University of Wisconsin-Milwaukee

Modern Algebra

Math 531

Exam 2

Author
Theodore Koss

Supervisor
Dr. Burns Healy

January 19, 2024

1 Problem 1

Let n be an integer greater than 1. For the symmetric group on n letters, find a normal subgroup. Describe the quotient of S_n by this normal subgroup.

Proof. For all groups S_n where $n > 1 \in \mathbb{Z}$, the alternating group, $A_n = \{\sigma \in S_n | \sigma \text{ is even}\}$. This is a subgroup by the (aptly named) Subgroup Test

Theorem 1 (Subgroup Test)**.** *Let G be a group and let H be a nonempty subset of G. If for all $a, b \in H$, $ab^{-1} \in H$, then $H \leqslant G$.*

Proof of 1 here
Suppose $\mu, \sigma \in A_n$, then $\mu = \tau_1 \dots \tau_{2k}$ and $\sigma = \tau'_1 \dots \tau'_{2m}$. $\sigma^{-1} = \tau'_{2m} \dots \tau'_1$. Then $\mu\sigma^{-1} = \underbrace{\tau_1 \dots \tau_{2k}\tau'_{2m} \dots \tau'_1}_{2(k+m) \text{ transpositions}}$. And since $2(k+m)$ is even, $\mu\sigma^{-1} \in A_n$ and thus A_n is a subgroup.
$|A_n| = \frac{n!}{2}$ by This result in math. Thus, since $|S_n| = n!$, $S_n - A_n = \{\sigma \in S_n | \sigma \text{ is odd}\}$, these two sets, A_n and $S_n - A_n$ describe the quotient of S_n.
QED

2 Problem 2

Let $G = Z \oplus Z$ be the group determined by pairs of integers, where addition is defined by adding each component. Find three (proper, not the whole group) subgroups of G none of which are isomorphic to each other. Prove that one of these subgroups is isomorphic to G itself, and is normal. Describe the quotient group of G by this last group.

Proof. 3 Subgroups:

(1) $H = \{(x, 0) | x \in G\}$. By the subgroup test, if $\forall a, b \in H, \quad ab^{-1} \in H$ then it is a subgroup. $ab^{-1} = (a - b, 0)$, and since $a - b \in G$ this is a subgroup.

(2) $H' = \{(0, y) | y \in G\}$. By the subgroup test, if $\forall a, b \in H, \quad ab^{-1} \in H$ then it is a subgroup. $ab^{-1} = (0, a - b)$, and since $a - b \in G$ this is a subgroup.

(3) $F = \{(x, y) | x, y \in 2\mathbb{Z}\}$. By the subgroup test, if $\forall a, b \in H, \quad ab^{-1} \in H$ then it is a subgroup. $ab^{-1} = (x_1 - x_2, y_1 - y_2)$, and since even integer

minus another even integer is always an even integer, both $(x_1 - x_2) \in 2\mathbb{Z}$ and $(y_1 - y_2) \in 2\mathbb{Z}$.
Conjecture: $G \cong F$. Let $\phi : G \to F$ be a function which takes $a = (x, y) \in G$ to $a' = (2x, 2y) \in F$, defined by $\phi(a) = 2a = a' \in F$. (It just doubles the input from G) N2S:.

i $\phi : G \to F$ is a homomorphism.
Consider some elements $a, b \in G$, such that $\phi(a) = a' \in F$ and $\phi(b) = b' \in F$.

$$\phi(a + b) = a' + b' = \phi(a) + \phi(b)$$

ii $\phi : G \to F$ is injective.
$\forall a \in G \; \exists a' \in F$ such that $\phi(a) = a'$. Let $\phi(a) = \phi(b)$, then $2a = 2b$, and therefore $a = b$. Thus this function is injective.

iii $\phi : G \to F$ is surjective.
Consider some arbitrary element a' in F, then there exists a unique element $\underbrace{a = \frac{a'}{2}}_{\text{Well defined because a' is in F}}$ in G such that $\phi(a) = a'$.
The quotient group of G consists of F, $(1, 0) + F$, $(0, 1) + F$ and $(1, 1) + F$.

QED

3 Problem 3

Let $E = \mathbb{Q}[i]$ be the set $\{a + bi | a, b \in \mathbb{Q}\}$. Show that E is a subfield of $\mathbb{C}$. Give a polynomial which splits in $E[x]$ but in $\mathbb{Q}[x]$.

Proof. $Q[i]$ is a subfield iff it passes the Subfield Test. We N2S:

1. $E^* \neq \emptyset$, clearly this is true.

2. $\forall x, y \in E : x - y \in E$. Consider some $x, y \in E$, then $x = a + bi$, $y = c + di$, then $x - y = (a - c) + (b - d)i$, and since $(a - c), (b - d) \in \mathbb{Q}$, this is true.

3. $\forall x, y \in E : x \cdot y \in E$. Consider some $x, y \in E$, then $x = a + bi$, $y = c + di$, then $x \cdot y = (a + bi)(c + di) = ac + adi + cbi - bd$, rewriting: $x \cdot y = (ac - bd) + (ad + cb)i$, and clearly, $(ac - bd), (ad + cb) \in \mathbb{Q}$.

4. $x \in E^* \implies x^{-1} \in E^*$. Consider some $x \in E^*$, then $x = a + bi$ where a and b cannot both be zero, and clearly $x^{-1} = \frac{a-bi}{a^2+b^2}$. This is well defined because if a is zero, b must not be, and if b is zero, a must not be. And of course, since $a, b \in \mathbb{Q}$, x^{-1} must be in E^*.

Where $E^* = E \backslash \{0_F\}$. Thus, E is a subfield of $\mathbb{C}$. QED

A polynomials which splits in $E[x]$ but not in $\mathbb{Q}[x]$ is $x^2 + 1$. It splits like so: $x^2 + 1 = (x + i)(x - i)$, which are both in E, but not in $\mathbb{Q}$.

4 Problem 4

For what values of $r \in \mathbb{R}$ is the following object a field?

$$E = \frac{\mathbb{R}[x]}{\langle x^2 + rx + 5 \rangle}$$

Proof. Results used:

1. Let F be a field and $p(x)$ be a nonconstant polynomial in $F[x]$. Then $p(x)$ is irreducible iff $\langle p(x) \rangle$ is a maximal ideal in $F(x)$.

2. Let R be a commutative ring with unity and M be an ideal of R. Then the factor ring R/M is a field iff M is a maximal ideal.

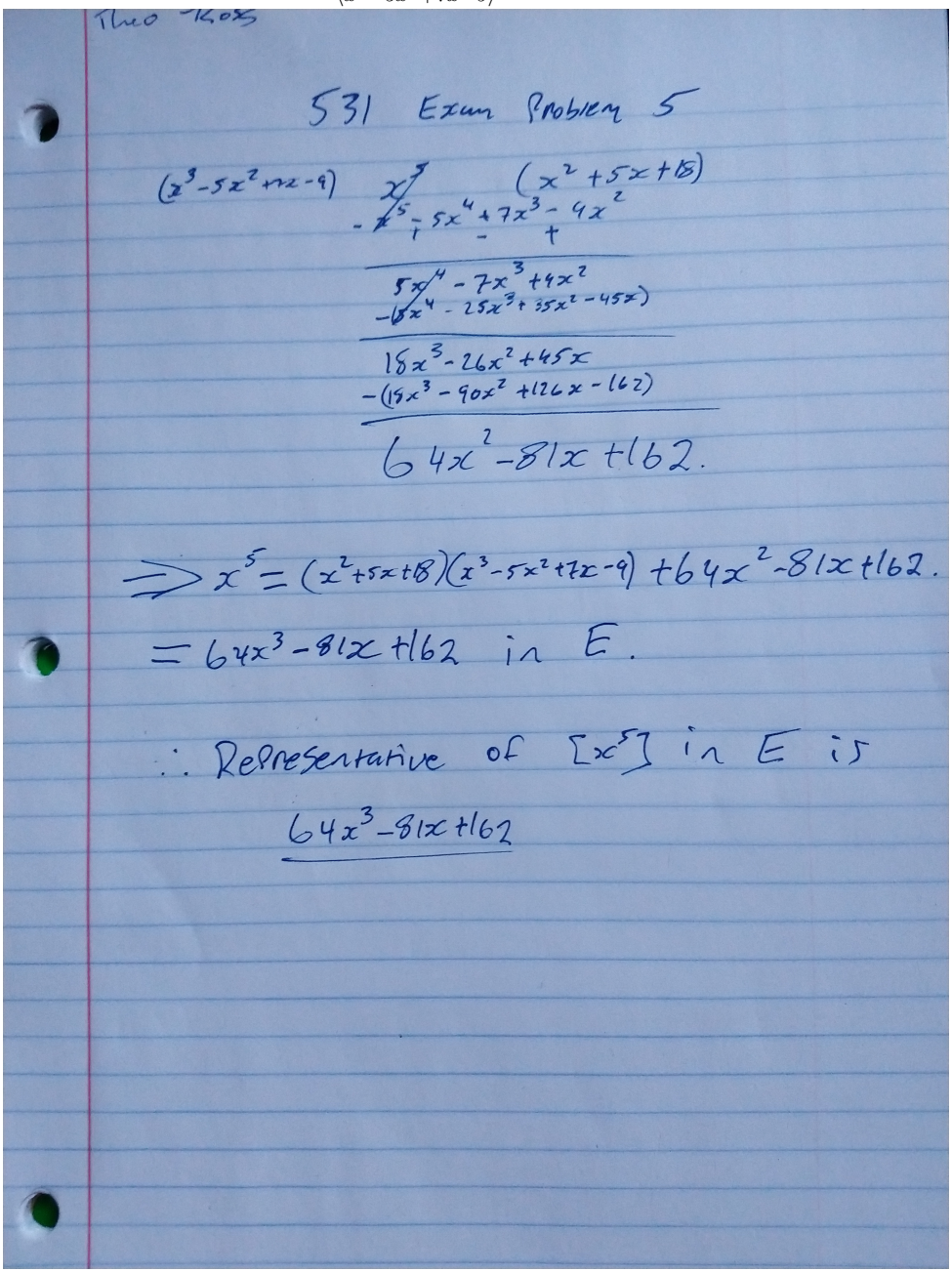
In the question, $\mathbb{R}$ is a field, and $\mathbb{R}[x]$ is a commutative ring with unity.
By result 2, $E = \frac{\mathbb{R}[x]}{\langle x^2+rx+5 \rangle}$ is a field iff $\langle x^2 + rx + 5 \rangle$ is maximal.
However by result 1, $\langle x^2 + rx + 5 \rangle$ is maximal iff $x^2 + rx + 5$ is irreducible.
Of course, in $\mathbb{R}[x]$, a second degree polynomial is irreducible iff it has no real roots.

$$r^2 - 20 < 0 \implies r^2 < 20 \implies r < \pm\sqrt{20}$$

Therefore for every $r \in (-\sqrt{20}, \sqrt{20})$ is when E is a field. QED

5 Problem 5

Find a representative in $\frac{\mathbb{Q}[x]}{\langle x^3-5x^2+7x-9\rangle}$ for the equivalence class $[x^5]$.



6 Problem 6

Find polynomials $p(x), q(x)$ and an integer p such that $q(x)|p(x)$ as elements of $\mathbb{Z}_p[x]$ but that $q(x) \nmid p(x)$ as elements of $\mathbb{R}[x]$. p, q will necessarily have integral coefficients.

Proof. Consider the polynomials $p(x) = x^2 + 1$, $q(x) = x + 1$, and $p = 2$. Since in $\mathbb{Z}_2[x]$, $-x = x$, we can divide $x^2 + 1$ by $(x + 1)$ leaving $(x + 1)$.

$$(x + 1)(x + 1) = x^2 + 2x + 1 \equiv x^2 + 1 \in \mathbb{Z}_2[x]$$

Therefore, in $\mathbb{Z}_2[x]$, $q(x)|p(x)$. Now consider these two polynomials in $\mathbb{R}[x]$. Again trying to do long division, we end with a remainder of 2, and therefore $q(x) \nmid p(x)$. QED