IntrotoAbstractAlgebra
Exam 2 Solutions

This exam has five questions, each worth 20 points, for a total of 100 points.

1. Give precise and complete statements of the following (no partial credit on this problem).

(a) The definition of a ring. (You can assume the definition of a group is known.)

A ring is a set R with two binary operations $+$ and $\cdot$ and distinct elements $0, 1 \in R$ such that

- $(R, +)$ is an abelian group with identity 0,
- $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$,
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$,
- $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$.

(b) The center of a group G is the set $Z(G)$ of elements of G commuting with all elements of G. That is, $Z(G) = \{a \in G : \ ab = ba\}$ for all $b \in G$.

(c) A quotient group.

Let G be a group and $H \lhd G$. The quotient group $G/H = \{gH : \ g \in G\}$, with multiplication $(aH)(bH) = abH$.

(d) An ideal in a ring $(R, +, \cdot)$ is a subgroup $(I, +) < (R, +)$, such that $rx \in I$ for all $r \in R$ and $x \in I$.

In the following problems, you may use any result proved in class or on the homework.

2. Let G be a group and let H be a normal subgroup of G. Assume that G/H is abelian.

Prove that $aba^{-1}b^{-1} \in H$ for all $a, b \in G$.

Proof: Let $a, b \in G$. Since G/H is abelian, we have $(aH)(bH) = (bH)(aH)$. This means $abH = baH$. Then we have $(ab)(ba)^{-1} \in H$, or $aba^{-1}b^{-1} \in H$. ■

Remark: The element $aba^{-1}b^{-1}$ is usually denoted $[a, b]$ and is called the *commutator* of a and b. The subgroup generated by all commutaters is called the *commutator subgroup* of G, and is denoted $[G, G]$. This problem showed that if G/H is abelian, then $[G, G] < H$. The converse is true as well. That is, G/H is abelian if and only if $[G, G] < H$.

3. Prove that $D_6/Z(D_6) \simeq S_3$.

Proof: D_6 is the symmetry group of a hexagon. We must find a surjective homomorphism $f : D_6 \to S_3$ with kernel $Z(D_6)$. First we have to find $Z(D_6)$. One element $z \in Z(D_6)$ is rotation by 180 degrees. If $|Z(D_6)| > 2$, then $|D_6/Z(D_6)| < 6$ and divides 6, hence would be prime, so $D_6/Z(D_6)$ would be cyclic, so D_6 would be abelian, which it is not. So $Z(D_6) = \langle z \rangle$ has order two.

To get a homomorphism $f : D_6 \to S_3$, note that D_6 permutes the three lines through opposite vertices of the hexagon. A rotation $r \in D_6$ of order six rotates the lines via a three-cycle, and the reflection about one of the lines permutes the other two. Hence f is surjective, and $|\ker f| = 2$. Since z sends each line to itself, we have $z \in \ker f$, so $\ker f = Z(D_6)$, as desired. ■

4. Find the minimal polynomial of $2^{1/10}$ over $\mathbb{Q}$.
You must prove that your polynomial is irreducible in $\mathbb{Q}[x]$.

Proof: The polynomial is $x^{10} - 2$. The prime 2 divides all of the coefficients but the leading one, and 2^2 does not divide the constant coefficient. Hence $x^{10} - 2$ is irreducible, by Eisenstein's criterion. ■

5. Prove that the polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

Proof: Since $f(0) = f(1) = 1$, there is no root in $\mathbb{Z}_2$. If $f(x)$ reduces, it must be a product of irreducible quadratic polynomials in $\mathbb{Z}_2[x]$. But the only irreducible quadratic polynomial in $\mathbb{Z}_2[x]$ is $x^2 + x + 1$. And $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, which is not $f(x)$. Hence $f(x)$ is irreducible in $\mathbb{Z}_2[x]$. ■

Remark: As a corollary, we have that if $abcd$ is odd, then $x^4 + ax^3 + bx^2 + cx + d$ is irreducible in $\mathbb{Q}[x]$. For if this reduced over $\mathbb{Q}$, then it reduces over $\mathbb{Z}$, by Gauss' lemma. Then the reduction mod 2, which is $f(x)$, would reduce over $\mathbb{Z}_2$, which it doesn't.