18-703 Modern Algebra: Spring 2013 Final Exam Answers

Amanuel Tewodros Getachew

March 4, 2025

Problem 1

i. **Definition of a Group:** A group is a set G equipped with a binary operation $(\cdot) : G \times G \to G$ satisfying the following properties:

   a. *Associativity:* For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

   b. *Identity Element:* There exists an element $e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$.

   c. *Inverse Element:* For every $a \in G$, there exists an element $b \in G$, denoted a^{-1}, such that $a \cdot b = b \cdot a = e$.

ii. **Definition of an Automorphism:** An automorphism φ of a group G is a bijective homomorphism $\varphi : G \to G$, satisfying $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for all $a, b \in G$.

iii. **Definition of the Dihedral Group D_n:** D_n is the group of symmetries of a regular n-gon, including rotations and reflections. Formally,

$$D_n := \{r^i s^j : r^n = 1, s^2 = 1, sr = r^{-1}s\},$$

   where r represents rotation and s represents reflection.

iv. **Definition of an Ideal:** An ideal I is a subset of a ring R such that for all $r \in R$, $rI \subseteq I$ and $Ir \subseteq I$.

v. **Definition of a Principal Ideal Domain (PID):** A principal ideal domain is an integral domain R in which every ideal is generated by a single element. That is, for any ideal $I \triangleleft R$, there exists $a \in R$ such that

$$I = (a) = \{ra : r \in R\}.$$

vi. **Definition of a Unique Factorization Domain (UFD):** A unique factorization domain is an integral domain R in which every nonzero element $a \in R$ can be expressed uniquely (up to units) as a product of irreducibles. Formally, if $a = p_1 \cdots p_r = q_1 \cdots q_s$, where p_i, q_i are irreducibles, then $r = s$ and $p_i = u_i q_i$ for some unit $u_i \in R$.

Problem 2

i. **Equivalence Relation on a Group:** Let G be a group and define a relation $g_1 \sim g_2$ if there exists $h \in G$ such that $g_1 = hg_2h^{-1}$. Prove that $\sim$ is an equivalence relation:

   a. *Reflexive:* For any $a \in G$, $a = haa^{-1}$. Thus, $a \sim a$.

   b. *Symmetric:* If $g_1 \sim g_2$, then $g_1 = hg_2h^{-1}$. Multiplying by h^{-1} on both sides, $h^{-1}g_1h = g_2$. Thus, $g_2 \sim g_1$.

   c. *Transitive:* If $g_1 \sim g_2$ and $g_2 \sim g_3$, then $g_1 = h_1g_2h_1^{-1}$ and $g_2 = h_2g_3h_2^{-1}$. Substituting, $g_1 = h_1(h_2g_3h_2^{-1})h_1^{-1} = (h_1h_2)g_3(h_1h_2)^{-1}$. Thus, $g_1 \sim g_3$.

ii. **Equivalence Classes in S_5:** Let $\overline{\sigma}$ denote the equivalence class containing $\sigma \in S_5$. By the theorem on conjugacy in symmetric groups, two permutations $\sigma_1, \sigma_2 \in S_5$ are conjugate if and only if they have the same cycle type. Thus, the equivalence classes in S_5 are:

   (1) $\overline{1} = \{1\}$
   (2) $\overline{(1\,2)} = \{\sigma : \text{type}(\sigma) = (2,1,1,1)\}$
   (3) $\overline{(1\,2)(3\,4)} = \{\sigma : \text{type}(\sigma) = (2,2,1)\}$
   (4) $\overline{(1\,2\,3)} = \{\sigma : \text{type}(\sigma) = (3,1,1)\}$
   (5) $\overline{(1\,2\,3)(4\,5)} = \{\sigma : \text{type}(\sigma) = (3,2)\}$
   (6) $\overline{(1\,2\,3\,4)} = \{\sigma : \text{type}(\sigma) = (4,1)\}$
   (7) $\overline{(1\,2\,3\,4\,5)} = \{\sigma : \text{type}(\sigma) = (5)\}$

Problem 3

Classification of Groups of Order at Most 10:

Using the fundamental theorem of finite abelian groups:

- For $n < 10$ prime: G is cyclic, $G \cong \mathbb{Z}/n\mathbb{Z}$ for $n \in \{2, 3, 5, 7\}$.
- $n = 4$: If G is abelian, $G \cong \mathbb{Z}/4\mathbb{Z}$ or V_4 (Klein four-group).
- $n = 6$: If G is abelian, $G \cong \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. If G is non-abelian, $G \cong S_3$.
- $n = 8$: If G is abelian, $G \cong \mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- If $n = 9$ and G is abelian, $G \cong 9$ or $G \cong 3 \times 3$. If G is non-abelian, then G is not cyclic and there force contains 3 cyclic sub-groups. Since 3 is prime, two sub-groups have the trivial sub-groups as intersection. WLOG, let $\langle a\rangle, \langle b\rangle, \langle c\rangle, \langle d\rangle$ be the three subgroups of G. Then ab can not be $e, a^{\pm 1}, b^{\pm 1}$. WLOG, let $ab = c$. This implies $ab = c$, $ac = d$ and $ad = b$. If $ab = ba$, then $ac = a^2b = aba = ca$ and $ad = a^2ca = aca = da$, which implies $a \in Z(G)$ making G commutative. Thus $ba = d$. But then $ad = b = a^2d = a^2ba = aca = da$ and by similar argument as above, G becomes abelian. Thus there is no non-abelian group of order 9.

- Let $n = 8$. If G is abelian, then G is isomorphic to either 8, 4×2 or $2 \times 2 \times 2$. If G is non-abelian, by Lagrange's theorem, then there is at least on element a of order 4. If $\langle a\rangle$ is cycle of order 4, and if all elements $b \in G - \langle a\rangle$ have order 2, then $G \cong D_4$. Let G contain two elements a, b of order 4. If $a \cap b = \{1\}$, then $ab = ba$ is an element of order 2. But $e = abab = aabb = a^2b^2 \implies a^2 = b^2$. Thus $a \cap b = \{1, a^2\}$ since $a^{\pm 1}$ is a generator of a. We know $ab, ba \in G - a - b$. Since $a^2 = b^2$, $aabb = e$ or $ab = a^3b^3 = (ba)^{-1}$. Thus $G \cong Q_8$.

Problem 4

1. State the second isomorphism theorem.

   Let G be a group and $H \leq G$ and $K \trianglelefteq G$. Then,

   $$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

2. Prove the second isomorphism theorem.

   Define a mapping $\phi : H \to HK/K$, as

   $$\phi(h) = hK.$$

   Note that ϕ is surjective because if $a = hK \in HK/K$, then $\phi(h) = a$. If $a, b \in H$, then $\phi(ab) = abK = aK \cdot bK = \phi(a)\phi(b)$. Thus ϕ is a homomorphism. Now, $\ker \phi = \{h \in H : hK = K\} = \{h \in H : h \in K\} = H \cap K$. By the first Isomorphism theorem, the theorem follows.

Problem 5

1. State Sylows theorems.

   (a) *First Sylow Theorem*: Let n be the order of a group G and $n = p^a m$ where p does not divide m. Then there is a subgroup of G with order p^a known as a Sylow p-group.

(b) *Second Sylow Theorem*: If P and Q are two Sylow p-subgroups of G, then P and Q are conjugates of each other.

(c) *Third Sylow Theorem*: If n_p is the number of Sylow p-subgroups of G, then $n_p \equiv 1 \bmod p$.

2. Let G be a group of order pqr, where p, q and r are distinct primes. Show that G is not simple.

   WLOG, let $p < q < r$. By the third Sylow theorem, $n_r = 1 + kr$ for some $k > 0$ by assumption. Since $n_r > r, p, q$, $n_r | pqr$ and $n_r \nmid r$, $n_r = pq$. However, this means there are $pq(r-1)$ distinct elements in the Sylow $r-$group of G. Let $n_p = 1 + p$, and $n_q = 1 + q$, yielding $(p-1)(p+1) = p^2 - 1$ and $(q-1)(q+1) = (q^2 - 1)$ distinct elements (resp.) in the Sylow p-subgroups and Sylow q-subgroups (resp.). Thus we have

$$pqr \geq pqr - pq + p^2 + q^2 - 1.$$

   Clearly, $q^2 > pq - p^2 = p(q-p) + 2$, yielding a contradiction and thus one of n_p, n_q and n_r is 1.

Problem 6

1. If the prime ideal P contains the product IJ of two ideals then prove that P contains either I or J.

   If $J \subseteq P$, there is nothing to prove, so let $J \nsubseteq P$. There is an element $j \in J$ not in P. We know $\{ij : i \in I\} \subseteq IJ \subseteq P$. Since P is prime, this means $I \subseteq P$.

2. Exhibit a natural bijection between the prime ideals of R/IJ and $R/I \cap J$.

   Let S_G be the collection of prime ideals in the group G. I claim that the mapping $\pi : S_{R/IJ} \to S_{R/I \cap J}$ defined by

$$\pi(P/IJ) = P/I \cap J$$

   is a bijection. By (i), if $IJ \subseteq P \in S_R$, then $I \cap J \subseteq P$. Therefore, π is defined on the whole of $S_{R/IJ}$. It remains to prove if P is a prime ideal that contains $I \cap J$, then it should also contain IJ. This follows from noting that if $i \in I$ and $j \in J$, then $ij \in I \cap J$ and all finite sums of the form $\sum ij \in I \cap J$, implying $IJ \subseteq I \cap J$.

3. Give an example of a ring R, and ideals I and J such that IJ and $I \cap J$ are different.

   Consider the ideals $I = 2$ and $J = 4$ in the ring $R = \mathbb{Z}$. $IJ \subseteq 8 \subset 4 = I \cap J$.

Problem 7

Does every UFD R, which is not a field, contain infinitely many irreducible elements which are pairwise not associates? If your answer is yes then prove it and if no then give an example.

No. DVTs are UFDs with finitely many primes(irreducibles) but infinite elements.

Problem 8

Give an example of an integral domain such that every element of R can be factored into irreducibles and yet R is not a UFD.

$R = \mathbb{Z}[\sqrt{-5}]$ is an integral domain that is not a UFD. To show that 6 can be written as a product of different pairs of irreducibles, as $6 = 2 \cdot 3$ and $6 = (1+\sqrt{-5})(1-\sqrt{-5})$. We prove that $2, 3, 1 \pm \sqrt{-5}$ are irreducibles in R. To do that, we define a function(norm) $N : R \mapsto \mathbb{Z}$ as $N(a + b\sqrt{-5}) = a^2 + 5b^2$. It is clear that $N(zw) = N(z)N(w)$. $N(2) = 4 = 2 \cdot 2$. Since $N(a + b\sqrt{-5}) = a^2 + 5b^2 \neq 2$ for $a, b \in \mathbb{Z}$, 2 must be irreducible. Similarly, 3 and $1 \pm \sqrt{-5}$ are irreducible in R. Thus R is not a UFD.

Problem 9

1. Show that $\mathbb{Z}[i]$ is a Euclidean domain.

   Define an evaluation norm $v : \mathbb{Z}[i] \mapsto \mathbb{N} \cup \{0\}$ as $N(a + bi) = a^2 + b^2$. Clearly, $v(0) = 0$ and $v(zw) = zw\overline{zw} = z\overline{z}w\overline{w} = v(z)v(w)$. Now we prove that if $0 \neq z, w \in \mathbb{Z}[i]$, then $z = qw + r$ such that $v(w) > v(r) \geq 0$. Let $x + yi = z/w$ and let $p + si$ be an element of $\mathbb{Z}[i]$ such that $|x - p| \leq 1/2$ and $|y - s| \leq 1/2$. If $r = z - w(p + si)$, then

   $$\begin{aligned} v(r) &= v(z - w(p + qi)) \\ &= z - w(p + qi)\overline{(z - w(p + qi))} \\ &= w(z/w - (p + qi))\overline{w(z/w - (p + qi)} \\ &= w\overline{w}(z/w - (p + qi)\overline{(z/w - (p + qi)} \\ &\leq v(w)(1/4 + 1/4) \\ &< v(w). \end{aligned}$$

   This proves $\mathbb{Z}[i]$ is a Euclidean domain.

2. Is $6 - i$ prime in $\mathbb{Z}[i]$?

   Since $v(zw) = v(z)v(w)$, if $z \mid 6 - i$, $v(z) \mid v(6 - i) = 37$. But 37 is a prime number and it's only divisors are 1 and itself, making $6 - i$ irreducible. Since $\mathbb{Z}[i]$ is Euclidean domain, and therefore PID, $6 - i$ is then prime.

Problem 10

Write down all irreducible polynomials of degree 2 over the field $\mathbb{F}_5$.

Let $p(x) = ax^2 + bx + c, a \neq 0, b, c \in \mathbb{F}_5$. We consider two cases: *Case 1*: $b = 0$. Substituting, $x = \pm 1$ and $x = \pm 2$ in $p(x)$, we obtain $a \neq \pm c$. Hence, the polynomials $x^2 \pm 2$ and their associates are irreducible. *Case 2*: if $b \neq 0$, we obtain $a + b + c \neq 0, -b, \pm 2b$, leaving only $a + b + c = b \implies a = -c$. In this case, the polynomial we need to investigate has the form $ax^2 + bx - a = a(x^2 + a^{-1}bx - 1)$. This implies $p(x)$ is irreducible iff $x^2 + b'x - 1$ is irreducible for $b' \neq 0$. Considering the latter, case by case, we obtain $x^2 \pm 2x - 1$ is irreducible. Hence The irreducible polynomials (upto multiplication by units) over the field $\mathbb{F}_5$ are $\{x^2 \pm 2, x^2 \pm 2x - 1\}$

Problem 11

1. State Gauss' Lemma and Eisenstein's criteria.

   - *Gauss' Lemma*: Let D be an integral domain and let F be its field of fraction. If $p(x)$ is a monic polynomial in $D[x]$ and it can be factorized in to two polynomials $f(x), g(x)$ in $F[x]$ as $p(x) = f(x)g(x)$, then $f(x) = u(x)v(x)$ such that $u(x), v(x) \in D[x]$ and $\deg f(x) = \deg u(x)$ and $\deg g(x) = \deg v(x)$.
   - *Eisenstein's Criterion*: Let $p(x) = \sum_i a_i x^i \in \mathbb{Z}[x]$ and let p be a prime. If $p \mid a_i$ for $0 \leq i < n$, $p \nmid a_n$ and $p^2 \nmid a_0$, then $p(x)$ is irreducible in $\mathbb{Z}[x]$ and hence in $\mathbb{Q}[x]$.

2. Show that the polynomial $1 + x^3 + x^6 \in \mathbb{Q}[x]$ is irreducible (Hint: try a substitution.)

   Let $p(x) = 1 + x + x^2$. The given polynomial is irreducible iff $p(x)$ is irreducible in $\mathbb{Q}[x]$. But $p(x)$ is irreducible if $p(x+1) = x^2 + 3x + 3$ is irreducible which it is by Eisenstein's criterion stated in (i) by taking $p = 3$.

3. Show that the polynomial $1 - t^2 + t^5$ is irreducible over $\mathbb{Q}$ (Hint: consider the ring $\mathbb{F}_2[t]$.)

   First, we observe that if a monic polynomial is not irreducible in $\mathbb{Q}[x]$, then it is clearly not irreducible in $\mathbb{F}_p(x)$. To show that let $p(x)$ factorize into $p_1(x) \cdots p_n(x)$ in $\mathbb{Z}[x]$. Then $p(x) + p = \left(\prod_i p_i(x)\right) + p = \prod_i (p_i(x) + p) \in \mathbb{F}_p(x)$. Hence, by contra-positive, $p(x)$ is irreducible in $\mathbb{Q}[x]$ if it is irreducible in $\mathbb{F}_p[x]$. Taking the special case, $p = 2$, $f(x) = 1 - x^2 + x^5 \neq 0$ for $x \in \{\pm 1, 0\}$. Hence, $f(t)$ must be irreducible in $\mathbb{Q}[t]$.