FINAL EXAM
MATH 103B, UCSD, SPRING 16

You have three hours.

There are 11 problems, and the total number of points is 155. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:______________________________

Signature:______________________________

Problem	Points	Score
1	30	
2	20	
3	15	
4	10	
5	10	
6	15	
7	10	
8	10	
9	10	
10	15	
11	10	
12	10	
13	10	
14	10	
15	10	
Total	155	

1. (30pts) (i) *Give the definition of a left coset of a subgroup H of a group G.*
A subset of the form

$$gH = \{ gh \mid h \in H \}$$

for any $g \in G$.

(ii) *Give the definition of the kernel of a homomorphism of groups.*
If $\phi\colon G \longrightarrow G'$ is a homomorphism of groups then the kernel is the inverse image of the identity.

(iii) *Give the definition of a normal subgroup H of a group G.*
H is a normal subgroup if the left cosets are equal to the right cosets, $gH = Hg$.

(iv) *Give the definition of a unit in a ring R with unity.*
$u \in R$ is a unit if u has an inverse v, so that, $uv = vu = 1$.

(v) *Give the definition of the Euler phi-function.*
$\varphi(n)$ is the number of integers between 0 and $n-1$ coprime to n.

(vi) *Give the definition of an irreducible polynomial over a field.*
A non-zero polynomial $f(x)$ over a field F is irreducible if whenever $f(x) = g(x)h(x)$ then one of $g(x)$ or $h(x)$ has degree equal to the degree of $f(x)$.

2. (20pts) (i) *Find all cosets of* $\langle 4 \rangle$ *inside the group* $\mathbb{Z}_{12}$.

$\langle 4 \rangle = \{ 0, 4, 8 \}$ $\quad 1+\langle 4 \rangle = \{ 1, 5, 9 \}$ $\quad 2+\langle 4 \rangle = \{ 2, 6, 10 \}$ $\quad$ and $\quad 3+\langle 4 \rangle = \{ 3, 5, 11 \}$

(ii) *Let* $\sigma = (1, 2, 4, 5)(3, 6)$ *in* S_6. *Find the index of* $\langle \sigma \rangle$ *in* S_6.
σ has order 4, so that $|\langle \sigma \rangle| = 4$. So by Lagrange the index is

$$\frac{|S_6|}{|\langle \sigma \rangle|} = \frac{6!}{4} = 6 \cdot 5 \cdot 3 \cdot 2 = 180.$$

(iii) *Find the order of* $(3, 6, 12, 16)$ *in* $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$.
3 has order 4 in $\mathbb{Z}_4$; 6 has order $2 = 12/6$ in $\mathbb{Z}_{12}$; 12 has order $5 = 20/4$ in $\mathbb{Z}_{20}$; 16 has order $3 = 24/8$ in $\mathbb{Z}_{24}$. The order of $(3, 6, 12, 16)$ in the product is the lowest common multiple of 4, 2, 5 and 3, which is 60.

(iv) *Find* $\phi(14)$, *if* $\phi \colon \mathbb{Z} \longrightarrow S_8$ *is a group homomorphism and* $\phi(1) = (2, 5)(1, 4, 6, 7)$.
$\phi(1)$ has order 4. Thus

$$\begin{aligned}
\phi(14) &= \phi(12 + 2) \\
&= \phi(12)\phi(2) \\
&= \phi(4)^3\phi(1)\phi(1) \\
&= (2, 5)(1, 4, 6, 7)(2, 5)(1, 4, 6, 7) \\
&= (1, 6)(4, 7).
\end{aligned}$$

3. (15pts) (i) *State the fundamental theorem of finitely generated abelian groups.*
Every finitely generated abelian group is isomorphic to a product

$$\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where $p_1, p_2, \ldots, p_n$ are prime numbers and $a_1, a_2, \ldots, a_n$ are positive integers. The direct product is unique, up to re-ordering the factors, so that the number of copies of $\mathbb{Z}$ and the prime powers are unique.

(ii) *Find all abelian groups of order* 1400*, up to isomorphism.*

$$1400 = 100 \cdot 14 = 2^2 \cdot 5^2 \cdot 2 \cdot 7 = 2^3 \cdot 5^2 \cdot 7.$$

Thus

(1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$
(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_7$
(3) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$
(4) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25} \times \mathbb{Z}_7$
(5) $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$
(6) $\mathbb{Z}_8 \times \mathbb{Z}_{25} \times \mathbb{Z}_7$,

is a complete list of abelian groups of order 1400, up to isomorphism.

4. (10pts) *Is there a homomorphism $S_6 \longrightarrow \mathbb{Z}_7$ which is onto? If there is one, give an example and if there is not, explain why not.*
There is no onto homomorphism. Suppose not, suppose that $\phi[S_6] = \mathbb{Z}_7$. By the first isomorphism theorem $\mathbb{Z}_7$ is isomorphic to S_6/K, where K is the kernel of ϕ. By Lagrange this has $6!/k$ elements, where k is the order of K. But 7 does not divide $6!$, so this is not possible.

5. (10pts) *Show that A_n is a normal subgroup of S_n and compute S_n/A_n.*
Let $\phi \colon S_n \longrightarrow \mathbb{Z}_2$ be the map which sends the permutation σ to 0 if σ is even and 1 if σ is odd. We check that ϕ is a group homomorphism. We have to check that

$$\phi(\sigma\tau) = \phi(\sigma) + \phi(\tau).$$

There are four cases, depending on the parity of σ and τ. If σ and τ are even then then so is $\sigma\tau$, the LHS is 0 and the RHS is $0 + 0 = 0$.
If one of σ and τ is odd and the other is even then $\sigma\tau$ is odd. The LHS is 1 and the RHS is $0 + 1 = 1$.
If both σ and τ are odd then $\sigma\tau$ is even. The LHS is 0 and the RHS is $1 + 1 = 0$.
Therefore ϕ is a group homomorphism. The kernel is A_n and so A_n is a normal subgroup. The quotient is isomorphic to $\mathbb{Z}_2$ by the first isomorphism theorem.

6. (15pts) (i) *Let* $\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ *be a group homomorphism. If* $\phi(1) = (a, b)$ *then what is* $\phi(2)$*?* $\phi(3)$*?* $\phi(n)$*?*
$\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = (a, b) + (a, b) = (2a, 2b)$. $\phi(3) = \phi(2 + 1) = \phi(2) + \phi(1) = (2a, 2b) + (a, b) = (3a, 3b)$. More generally $\phi(n) = (na, nb)$ by induction.

(ii) *Let* $\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ *be a ring homomorphism. If* $\phi(1) = (a, b)$ *then what are the possible values of* a *and* b*?*
$1 = 1 \cdot 1$ so that $(a, b) = \phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1) = (a, b)(a, b) = (a^2, b^2)$. So $a^2 = a$ and $b^2 = b$. It follows that a and b are individually either zero or one.

(iii) *Describe all ring homomorphisms* $\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$*.*
By part (i) it suffices to determine all possible values of a and b.
There are four possible choices of a and b, $a = b = 0$; $a = 1$, $b = 0$; $a = 0$, $b = 1$ and $a = b = 1$. We check that these are ring homomorphisms. In the first case we have the zero homomorphism, $n \longrightarrow (0, 0)$. The next two cases are inclusion into either factor, $n \longrightarrow (n, 0)$ and $n \longrightarrow (0, n)$. The last case is the inclusion $n \longrightarrow (n, n)$ which is a ring homomorphism.

7. (10pts) *Find a generator of the group of units of* $\mathbb{Z}_{17}$.
The group of units has 16 elements. As the order of any element divides 16 by Lagrange, the possible orders are 1, 2, 4, 8 and 16. If $a \in \mathbb{Z}_{17}$ has order at most 8 then $a^8 = 1 \mod 17$. So it suffices to find a such that $a^8 \neq 1 \mod 17$. We apply trial and error. If $a = 2$ then $2^2 = 4$, $2^4 = 16 = -1$ and so $2^8 = 1$, no good. $3^2 = 9$, $3^3 = 27 = 10$, $3^4 = 30 = 13 = -4$ and $3^8 = (-4)^2 = 16 = -1$. So 3 is a generator.

8. (10pts) *Find the remainder of* 37^{49} *when it is divded by* 7.
$37 = 2 \mod 7$ and so we just need to compute 2^{49}.
Fermat implies that $2^6 = 1 \mod 7$. $49 = 48 + 1 = 8 \cdot 6 + 1$. Thus

$$\begin{aligned} 37^{49} &= 2^{49} \\ &= 2^{8 \cdot 6 + 1} \\ &= (2^6)^8 \cdot 2 \\ &= 2 \mod 7. \end{aligned}$$

9. (10pts) *If* $f(x) = x^4 + 5x^3 - 3x^2$ *and* $g(x) = 5x^2 - x + 2$ *then find* $q(x)$ *and* $r(x) \in \mathbb{Z}_{11}[x]$ *such that* $f(x) = q(x)g(x) + r(x)$*, by applying the division algorithm.*
Applying the division algorithm we get

$$\begin{aligned} f(x) &= q(x)g(x) + r(x) \\ x^4 + 5x^3 - 3x^2 &= (9x^2 + 5x + 10)(5x^2 - x + 2) + 2. \end{aligned}$$

10. (15pts) (i) *Express* x^3+2x+3 *as a product of irreducible polynomials over* $\mathbb{Z}_5$.

Let $f(x) = x^3 + 2x + 3$. We check for zeroes of $f(x)$

$f(0) = 3$ $f(1) = 1$ $f(2) = 8+4+3 = 0$ $f(3) = 27+3+6 = 1$ and $f(4) = 64+8+3 = 0$.

Thus $\alpha = 2$ and $\alpha = 4$ are zeroes. Thus $f(x)$ has two linear factors. It must have another one as it is a cubic. The product of the zeroes is $-3 = 2$ and the product of 2 and 4 is 3. So the third zero is $2/3 = 4$. Thus

$$x^3 + 2x + 3 = (x-2)(x-4)^2 = (x+3)(x+1)^2.$$

(ii) *Show that* $x^2 + 6x + 12$ *is irreducible over* $\mathbb{Q}$.

There are many ways to do this. Probably the easiest is to apply Eisenstein with $p = 3$.

(iii) *Is* $x^2 + 6x + 12$ *irreducible over* $\mathbb{R}$*? Over* $\mathbb{C}$*?*

The discriminant is $36 - 48 < 0$. Thus $x^2 + 6x + 12$ has two complex conjugate roots and no real roots. It follows that $x^2 + 6x + 12$ is irreducible over $\mathbb{R}$ and reducible over $\mathbb{C}$.

11. (10pts) *State Eisenstein's criteria. Prove that the polynomial* $f(x)$

$$3x^{13}-15x^{12}+25x^{11}+30x^{10}-40x^9+10x^8+15x^7-5x^6-30x^5+10x^4+15x^3-5x^2+20x+5,$$

is an irreducible element of $\mathbb{Q}[x]$.

Let $f(x)$ be a polynomial with integer coefficients. Suppose that p is a prime that divides all but the leading coefficient (so that p does not divide the leading coefficient) and p^2 does not divide the constant coefficient. Then $f(x)$ is irreducible over $\mathbb{Q}$.

Apply Eisenstein with $p = 5$.

Bonus Challenge Problems

12. (10pts) *Prove Lagrange's theorem.*

Let H be a subgroup of the finite group G. If $g \in G$ define a map

$$\psi \colon H \longrightarrow gH \qquad \text{by sending} \qquad h \longrightarrow gh.$$

Note that ψ has an inverse map,

$$\phi \colon gH \longrightarrow H \qquad \text{by sending} \qquad gh \longrightarrow h.$$

Therefore ψ is one to one and onto. Since the left cosets of H in G are a partition of G and every left coset has the same size as H, we have

$$|G| = |H|[G : H].$$

13. (10pts) *Find all irreducible polynomials of degree at most* 3 *over* $\mathbb{Z}_3$.
We first find all monic polynomials of degree at most 3. Every linear polynomial is irreducible;

$$x \qquad x+1 \qquad \text{and} \qquad x+2.$$

Multiplying by 2 we get

$$2x \qquad 2x+2 \qquad \text{and} \qquad 2x+1.$$

A general monic quadratic polynomial looks like $x^2 + ax + b$. This is irreducible if it has no zeroes. $b \neq 0$ if $\alpha = 0$ is not a zero.

$$f(1) = a + b + 1 \qquad \text{and} \qquad f(2) = 4 + 2a + b = 2a + b + 1.$$

Thus $b \neq 0$, $a + b \neq 2$ and $2a + b \neq 2$. The possibilities are

$$x^2 + 1 \qquad x^2 + x + 2 \qquad \text{and} \qquad x^2 + 2x + 2.$$

Multiplying by 2 we get

$$2x^2 + 2 \qquad 2x^2 + 2x + 1 \qquad \text{and} \qquad 2x^2 + x + 1.$$

A general monic cubic polynomial looks like $x^3 + ax^2 + bx + c$. This is irreducible if it has no zeroes. $c \neq 0$ if $\alpha = 0$ is not a zero.

$$f(1) = a+b+c+1 \qquad \text{and} \qquad f(2) = 8+4a+2b+c = a+2b+c+2.$$

Thus $c \neq 0$, $a + b + c \neq 2$ and $a + 2b + c \neq 1$. The possibilities are

$$x^3+2x+1 \qquad x^3+x^2+2x+1 \qquad x^3+2x^2+1 \qquad \text{and} \qquad x^3+2x^2+x+1,$$

when $c = 1$ and

$$x^3+2x+2 \qquad x^3+x^2+2 \qquad x^3+x^2+x+2 \qquad \text{and} \qquad x^3+2x^2+2x+2,$$

when $c = 2$.
Multiplying by 2 we get

$$2x^3+x+2 \qquad 2x^3+2x^2+x+2 \qquad 2x^3+x^2+2 \qquad \text{and} \qquad 2x^3+x^2+2x+2,$$

and

$$2x^3+x+1 \qquad 2x^3+2x^2+1 \qquad 2x^3+2x^2+2x+1 \qquad \text{and} \qquad 2x^3+x^2+x+1.$$

14. (10pts) *Show that every finite subroup G of the multiplicative group of a field F is cyclic.*
See the lecture notes.

15. (10pts) *Show that if* p *is a prime then* $x^{p-1} + x^{p-2} + \cdots + 1$ *is an irreducible polynomial over* $\mathbb{Q}$.
See the lecture notes.