MA553 Past Qualifying Examinations

Carlos Salinas

December 29, 2015

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 dihedral group on n vertices, D_{2n}, imbeds into S_n, i.e., there exists an injective homomorphism $\varphi\colon D_{2n} \hookrightarrow S_n$.*

Proof of lemma. The group D_{2n} acts transitively on the set $S \coloneqq \{1, ..., n\}$ via the action $\cdot\colon D_{2n} \times S \to S$

$$x \cdot k \coloneqq \begin{cases} k + m & \text{if } x = r^m \\ n - k & \text{if } x = s. \end{cases}$$

♣

■

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. ■

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. ■

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. ■

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. ■

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

Proof. ■

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. ■

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. ■

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. ■

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

Proof. ■

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

Proof. ■

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.

Proof. ■

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

Proof. ■

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

Proof. ■

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

Proof. ■

1.2 Rings

Problem 1.16. Let R be a commutative ring with $1 \neq 0$ and let P be a prime ideal of R. Let I and J be ideals of R such that $I \cap J \subseteq P$, prove that either $I \subseteq P$ or $J \subseteq P$

Proof. ∎

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

Proof. ∎

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. ∎

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. ∎

Problem 1.20. Let R be an integral domain and F be its field of fractions. Let P be a prime ideal in R and $R_p = \left\{ \frac{a}{b} \;\middle|\; a, b \in R,\, b \notin P \right\} \subseteq F$. Show that R_P has a unique maximal ideal.

Proof. ∎

Problem 1.21. Let m and n be relatively prime integers. Show that there is an isomorphism $\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$.

Proof. ∎

Problem 1.22. Show that if x is non-nilpotent in R then a maximal ideal P of R, which does not contain x^n for $n = 1, 2, ...$, is prime.

Proof. ∎

Problem 1.23. Let $\mathbb{Q}$ be the field of rational numbers and $D = \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q} \right\}$.

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

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

Proof. ∎

Problem 1.24. Show that if p is a prime such that $p \equiv 1 \mod 4$, 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 $p \equiv 3 \mod 4$, 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

2 Field Theory

Problem 2.1. 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. ■

Problem 2.2. 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. ■

Problem 2.3. 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 2.4. Prove or disprove that every finite algebraic extension field of $\mathbb{F}_{p^n}$ is Galois.

Proof. ■

Problem 2.5. If $[K : \mathbb{F}_p]$ divides $[L : \mathbb{F}_p]$, does it follow that K is isomorphic to a subfield of L.

Proof. ■

Problem 2.6. 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 n-th root of unity. Show that $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = a$ is the least positive integer such that $p^a \equiv 1 \mod n$. [*Hint:* the Galois group of the extension of $\mathbb{F}_p$ is generated by the Frobenius automorphism.]

Proof. ■

Problem 2.7. 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 $\mathrm{Gal}(\mathbb{F}_p(f)/\mathbb{F}_p) \cong \mathbb{Z}_p$.

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 2.8. 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 2.9. 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 2.10. 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 2.11. Give an example where K/F and L/K are p-extensions, but L/F is not Galois.

Proof. ■

Problem 2.12. 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 $\mathbb{Q}$.

Subfield lattice. Alright. Let's crank it out! Let $f(x) = x^6 - 2$. The splitting field of this polynomial is just $L = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$ with index $[L : \mathbb{Q}] = 6 \cdot \varphi(6) = 6 \cdot 2 = 12$. First, we'll calculate the Galois group of this extension. To that end, it suffices to look at the automorphisms on the generators of L.

Clearly

$$\mathrm{Gal}(L/\mathbb{Q}) = \left\langle \sigma, \tau \;\middle|\; \sigma^6 = \tau^2 = 1,\, \tau\sigma = \sigma^5\tau \right\rangle,$$

where

$$\sigma\colon \begin{cases} \sqrt[6]{2} & \longmapsto \zeta_6 \sqrt[6]{2}, \\ \zeta_6 & \longmapsto \zeta_6, \end{cases}, \qquad \tau\colon \begin{cases} \sqrt[6]{2} & \longmapsto \sqrt[6]{2}, \\ \zeta_6 & \longmapsto \zeta_6^5. \end{cases}$$

Clearly $\sigma^6 = \tau^2 = 1$. What is less trivial is showing $\sigma\tau = \tau\sigma^5$. Observe

$$\sigma^5\colon \begin{cases} \sqrt[6]{2} & \longmapsto \zeta_6^5 \sqrt[6]{2}, \\ \zeta_6 & \longmapsto \zeta_6, \end{cases},$$

$$\sigma\tau\colon \begin{cases} \sqrt[6]{2} & \longmapsto \zeta_6 \sqrt[6]{2}, \\ \zeta_6 & \longmapsto \zeta_6^5, \end{cases}, \qquad \tau\sigma^5\colon \begin{cases} \sqrt[6]{2} & \longmapsto (\zeta_6^5)^5 \sqrt[6]{2} = \zeta_6 \sqrt[6]{2}, \\ \zeta_6 & \longmapsto \zeta_6^5. \end{cases}$$

Thus $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$. From here, we simply use the Fundamental Theorem of Galois Theory and observe the correspondence between subfields of L and subgroups of D_{12}. (If only I knew the subgroup lattice of D_{12}). ■

(b) Give generators for each subfield K of L for which $[K:\mathbb{Q}] = 2$. How many are there?

Solution. There is at least one and it corresponds to the subgroup $\langle\sigma\rangle \leq D_{12}$ whose index $[D_{12} : \langle\sigma\rangle] = 2$. Therefore, the only subfield is $K = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$ (a degree 2 extension over $\mathbb{Q}$).at ■

(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 $[L:K] = 2$?

Solution. This is also has at least one such subfield corresponding to the subgroup $\langle\tau\rangle \leq D_{12}$. The field is $\mathbb{Q}(\sqrt[6]{2})$. The extension to L is certainly degree 2. ■

Problem 2.13. 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 2.14. Let f be an irreducible polynomial of degree k over $\mathbb{F}_p$. Find the splitting field of f and its Galois group.

Proof. Without loss of generality, assume $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$. Since f is irreducible over $\mathbb{F}_p$, then ■

Problem 2.15. 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. Assume otherwise. Then F_1 and F_2 both have index d over $\mathbb{Q}$. ■

Problem 2.16. 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 2.17. 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 2.18. 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 2.19. Show that $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, where $\zeta_3^2 + \zeta_3 + 1 = 0$.

Proof. ■

Problem 2.20. 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 2.21. 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 2.22. 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 2.23. 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. ■

3 January 2007

Problem 3.1. Let $(G, \cdot)$ be a group. Show that G is Abelian whenever $\mathrm{Aut}(G)$ is a cyclic group under composition.

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

Lemma 2. *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 3.2. Let $(G, \cdot)$ be an Abelian group. The *torsion subgroup of* G is defined as the collection of elements of finite order:

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

(a) Show that the quotient group $G/\mathrm{Tor}(G)$ is *torsion free*, i.e., it contains no nontrivial elements of finite order.
(b) Show that $\mathrm{Tor}(G)$ 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 $T \coloneqq \mathrm{Tor}(G/\mathrm{Tor}(G))$. 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 $\bar{g} \in G/\mathrm{Tor}(G)$ and $\bar{g}^m = \bar{e}$ for some positive integer m. But $\bar{g}^m = \bar{e}$ implies that $g^m \,\mathrm{Tor}(G) = \mathrm{Tor}(G)$, i.e., $g^m \in \mathrm{Tor}(G)$. Thus, $(g^m)^n = g^{mn} e$ for some positive integer n. Thus, $g \in \mathrm{Tor}(G)$ so we must have $\bar{g} = \bar{e}$.

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

Problem 3.3. Let $(G, \cdot)$ be a group of order $|G| = 351$. Show that G is solvable.

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

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

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

Problem 3.4. Let $(G, \cdot)$ be a group, and $H < G$ a subgroup of finite index. Show that there exists a normal subgroup $N \lhd G$ contained in H which is also of finite index. (Do not assume that G is finite.)

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

Problem 3.5. Let $(G, \cdot)$ be a finite group, and $\varphi\colon G \to G$ be a group homomorphism. Show that for all normal Sylow p-subgroups $P \lhd G$ we have $\varphi(P) < P$.

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

Problem 3.6. Let $(R, +, \cdot)$ be a commutative ring with $1 \neq 0$.

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

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

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

(b) ∎

Problem 3.7. 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 3.8. 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 3.9. Let $(\mathbb{F}_p, +, \cdot)$ be a finite field whose Cardinality p is prime. Fix a positive integer n which is not divisible by p, and let ζ_n be a primitive nth root of unity. Show that $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = \alpha$ is the least positive integer such that $p^\alpha \equiv 1 \pmod{n}$.

Proof. ■

Problem 3.10. 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. ■

4 Spring 2008

Problem 4.1. Let $(G, \cdot)$ be a group, $(H, +)$ be an Abelian group, and $\varphi\colon G \to H$ be a group homomorphism. If N is a subgroup such that $\ker\varphi < N < G$, show that $N \lhd G$ is a normal subgroup.

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

Problem 4.2. Let $(G, \cdot)$ be a finite Abelian group of even order, i.e., $|G| = 2k$ for some $k \in \mathbb{N}$.

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

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

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

Problem 4.3. Let $(G, \cdot)$ be a finite group of odd order, and $H \lhd G$ be a normal subgroup of prime order $|H| = 17$. Show that $H < Z(G)$.

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

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

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

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

Problem 4.4. Let $(G, \cdot)$ be a finite group. Show that there exists a positive integer n such that G is isomorphic to a subgroup of A_n, the alternating group on n letters. [*Hint:* Show that A_n contains a copy of S_{n-1} when $n \geq 3$.]

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

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

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

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

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

Problem 4.5. 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 4.6. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be commutative rings with $1 \neq 0$, and let $\varphi \colon R \to S$ be a surjective ring homomorphism. Assuming that R is local, i.e., it has a unique maximal ideal, show that S is also local.

Proof. ■

Problem 4.7. 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 4.8. 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 4.9. 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 $\mathrm{Gal}(\mathbb{F}_p(f)/\mathbb{F}_p) \cong Z_p$.

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

Proof. ∎

Problem 4.10. Determine the Galois group of the splitting field over $\mathbb{Q}$ of $f(x) = x^4 + 4$.

Proof. ∎

5 August, 2015

Problem 5.1.

Proof. ∎

5.1 August 2010