Math 31
Final Examination

Elements of solution

Problem 1. Cauchy's Theorem for abelian groups and application

Let G be an abelian group with order $n \geq 2$.

a. Let g be an element of order m in G. Prove that for every positive divisor d of m, there exists an element of G with order d.

If $d|m$, then $\frac{m}{d}$ is an integer and $g^{\frac{m}{d}}$ has order d.

The purpose of this problem is to prove by induction on n that if p is a prime divisor of n, then G contains at least one element of order p.

b. Check that the result holds for $n \in \{2, 3, 4\}$.

By Lagrange's Theorem, the order of any element divides the order of the group so if n is prime like 2 and 3, then every element different from the identity has order n. If $n = 4$, then G is either cyclic, if which case the square of a generator has order 2, or isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, in which case every element has order 2.

Now we fix n and assume that the property is satisfied for every group of order $< n$.

c. Let $\gamma \in G \setminus \{e_G\}$ be an element of order relatively prime with p, a prime divisor of n. Prove that $G/\langle\gamma\rangle$ contains an element of order p.

Let N denote the order of γ. The subgroup generated by γ is automatically normal because G is abelian and the quotient $G/\langle\gamma\rangle$ has order $\frac{n}{N} < n$. Since $p|n$ and p is relatively prime with N, then p is a prime divisor of the order of $G/\langle\gamma\rangle$ which therefore contains an element of order p.

d. Deduce that G contains an element of order p.

If G contains an element γ as in the previous question, then there exists an element $g \in G$ such that $[g] = g\langle\gamma\rangle$ has order p in $G/\langle\gamma\rangle$. Since the natural surjection is a homomorphism, it follows that the order of g in G is a multiple of p. Then by question **a.** there exists an element of order p in G. If every element of G has order a multiple of p the last part of the argument applies directly.

From now on, let G be an abelian group of order 10.

e. Prove that G contains an element τ of order 2 and an element σ of order 5.

This is an immediate consequence of Cauchy's Theorem, which we just proved.

f. Construct an isomorphism between $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and G.

Observe that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is generated by $t = (1, 0)$ and $s = (0, 1)$. Since these two elements commute and have order 2 and 5 respectively, one can define $\varphi \in \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, G)$ by letting $\varphi(t) = \tau$ and $\varphi(s) = \sigma$. One checks that φ is an isomorphism and that

$$G = \{e_G, \tau, \sigma, \sigma^2, \sigma^3, \sigma^4, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4\}.$$

g. Is G cyclic? Yes, $G = \langle \tau\sigma \rangle$.

Problem 2. Field extensions

a. Find a monic irreducible polynomial P in $\mathbb{Q}[X]$ such that $\mathbb{Q}[1 + \sqrt{2}] \simeq \mathbb{Q}[X]/\langle P \rangle$.

Note that $\alpha = 1 + \sqrt{2} \notin \mathbb{Q}$ so no polynomial of degree 1 over $\mathbb{Q}$ has α as root. Observe that $\alpha^2 = 2\alpha + 1$ so that $X^2 - 2X - 1$ is the minimal polynomial of α over $\mathbb{Q}$.

b. Let $F = \mathbb{Z}/2\mathbb{Z}$. Prove that $F[X]/\left\langle X^3 + X + 1 \right\rangle$ is a field and construct its addition and multiplication tables.

To prove that the quotient is a field, it suffices to verify that $\left\langle X^3 + X + 1 \right\rangle$ is maximal, which is equivalent to $X^3 + X + 1$ being irreducible. If it was not, since it has degree 3, it would have a root in $\mathbb{Z}/2\mathbb{Z}$. Since $0^3 + 0 + 1$ and $1^3 + 1 + 1$ are both odd, we can conclude that $X^3 + X + 1$ is irreducible on $\mathbb{Z}/2\mathbb{Z}$.

Denote by c the class of X in $K = F[X]/\left\langle X^3 + X + 1 \right\rangle$. Then K consists of all the combinations of the form $\alpha c^2 + \beta c + \gamma$ with $\alpha, \beta, \gamma \in \mathbb{Z}/2\mathbb{Z}$. In other words, $K = \{0\,,\ 1\,,\ c\,,\ c + 1\,,\ c^2\,,\ c^2 + 1\,,\ c^2 + c\,,\ c^2 + c + 1\}$ with ordinary rules and the relation $c^3 = 1 - c$.

c. Let K be a subfield of a field F. Prove that the elements of F that are algebraic over K form a subfield of F.

All elements of K are trivially algebraic over K so the set is not empty.

Moreover, we know that an element $\alpha \in F$ is algebraic over K if and only if the subfield $K[\alpha]$ of F generated by K and α is a finite extension of K.

Let α and β be algebraic over K. Then $K[\alpha, \beta] = K[\alpha][\beta]$ is an extension of K of degree at most $[K[\alpha] : K] \cdot [K[\beta] : K]$. Since $\alpha - \beta$ and $\alpha\beta^{-1}$ (with $\beta \neq 0$) are elements of $K[\alpha, \beta]$, it follows that $K[\alpha + \beta]$ and $K[\alpha\beta^{-1}]$ are finite extensions, so $\alpha - \beta$ and $\alpha\beta^{-1}$ are algebraic, hence the result.

Problem 3. Isomorphism of two quotient rings

The goal of this problem is to determine whether the rings

$$A = \mathbb{R}[X]/\left\langle X^2 - 1\right\rangle \qquad \textbf{and} \qquad B = \mathbb{R}[X]/\left\langle X^2 - 2X + 1\right\rangle$$

are isomorphic or not.

a. Verify that the map

$$\begin{array}{rcl} \varphi : \mathbb{R}[X] & \longrightarrow & \mathbb{R}[X]/\left\langle X-1\right\rangle \times \mathbb{R}[X]/\left\langle X+1\right\rangle \\ P & \longmapsto & \left(P + \left\langle X-1\right\rangle, P + \left\langle X+1\right\rangle\right) \end{array}$$

is a ring homomorphism.

Notice that $\varphi(P) = (\pi(P), \pi'(P))$ where π and π' are the natural surjections from $\mathbb{R}[X]$ onto $\mathbb{R}[X]/\left\langle X-1\right\rangle$ and $\mathbb{R}[X]/\left\langle X+1\right\rangle$ respectively. Both maps are rings homomorphisms, therefore so is φ.

b. Prove that A is isomorphic to $\mathbb{R}[X]/\left\langle X-1\right\rangle \times \mathbb{R}[X]/\left\langle X+1\right\rangle$.

The Isomorphism Theorem implies that $A/\ker\varphi$ is isomorphic to the image of φ.
Observe that $\varphi(P) = 0$ if and only if

$$\pi(P) = 0_{\mathbb{R}[X]/\langle X-1\rangle} \qquad \text{and} \qquad \pi'(P) = 0_{\mathbb{R}[X]/\langle X+1\rangle},$$

that is $P \in \langle X-1\rangle \cap \langle X+1\rangle$. Since $X-1$ and $X+1$ are relatively prime, this is equivalent to $P \in \langle (X+1)(X-1)\rangle = \left\langle X^2-1\right\rangle$. In other words, $\boxed{\ker\varphi = \left\langle X^2-1\right\rangle.}$

To verify that φ is surjective, note that every element in $\mathbb{R}[X]/\left\langle X-1\right\rangle$ or $\mathbb{R}[X]/\left\langle X+1\right\rangle$ has a representative of degree 0, that is, a constant. For (a,b) in $\mathbb{R}\times\mathbb{R}$, one can consider the polynomial $P_{a,b} = \frac{a}{2}(X+1) - \frac{b}{2}(X-1)$ and verify that $\varphi(P_{a,b}) = (a,b)$.

c. Prove that B contains an element $b \neq 0$ such that $b^2 = 0$.

Observe that $B = \mathbb{R}[X]/\left\langle (X-1)^2\right\rangle$ and consider the class of $X-1$ in B. It is not zero because it is not a multiple of $(X-1)^2$ but its square is.

d. Are A and B fields? Are they isomorphic rings?

Both rings are quotients by non-prime ideals so they are not even integral domains.

If there was a ring isomorphism u between B and A, then $u(b)$ would be a non-zero element of A with square 0. We prove that A contains no such element. If there was, any of its representatives P in $\mathbb{R}[X]$ would be such that

$$(X-1)(X+1) \nmid P \qquad \text{and} \qquad (X-1)(X+1) \mid P^2.$$

In particular, either $X-1$ or $X+1$ does not divide P. Without loss of generality, assume that it is $X-1$. Since $X-1$ divides P^2 and is irreducible, Euclid's Lemma implies that $X-1$ divides one of the prime factors of P^2. However, these factors are the same as those of P so $X-1$ divides P, which is a contradiction.

It follows that $\boxed{A \text{ and } B \text{ are not isomorphic}}$.

Problem 4. Is $\mathbb{Z}[X]$ a Euclidean ring?

a. Describe the smallest ideal I of $\mathbb{Z}[X]$ that contains 2 and X.

Any such ideal must contain all the multiples of 2 as well as all the multiples of X and all the combinations of such elements. In other words, I necessarily contains the polynomials of the form $m + XQ$ with m even and $Q \in \mathbb{Z}[X]$. Conversely, one checks that this set is an ideal in $\mathbb{Z}[X]$ so $I = \{P \in \mathbb{Z}[X]\ ,\ 2|P(0)\}$.

b. Is I principal?

Assume that $I = \langle P \rangle$ with $P \in \mathbb{Z}[X]$. Then $P|2$ so P must be constant and a divisor of 2. It cannot be ± 1 because I is a strict ideal, so $P = \pm 2$, which is impossible since X is not a multiple of 2 in $\mathbb{Z}[X]$. Therefore, I is not a principal ideal.

c. Does the Euclidean Division Theorem apply in $\mathbb{Z}[X]$?

No: in a ring where the theorem applies, every ideal is principal.

Problem 5. Final question

Read up on Evariste Galois and Niels Abel. Suggest actors to play their role in Hollywood biopics (not just based on their looks).

Many names have been suggested, with various (almost always pertinent) rationales.

For Evariste Galois:

- Jim Parsons $\times 2$
- Matt Damon
- Jessie Eisenberg
- Shia Labeouf
- Liam Hemsworth
- Paul Dano
- Gaspard Ulliel
- Heath Ledger
- Jared Leto
- Kit Harrington
- Andrew Garfield
- Edward Norton
- Robert Downey Jr
- John Franklin
- Vincent Lacoste
- Skandar Keynes
- Russel Crowe
- Jean-Michel Basquiat
- Zac Efron
- Jeremy Kapone
- Freddie Highmore
- Jamie Bell

For Niels Abel:

- Eddie Redmayne $\times 2$
- Matt Damon $\times 2$
- Russel Crowe
- (Young) Russel Crowe
- Jessie Eisenberg
- Shia Labeouf
- Chris Hemsworth
- Matthew Gubler
- Freddie Highmore
- Owen Wilson
- (Young) Morgan Freeman
- Tobey Maguire
- Joseph Gordon-Levitt
- Daniel Radcliffe
- Will Smith
- Robert Pattinson
- Ewan McGregor
- Jakob Oftebro
- Jack Gleeson