Math 113 Final Exam Solutions

1. a) (5 points) A ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Show that $xy = -yx$ for all $x, y \in R$ in a Boolean ring R. *(Hint: consider $(x+y)^2$)*

$(x+y)^2 = x^2 + xy + yx + y^2$. Since R is Boolean, we also have $(x+y)^2 = x+y$ as well as $x^2 = x$, $y^2 = y$. So we have $x+y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$. Adding $-x - y$ to each side, we get $0 = xy + yx$, or $xy = -yx$ as desired.

b) (3 points) Show that if R is Boolean, then $y = -y$ for all $y \in R$. Combine this with part (a) to deduce that every Boolean ring is commutative.

If R is Boolean, we have $-y = (-y)^2 = y^2 = y$ as desired. Combining this with part (a), we get $xy = -yx = yx$ for all $x, y \in R$, and so R is commutative.

b) (4 points) Show that any Boolean ring which is also an integral domain is isomorphic to $\mathbb{Z}_2$. *(Hint: rewrite $a^2 = a$ as something of the form $n \cdot m = 0$)*

Suppose a Boolean ring R is also an integral domain. Then R contains unity 1. Also, $a^2 = a$ for all $a \in R$ implies $a^2 - a = 0$, or $a(a-1) = 0$, giving us zero divisors a and $a-1$ in R unless $a = 0$ or $a = 1$. So if R is to have no zero divisors it must only contain two elements: 0 and 1. Thus R must be isomorphic to $\mathbb{Z}_2$.

2. a) (6 points) Let $H = \langle (2,4) \rangle$ be a subgroup of $\mathbb{Z} \times \mathbb{Z}$. Show that the cosets of H in $\mathbb{Z} \times \mathbb{Z}$ are precisely those of the form $(0,n)H$ and $(1,n)H$, where n can be any integer.

Suppose $(r,n)H = (s,m)H$ where $s, r = 0$ or 1. Then we have $(r-s, n-m) \in H$. Note that $|r-s| = 0$ or 1. At the same time, since $H = \langle (2,4) \rangle$, we have $2|r-s$, so $r-s = 0$ necessarily. But then $n-m = 0 \cdot 4 = 0$, and so we have that $(r,n)H = (s,m)H$ implies $r = s$ and $n = m$ if $0 \leq r,s \leq 1$. Thus all of the cosets of the form above are distinct. Also, for any integer a there are integers $k, 0 \leq r \leq 1$ such that $a = 2k + r$. So if $a, b \in \mathbb{Z}$ we have $(a,b)H = (2k+r,b)H = (r, b-4k)H$ which is of the form above.

b) (6 points) Determine all of the elements of finite order in $\mathbb{Z} \times \mathbb{Z}/\langle (2,4) \rangle$.

To determine elements of finite order, we solve $(kx, ky) = (2j, 4j)$ for a positive integer k, where $0 \leq x \leq 1$ and y are integers. If $x = 0$, then $j = 0$, giving us that $ky = 0$ meaning $y = 0$. This yields the trivial element of finite order. If $x = 1$, then $k = 2j$, so $2jy = 4j$, giving the solution $y = 2$. So the only elements of finite order are H of order 1 and $(1,2)H$ of order 2.

c) (4 points) Classify $\mathbb{Z} \times \mathbb{Z}/\langle (2,4) \rangle$ according to the fundamental theorem of finitely generated abelian groups. *(Hint: use parts (a) and (b))*

This group is isomorphic to $\mathbb{Z} \times \mathbb{Z}_2$. This is because the group is clearly infinite by part (a), and contains exactly two elements of finite order by part (b).

3. a) (8 points) Write the following two permutations in S_8 as a product of disjoint cycles. Are these permutations even or odd?

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 1 & 6 & 8 & 2 & 3 & 5 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 8 & 5 & 7 & 3 & 4 & 6 \end{pmatrix}$$

$\sigma_1 = (1,7,3)(2,4,6)(5,8)$ and $\sigma_2 = (1,2)(3,8,6)(4,5,7) = (3,8,6)(4,5,7)(1,2)$. In each case, the product of the 3-cycles is even, so we can write both σ_1 and σ_2 as a product of an odd number of transpositions, giving us that both permutations are odd.

b) (4 points) Find an element $\tau \in S_8$ such that $\tau\sigma_1\tau^{-1} = \sigma_2$.

Since these are of the same cycle type, they are indeed conjugate, and we know how to find τ from one of our homeworks. One such τ is

$$\begin{pmatrix} 1 & 7 & 3 & 2 & 4 & 6 & 5 & 8 \\ 3 & 8 & 6 & 4 & 5 & 7 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 5 & 1 & 7 & 8 & 2 \end{pmatrix}.$$

c) (4 points) Describe two different subgroups of order 10 in S_8: they are allowed to be isomorphic. Make sure to indicate why they are of order 10 and why they are different. *(Hint: this might be easiest if you look for cyclic subgroups)*

We produce two cyclic groups of order 10 by finding two elements of order 10 in S_8. For example, take $H = \langle (1,2,3,4,5)(6,7) \rangle$ and $H' = \langle (1,2,3,4,5)(6,8) \rangle$. Both have order 10 since the order is just the lcm of the cycle lengths in the disjoint cycle decomposition, and they are different because H leaves 8 fixed while H' does not.

4) a) (6 points) For $n > 2$, demonstrate that the multiplicative group of units in the ring $\mathbb{Z}_{2^n}$ has two distinct subgroups of order 2.

Any subgroup of order 2 will be cyclic since 2 is prime, so we need only find two distinct elements of order 2 in $\mathbb{Z}_{2^n}^*$. Note first that the elements in $\mathbb{Z}_{2^n}^*$ are precisely those which are relatively prime to 2^n, or precisely the odd ones. One such element of order 2 is $2^n - 1$, since $(2^n - 1)^2 = 2^{2n} - 2^{n+1} + 1 \equiv 1 \bmod 2^n$ and $2^n - 1 \neq 1$ for $n > 1$. Another is $2^{n-1} + 1$ since $(2^{n-1} + 1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \bmod 2^n$ and different from $2^n - 1$ as long as $n > 2$. So the groups generated by these two give two distinct subgroups of order 2.

b) (4 points) Deduce that the group of units in part (a) is not cyclic (explain how you can deduce this).

Any cyclic group G has exactly one subgroup of order d for $d \,||G|$. In particular, a cyclic group cannot have two different subgroups of the same order, so $\mathbb{Z}_{2^n}^*$ is not cyclic by part (a).

5) a) (5 points) Let R be a finite commutative ring with unity. Show that every prime ideal I in R is maximal. *(Hint: consider R/I)*

Suppose I in R is prime. Then R/I is an integral domain, and it is finite since R is finite. But finite integral domains are fields, so R/I is a field, and thus I is maximal.

b) (5 points) Find a factorization of $3-4i$ into irreducibles in $\mathbb{Z}[i]$.

We find that the norm of $3-4i$ is $9+16=25$, so if it factors into irreducibles (up to multiplication by a unit) one of its factors must be $1\pm 2i$. Indeed,

$$\frac{3-4i}{1+2i}\cdot\frac{1-2i}{1-2i}=\frac{3-8-4i-6i}{5}=-1-2i$$

so we have $3-4i=(-1-2i)(1+2i)$ which is a product of irreducibles since the norms of $1+2i$ and $-1-2i$ are prime.

6. a) (6 points) Let $\phi_{\sqrt[3]{3+i}} : \mathbb{Q}[x] \to \mathbb{C}$ be the homomorphism which takes a polynomial $f(x) \in \mathbb{Q}[x]$ to $f(\sqrt[3]{3+i})$. The kernel of this map is an ideal of the form $\langle p(x) \rangle$. Determine $p(x)$.

The kernel is precisely the ideal generated by the minimal polynomial of $\alpha = \sqrt[3]{3+i}$. Note that $\alpha^3 - 3 = i$, and so $\alpha^6 - 6\alpha^3 + 10 = 0$. Thus α is a zero of $x^6 - 6x^3 + 10$. This polynomial is irreducible by Eisenstein's Criterion with $p = 2$, so it is in fact the minimal polynomial of α.

b) (4 points) Let $\alpha = \sqrt[3]{3+i}$. Write α^7 in the form $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 + a_5\alpha^5$ where $a_i \in \mathbb{Q}$ for all $0 \leq i \leq 5$.

There are a couple ways to approach this. I will use the algorithm discussed in class. We know $\alpha^6 - 6\alpha^3 + 10 = 0$, so we have $\alpha^6 = 6\alpha^3 - 10$. Then $\alpha^7 = \alpha \cdot \alpha^6 = 6\alpha^4 - 10\alpha$, and so one can write $\alpha^7 = 0 - 10\alpha + 0 \cdot \alpha^2 + 0 \cdot \alpha^3 + 6\alpha^4 + 0 \cdot \alpha^5$.

c) (2 points) Show that the field $\mathbb{Q}(i)$ is contained in $\mathbb{Q}(\sqrt[3]{3+i})$ and determine $[\mathbb{Q}(\sqrt[3]{3+i}) : \mathbb{Q}(i)]$.

$\mathbb{Q}(i)$ is contained in $\mathbb{Q}(\sqrt[3]{3+i})$ since $i = (\sqrt[3]{3+i})^3 - 3$ is contained in $\mathbb{Q}(\sqrt[3]{3+i})$. Thus $6 = [\mathbb{Q}(\sqrt[3]{3+i}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3+i}) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt[3]{3+i}) : \mathbb{Q}(i)]$ and so $[\mathbb{Q}(\sqrt[3]{3+i}) : \mathbb{Q}(i)] = 3$.

7) a) (4 points) Let G be a group and let X be a G-set. Define the set $G_X = \{g \in G \mid gx = x \text{ for all } x \in X\}$. Show that G_X is a subgroup of G.

First, note that $e_G \in G_X$ by the definition of group action. Next, if $a, b \in G_X$, then $(ab)x = a(bx) = ax$ for all $x \in X$, and in turn $ax = x$ for all $x \in X$. Thus we have $(ab)x = x$ for all $x \in X$ and so $ab \in G_X$. Finally, if $a \in G_X$, then $x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}x$ for all $x \in X$, and so $a^{-1} \in G_X$. Therefore $G_X \leq G$.

b) (2 points) How is G_X related to the stabilizers G_x of elements $x \in X$? No justification necessary.

It is the intersection of all of the stabilizers:

$$G_X = \bigcap_{x \in X} G_x.$$

c) (4 points) Let H be a subgroup of G. H acts on G by conjugation: $h(g) = h^{-1}gh$. Show that the group H_G as defined in part (a) is contained in the center of G.

The group H_G is one in which every element h has the property that $h^{-1}gh = g$ for all $g \in G$. Thus in particular $gh = hg$ for all $h \in H_G$ and all $g \in G$. Since the center of G is simply $\{a \in G \mid ag = ga \text{ for all } g \in G\}$, H_G is contained in the center.

8. (2 points each) Mark each of the following as True or False. Please justify with a few words or a counterexample (no need to write an essay, just make me believe you understand why the answer you chose is the right one).

a) $\mathbb{Z}_3[x]/\langle x^3+x^2+1\rangle$ is a field containing 27 elements.

False: x^3+x^2+1 has a zero $1 \in \mathbb{Z}_3$ and is therefore reducible in $\mathbb{Z}_3[x]$. Thus $\mathbb{Z}_3[x]/\langle x^3+x^2+1\rangle$ is not a field.

b) The collection of zero-divisors together with the 0 element in a ring make up an ideal in that ring.

False: consider $R = M_{2\times 2}(\mathbb{R})$ with matrix addition and multiplication. We have that the sum of the following two zero divisors is not a zero divisor

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

so this set in this case is not closed under addition and therefore not an ideal.

c) The commutator subgroup of a simple group is trivial.

False: Consider the group A_5. Its commutator subgroup is not trivial since $A_5/\{\sigma_e\}$ is not abelian.

d) $\mathbb{Q}, +$ is a cyclic group.

False: if $\mathbb{Q}$ were $\langle a/b\rangle$, where $a, b \in \mathbb{Z}\backslash\{0\}$, then we would have that $a/2b$ is not in $\mathbb{Q}$.

e) The field of quotients of $\mathbb{Q}[\pi]$ is isomorphic to $\mathbb{Q}(x)$, the field of rational functions.

True, since π is transcendental over $\mathbb{Q}$ we have $\mathbb{Q}[\pi] \cong \mathbb{Q}[x]$ and so its field of quotients is isomorphic to $\mathbb{Q}(x)$.

f) A commutative ring with unity R is a field if and only if $\{0\}$ is a maximal ideal in R.

True: A commutative ring with unity R is a field if and only if $\{0\}$ and R are the only ideals, which is if and only if $\{0\}$ is a maximal ideal in R.

g) Let G be a group. The map $\phi : G \to G$ where $\phi(g) = g^{-1}$ is a group homomorphism if and only if G is abelian.

True: ϕ is a homomorphism iff $b^{-1}a^{-1} = (ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$. Multiplying this equation by ab from the left and by ba from the right, we have that this is iff $ba = ab$ for all $a, b \in G$, which is iff G is abelian.