that ab^{-1} is a root of $x^2 + 1$. First note that

$$(ab^{-1})^2 + 1 = a^2 b^{-2} + 1.$$

Since $a^2 + b^2 \equiv 0 \pmod p$, it follows that $b^{-2}(a^2 + b^2) \equiv 0 \pmod p$, but $b^{-2}(a^2 + b^2) = a^2 b^{-2} + 1$. Thus, $a^2 b^{-2} + 1 = 0$ in $\mathbb{F}_p$. Thus, $a^2 b^{-2} + 1 = 0$ in $\mathbb{F}_p$ so $x^2 + 1$ has a root in $\mathbb{F}_p[x]$ and hence, is reducible. ■

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

Proof. Note that $p - 1 \equiv 2 \pmod 4$. In particular, we see that $4 \nmid p - 1$ for all primes p satisfying the conditions above. Now, consider multiplicative subgroup $(\mathbb{F}_p[x])^\times \cong Z_{p-1}$ of $\mathbb{F}_p[x]$, this is a cyclic group of order $p - 1$. If $F_p^\times$ had an element of order 4 then, by Lagrange's theorem, $4 \mid p - 1$. But this is false. Now suppose there exists $a \in \mathbb{F}_p$ such that $a^2 = -1$. Then $a^4 = (-1)^2 = 1$. It follows that $a \neq 1$ and $a^3 \neq 1$, so a is an element of order 4 in $\mathbb{F}_p^\times$. Thus, x^2 does not have a root in $\mathbb{F}_p[x]$. Since $x^2 + 1$ is of degree 2, it follows that $x^2 + 1$ is irreducible in $\mathbb{F}_p[x]$ for $p \equiv 3 \pmod 4$. ■

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. It suffices to exhibit an ideal that is not generated by a single element. To that end, consider the ideal generated by ■

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 $\mathbb{F}_p[x]$ 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 $\mathrm{ch}(F) = p$. Let L/F be a finite extension such that p does not divide $[L : F]$. Show that L/F is a separable extension.

Proof. Seeking a contradiction, suppose that L/F is not separable. The there exists an element $\alpha \in L$ such that its minimal polynomial $m_{\alpha,F}(X)$ is not separable, i.e., $m_{\alpha,F}$ has a multiple root. But recall that an irreducible polynomial $g(X)$ is separable if $\deg(D(g)) = \deg(g) - 1$. Thus, we must have $\deg(D(m_{\alpha,F})) < \deg(m_{\alpha,F}) - 1$ (since for any polynomial f, $\deg(D(f)) \leq \deg(f) - 1$). But since $\mathrm{ch}(F) = p$, this is true only if $p \mid \deg(m_{\alpha,F})$. For suppose not. Then $m_{\alpha,F}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ and

$$D(m_{\alpha,F}) = nX^{n-1} + \text{some terms of lower degree.}$$

so that $\deg(D(m_{\alpha,F})) = n - 1 = \deg(m_{\alpha,F}) - 1$. Hence, we have $p \mid [F(\alpha) : L]$ and by the tower theorem,

$$[L : F] = [L : F(\alpha)][F(\alpha) : L]$$

implies that $p \mid [L : F]$. This is a contradiction. Thus, L/F is separable. ■

Problem 1.34. Let ζ_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 θ over $\mathbb{Q}$ is $m_{\theta,\mathbb{Q}}(X) = X^2 + X - 1$.

Proof. Via some algebra, **:^)**, we have

$$({\zeta_5} + {\zeta_5}^{-1})^2 + ({\zeta_5} + {\zeta_5}^{-1}) - 1 = {\zeta_5}^2 + 2 + {\zeta_5}^{-2} + \zeta_5 + {\zeta_5}^{-1} - 1,$$

but since ${\zeta_p}^{-k} = {\zeta_p}^{p-k}$ we have

$$\begin{aligned} &= {\zeta_5}^2 + 2 + {\zeta_5}^3 + \zeta_5 + {\zeta_5}^4 - 1 \\ &= {\zeta_5}^4 + {\zeta_5}^3 + {\zeta_5}^2 + \zeta_5 + 1 \\ &= 0. \end{aligned}$$

Thus, $m_{\theta,\mathbb{Q}}$ satisfies θ. This implies that the minimal polynomial of θ divides $m_{\theta,\mathbb{Q}}$. Therefore, to show that the minimal polynomial of θ is in fact $m_{\theta,\mathbb{Q}}$ we must show that $m_{\theta,\mathbb{Q}}$ is irreducible.

To see that $m_{\theta,\mathbb{Q}}$ is irreducible we employ Eisetnstein's criterion. Consider the shifted polynomial

$$m_{\theta,\mathbb{Q}}(X + 2) = (X + 2)^2 + (X + 2) - 1 = X^2 + 4X + 4 + X + 2 - 1 = X^2 + 5X + 5.$$

By Eisenstein's criterion, $5 \mid 5$ and $5 \mid 5X$, but $5^2 \nmid 5$. Thus, $m_{\theta,\mathbb{Q}}(X + 2)$ is irreducible so $m_{\theta,\mathbb{Q}}(X)$ is irreducible. Therefore, the minimal polynomial of θ is $m_{\theta,\mathbb{Q}}$.

Now, since $\mathbb{Q}$ is characteristic 0, $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/(5))^\times \cong Z_4$. Since Z_4 has a unique subgroup of order 2, by he fundamental theorem of Galois theory, $\mathbb{Q}(\theta)$ is the only extension of degree 2 under $\mathbb{Q}(\zeta_5)$. Similarly, $\mathbb{Q}$ is the only other proper subfield since the only other subgroup of Z_4 is the trivial subgroup. ■

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. This is false. Consider the polynomial $f(X) = X^3 - 2$. The splitting field of this polynomial is $\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$. However, by the primitive element theorem, there exists $\alpha \in \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ such that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\alpha)$ and the $\deg(m_{\alpha,\mathbb{Q}}) = \big[\mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big) : \mathbb{Q}\big] = 6$. ■

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

Proof. The adjective *algebraic* is redundant in the above for every finite extension is necessarily algebraic.

Let F be a finite extension of $\mathbb{F}_{p^n}$. Then F must be a finite field of characteristic p since $\mathbb{F}_p \subset \mathbb{F}_{p^n} \subset F$. By the uniqueness theorem for finite fields, $F \cong \mathbb{F}_{p^m}$ for some positive integer m. Hence, $\mathbb{F}_{p^m}/\mathbb{F}_p$ is Galois, being the splitting field of the separable polynomial $X^{p^m} - X$.

By the fundamental theorem of Galois theory, since F is Galois over $\mathbb{F}_p$, F is Galois over any subfield containing $\mathbb{F}_p$. Thus, $F/\mathbb{F}_p$ is Galois. ■

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. Yes. Put $n \coloneqq [K : \mathbb{F}_p]$, $m \coloneqq [L : \mathbb{F}_p]$, and suppose $n \mid m$. By the fundamental theorem for finite fields, $K \cong \mathbb{F}_{p^n}$ and $L \cong \mathbb{F}_{p^m}$. Now, $\mathrm{Gal}(L/\mathbb{F}_p) \cong Z_m$ (generated by the Frobenius automorphism). Since $n \mid m$, Z_m has a subgroup of order $Z_{m/n}$. Thus, by the fundamental theorem of Galois theory, L has a subfield E such that

$$[E : \mathbb{F}_p] = \big[Z_m : Z_{m/n}\big] = m/(m/n) = n.$$

Thus, by the fundamental theorem for finite fields, $E \cong \mathbb{F}_{p^n} \cong K$. ■

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 ζ_n be a primitive nth 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. By the fundamental theorem of finitely fields, $G \coloneqq \mathrm{Gal}(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p) = \langle \sigma \rangle$ where σ is the Frobenius automorphism. Since $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = a$, the order of σ is a. Since ζ_n generates $\mathbb{F}_p(\zeta_n)$, by the fundamental theorem of Galois theory, the identity automorphism is the only automorphism in G which fixes ζ_n: If b is a positive integer with $b < a$, then ${\zeta_n}^{p^b} = \sigma^b(\zeta_n) \neq \zeta_n$. Hence, $p^b \not\equiv 1 \pmod{n}$.

Since $\sigma_a = \mathrm{id}_{\mathbb{F}_p(\zeta_n)}$, we have that $\sigma_a(\zeta_n) = \zeta_n$. But $\sigma_a(\zeta_n) = {\zeta_n}^{p^a}$. Hence ${\zeta_n}^{p^n} = \zeta_n$. Since the nth roots of unity form a cyclic multiplicative group generated by ζ_n of order n, it follows from ${\zeta_n}^{p^a} = \zeta_n$ that $p^a \equiv 1 \pmod{n}$. ■

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. Show that $a \mapsto a + 1$ defines an automorphism of $\mathbb{F}_p(f)$. Show that $\mathrm{Gal}(\mathbb{F}_p(f)/\mathbb{F}_p) \cong \mathbb{Z}_p$. Prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$. $\mathbb{F}_p(f)/\mathbb{F}_p$ is called an Artin–Schreier Extension.

Proof. Since $\mathbb{F}_p$ is of characteristic p, the *freshman's dream holds*, i.e.,

$$(a+1)^p - (a+1) - 1 = a^p + 1^p - a - 1 - 1 = a^p - a - 1 = 0.$$

Thus, $a+1$ is a root of f. Note that if $a \in \mathbb{F}_p$, then 0 is a root of f since $a+1, a+2, \cdots a+(p-a) = 0$ would be the roots of this polynomial. But $f(0) = 0^p - 0 - 1 = -1 \neq 0$. Thus, $a \notin \mathbb{F}_p$.

Now, we note that $\mathbb{F}_p(a) = \mathbb{F}_p(a+1)$: $1, a \in \mathbb{F}_p(a)$ so $a+1 \in \mathbb{F}_p(a)$ and $a, -1 \in \mathbb{F}_p(a+1)$ so $(a+1) - 1 = a \in \mathbb{F}_p(a+1)$. Thus,

$$\mathbb{F}(a) = \mathbb{F}(a+1) = \mathbb{F}(a+2) = \cdots = \mathbb{F}(a+p-1).$$

Since all of $a, a+1, ..., a+p-1$ are roots of f, and all of these fields are equal, $\mathbb{F}_p(a) = \mathbb{F}_p(f)$, i.e., $\mathbb{F}_p(a)$ is the splitting field of f. Hence, any map $a \mapsto a+i$, for $0 \leq i \leq p-1$, determines an automorphism of $\mathbb{F}_p(f)$. Note that $a \mapsto a+i$ is just $i-1$ applications of the map $a \mapsto a+1$. hence, $\mathrm{Gal}(\mathbb{F}_p(f)/\mathbb{F}_p)$ is cyclic generated by $a \mapsto a+1$. Moreover, this is a group of order p since $a+p = a$ but $a+i \neq a$ for all $1 \leq i \leq p-1$. Thus, $\mathrm{Gal}(\mathbb{F}_p(f)/\mathbb{F}_p) \cong Z_p$.

Since f is a monic polynomial of degree $p = [\mathbb{F}_p(a) : \mathbb{F}_p]$, with a as root, it follows that $f(X) = m_{\alpha, \mathbb{F}_p}(X)$. Hence, f is irreducible in $\mathbb{F}_p[X]$.

Since $\mathbb{Z}$ is an integral domain, f is a nonconstant monic polynomial in $\mathbb{Z}[X]$ and (p) is a proper ideol of $\mathbb{Z}$, and $\bar{f} = f$ is irreducible in $\mathbb{F}_p[X] \cong (\mathbb{Z}/(p))[X]$, if f is irreducible in $\mathbb{Z}[X]$. ■

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. This is from Dummit and Foote:

Consider the polynomial $f(T) = T^2 - X^2 \in \mathbb{F}_2(X^2, Y^2)[T]$. The roots of this polynomial are X, $-X$, neither of which are contained in $\mathbb{F}_2(X^2, Y^2)$. Thus, $T^2 - X^2$ is irreducible in $\mathbb{F}_2(X^2, Y^2)[T]$. Thus, $\left[\mathbb{F}_2(X, Y) : \mathbb{F}_2(X^2, Y^2)\right] = 2$. Similarly, $T^2 - Y^2$ is irreducible over $\mathbb{F}_2(X, Y^2)[T]$, so by the tower theorem, we have

$$\left[\mathbb{F}_2(X, Y) : \mathbb{F}_2(X^2, Y^2)\right] = \left[\mathbb{F}_2(X, Y) : \mathbb{F}_2(X, Y^2)\right]\left[\mathbb{F}_2(X, Y^2) : \mathbb{F}_2(X^2, Y^2)\right] = 2 \cdot 2 = 4.$$

for $c \in \mathbb{F}_2(X^2, Y^2)$, consider the subfield $\mathbb{F}_2(X + cY)$. Since $(X + cY)^2 = X^2 + c^2Y^2$ (by the freshman's dream), we have

$$\mathbb{F}_2(X^2, Y^2) \subset \mathbb{F}_2(X + cY), \qquad \text{and} \qquad \mathbb{F}_2(X + cY) \subset \mathbb{F}_2(X, Y).$$

Now, $T^2 - X^2 - c^2 - Y^2$ has $X + CY$ as a root, so

$$\left[\mathbb{F}_2(X + cY) : \mathbb{F}_2(X^2, Y^2)\right] \leq 2.$$

Bit if there were only finitely many subfields, then for some $c \neq c' \in \mathbb{F}_2(X^2, Y^2)$, $\mathbb{F}_2(X + cY) = \mathbb{F}_2(X + c'Y)$, so $x + cy, x + c'y \in \mathbb{F}_2(X^2, Y^2)$. Thus, $(X + cY) - (X + c'Y) = (c - c')Y \in \mathbb{F}_2(X + cY)$ so $Y \in \mathbb{F}_2(X + cY)$. Thus, $X \in \mathbb{F}_2(X + cY)$. Thus,

$$\mathbb{F}_2(X + cY) \subset \mathbb{F}_2(X, Y) \subset \mathbb{F}_2(X + cY),$$

so $\mathbb{F}_2(X, Y) = \mathbb{F}_2(X + cY)$. But this is absurd since

$$\left[\mathbb{F}_2(X, Y) : \mathbb{F}_2(X^2, Y^2)\right] = 4 \neq 2 = \left[\mathbb{F}_2(X + cY) : \mathbb{F}_2(X^2, Y^2)\right],$$

so $\mathbb{F}_2(X, Y) = \mathbb{F}_2(X + cY)$. This is a contradiction. Thus, there are infinitely many intermediate subfields. ■

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 $\mathrm{Gal}(F/\mathbb{Q})$ 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 aan odd prime.

(a) Show that hhere exits a unique queadratic 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 he 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 MA 553: Midterm, Fall 2015

Problem 2.1. (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 $D_{2n} \cong Z_2 \bowtie Z_n$.

Proof. (a) Suppose G is Abelian and define the map $\varphi \colon G \to G$ via the rule $\varphi(x) := x^{-1}$. We show that φ is an automorphism.

First, let us check that φ is in fact a homomorphism. Take $g, h \in G$, then

$$\begin{aligned}\varphi(gh) &= (gh)^{-1} \\ &= h^{-1}g^{-1}\end{aligned}$$

but since G is Abelian, the latter is just

$$\begin{aligned}&= g^{-1}h^{-1} \\ &= \varphi(g)\varphi(h).\end{aligned}$$

Thus, φ is a homomorphism.

It is easy to see that φ is surjective: Take any $g \in G$ then $\varphi(g^{-1}) = (g^{-1})^{-1} = g$. To see that φ is injective we show that its kernel is the identity subgroup: Let $g \in \ker\varphi$ then $\varphi(g) = g^{-1} = e$ implies that $e = gg^{-1} = ge = g$. Thus, $\ker\varphi = \{e\}$ and φ is injective. Thus, φ is an automorphism of G.

(b) First, note that the subgroups generated by s and r are cyclic and hence isomorphic to Z_2 and Z_n, respectively. Moreover, since $[D_{2n} : \langle r\rangle] = 2$ is the smallest prime dividing the order of D_{2n}, $\langle s\rangle \lhd D_{2n}$. Lastly, note that $\langle s\rangle \cap \langle r\rangle = \{e\}$. By part (a), the map given by $s \mapsto srs^{-1} = r^{-1}$ gives homomorphism $\varphi \colon Z_2 \to \mathrm{Aut}(Z_n)$. Thus, $D_{2n} = \langle s\rangle\langle r\rangle \cong Z_2 \rtimes Z_n$. ■

Problem 2.2. 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}. 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 2.3. 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 2.4. Let R and S be rings and suppose that $\varphi\colon R \to S$ is a ring homomorphism. Let I be an ideal of R and J and 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 φ is surjective, then $\varphi(I) := \{\, \varphi(r) \mid r \in I \,\}$ is an ideal in S.

(c) Given an example where φ 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 φ 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 $\varphi(b_2) = b_2$ 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 $\varphi\colon Z_4 \to Z_2 \times Z_2$ 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

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

But note that φ 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 2.5. (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 $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $R/\mathfrak{p}$ is an integral domain. Now, let $r \in R \setminus \mathfrak{p}$ and $\pi\colon R \to R/\mathfrak{p}$ 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 $p_1, ..., p_n$ 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 $\mathfrak{p} = (p)$. ∎

3 MA 553: Final, Fall 2015

Problem 3.1. 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 $Z(G) \lhd G$, 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 3.2. Let

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

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

(b) Show $N := \{ \left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right] \mid b \in \mathbb{Z}/(5) \}$ is a Sylow 5-subgroup of G.

Suppose a, b, c have been chosen. Then $d \equiv (ab-1)d^{-1} \pmod 5$. Then, there are $5^2 + 4 = 28$ possible choices for these and 4 possible ways to choose fix one of a, b, c, d. Thus, there are at least $4 \cdot 28 = 2^2 \cdot 3 \cdot 7$.

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

Proof. (a) We know the since of $\mathrm{GL}_2(\mathbb{Z}/(5))$. This is $(5^2-1)(5^2-5) = 24 \cdot 20 = 2^5 \cdot 3 \cdot 5$.

(b) It suffices to show that the order of N is 5 since 1 is the largest exponent of 5 dividing $120 = 2^3 \cdot 3 \cdot 5$. But this is clear, since N must satisfy $1 - b \cdot 0 \equiv 1 \equiv 1 \pmod 5$ which is true for any $b \in \mathbb{Z}$. Hence, there are 5 elements in N. Thus, N is a Sylow 5-subgroup.

(c) By Sylow's theorem, there are $n_5 = 1$ or 6. We will show that N is not normal in $\mathrm{SL}_2(\mathbb{Z}/(5))$ so that $n_5 \neq 1$. Let $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}/(5))$. 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 $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. Thus, $N \ntriangleleft \mathrm{SL}_2(\mathbb{Z}/(5))$ so $n_5 = 6$. ∎

Problem 3.3. 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. ∎

Problem 3.4. 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. ■

Problem 3.5. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$, and let $f(X) \in \mathbb{Q}[x]$ be its minimal polynomial. Let $\sqrt{\alpha}$ be a square root of α, and let $g(X) \in \mathbb{Q}[X]$ be its minimal polynomial.

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

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

Proof. ■

Problem 3.6. Let $f(X) = X^6 + 3 \in \mathbb{Q}[X]$.

(a) Let α 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 $\mathbb{Q}$.

Proof. (a) Put $\zeta_6 \coloneqq (\alpha^3 + 1)/2$.

(b) ■

Problem 3.7. Let $R \coloneqq (\mathbb{Z}/(3))[X]$. Consider the ideals $I_1 \coloneqq (X^2 + 1)$, and $I_2 \coloneqq (X^2 + X + 2)$. 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. ■

Problem 3.8. Suppose F is a field, $K = F(\alpha)$ is a Galois extension, with cyclic Galois group generated by $\sigma(\alpha) \coloneqq \alpha + 1$. Show that $\mathrm{ch}(K) = p \neq 0$, and $\alpha^p - \alpha \in F$.

Proof. ■

4 Qualifying Exam, January 2000

Problem 4.1. Find all groups of order $7 \cdot 11^3$ which have a cyclic subgroup of order 11^3.

Proof. ■

Problem 4.2. 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. ■

Problem 4.3. 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

$$\varphi\colon \operatorname{Gal}(EL/L) \hookrightarrow \operatorname{Gal}(E/F).$$

Find the fixed field of the image of φ.

(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. ■

Problem 4.4. 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 $|H_A| \mid p^k$.

Proof. ■

Problem 4.5. Let $R = \mathbb{Z} + X\mathbb{Q}[X] \subset \mathbb{Q}[X]$ 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 $(X) \coloneqq Rx$ 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. ■

5 Qualifying Exam, January 2011

Problem 5.1. Let

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

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

(b) Show

$$N \coloneqq \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \,\middle|\, b \in \mathbb{Z}/(5) \right\}$$

is a Sylow 5-subgroup of G.

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

Proof. ∎

Problem 5.2. (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

$$G_0 \coloneqq G \supset G_1 \supset G_2 \supset \cdots \supset G_n \coloneqq H,$$

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

(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 $G_0 \coloneqq G \supset G_1 \supset \cdots \supset G_n \coloneqq H$, with $[G_i : G_{i+1}] = 2$, for all i.

Proof. ∎

Problem 5.3. 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 $\sqrt{I} \coloneqq \{ r \in R \mid r^n \in R \text{ for some } n > 0 \}$.

(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 intstance.

Proof. ∎

Problem 5.4. Let S be the subring of $\mathbb{C}[X] \times \mathbb{C}[Y]$ consisting of pairs (f, g) with $f(0) = g(0)$.

(a) Let $\varphi \colon \mathbb{C}[X, Y] \to S$ be defined by $\varphi(h) = (f, g)$, where $f(X) = h(x, 0)$, and $g(Y) = g(0, Y)$. Prove φ is a surjective homomorphism.

(b) Prove $\mathbb{C}[X, Y]/(X, Y) \cong S$.

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

Proof. ■

Problem 5.5. Let p be a prime, let $F = \mathbb{F}_p$ be the field of p elements and $K = \mathbb{F}_{p^{10}}$ 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 5.6. Let $f(X) = (X^2 - 3)(X^3 - 7) \in \mathbb{Q}[X]$. Let K be the splitting field of $f(X)$ over $\mathbb{Q}$.

(a) Find the degree of K over $\mathbb{Q}$.

(b) Classify the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

(c) Find all subfields E of K so that $E/\mathbb{Q}$ is a quadratic extension.

Proof. ■