PRACTICE FINAL
MATH 18.703, MIT, SPRING 13

You have three hours. This test is closed book, closed notes, no calculators.

There are 11 problems, and the total number of points is 180. Show all your work. *Please make your work as clear and easy to follow as possible.* Points will be awarded on the basis of neatness, the use of complete sentences and the correct presentation of a logical argument.

Name:______________________________

Signature:______________________________

Student ID #:______________________________

Problem	Points	Score
1	30	
2	15	
3	15	
4	15	
5	15	
6	15	
7	10	
8	10	
9	15	
10	10	
11	25	
Presentation	5	
Total	180	

1. (30pts) Give the definition of a group.

Solution: A group G is a set together with a binary operation of multiplication which is associative, so that $g \cdot (h \cdot k) = (g \cdot h) \cdot k$, there is an identity element $e \in G$ such that $e \cdot g = g \cdot e = g$ and every element g has an inverse g^{-1} such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

(ii) Give the definition of an automorphism of groups.

Solution: An automorphism is an isomorphism $\rho\colon G \longrightarrow G$.

(iii) Give the definition of D_n, the dihedral group.

Solution: The symmetries of a regular n-gon.

(iv) Give the definition of an ideal.

Solution: An ideal $I \subset R$ in a ring R is an additive subgroup such that if $r \in R$ and $a \in I$ then $r \cdot a \in I$.

(v) Give the definition of a principal ideal domain.

Solution: An integral domain such that every ideal is principal.

(vi) Give the definition of a unique factorisation domain.

Solution: A UFD is an integral domain such that every non-zero element, not a unit has a factorisation into prime elements unique up to order and associates.

2. (15pts)
(i) Let G be a group and let $\sim$ be the relation $g_1 \sim g_2$ if there is an element $h \in G$ such that $g_2 = hg_1h^{-1}$. Show that $\sim$ is an equivalence relation.

Solution:
$g_1 \sim g_1$ as $g_1 = eg_1e^{-1}$, so that $\sim$ is reflexive. If $g_1 \sim g_2$ then $g_2 = hg_1h^{-1}$, so that $g_1 = h^{-1}g_2h = (h^{-1})g_2(h^{-1})^{-1}$ and $g_2 \sim g_1$. Thus $\sim$ is symmetric. Finally suppose that $g_1 \sim g_2$ and $g_2 \sim g_3$ so that $g_2 = hg_1h^{-1}$ and $g_3 = kg_2k^{-1}$. Then

$$g_3 = kg_2k^{-1} = k(hg_1h^{-1})k^{-1} = (kh)g_1(kh)^{-1},$$

so that $g_1 \sim g_3$ and $\sim$ is transitive. Thus $\sim$ is an equivalence relation.

(ii) If $G = S_5$ then identify the equivalence classes.

Solution: Two elements of S_n are conjugate if and only if they have the same cycle type. The cycle types in S_5 are [1|1|1|1|1] (fix everything) [2|1|1|1] (a transposition) [3|1|1] (a 3-cycle) [4|1] (a 4-cycle), [5] (a 5-cycle), [2|2|1] (product of two transpositions), [2|3] (product of a transposition and a 3-cycle).

3. (15pts) Classify all groups of order at most ten.

Solution:
There are the ten cyclic groups of order $1 \leq n \leq 10$.
If G is a finite abelian group then G is a product of cyclic groups whose successive orders divide each other. Other than the cyclic groups there are therefore three other abelian groups $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
If G has order a prime then G is cyclic. Suppose that every element in G has order two. Let a and b be two elements of G.

$$ab = (ab)^2 = abab.$$

Cancelling we have $ab = ba$ and G is abelian. Thus we may assume that not every element of G has order 2. Let G be a group of order 4. If there is an element of order 4 then G is cyclic. Otherwise every element of G has order 2 by Lagrange and so G is abelian.
Suppose that G has order $2n$, $n = 3$, 4 or 5. Then one example of a non-abelian group of order $2n$ is D_n. A presentation of D_n is given by two elements a and b, orders n and 2 such that $bab = a^{-1}$.
Suppose that G has order 6. By Sylow's theorem there is a subgroup H of order 3. If $a \in H$ is not the identity then $H = \langle a \rangle$. H is normal as it has index 2. Pick $b \in G - H$. Then bH has order two in G/H so that $b^2 \in H$. But then $b^2 = e$, otherwise b has order 6. a and b are clearly generators of G. We have $bab^{-1} \in H$ as H is normal, so that $bab \in H$. bab cannot be e and if $bab = a$ then a and b commute so that G is abelian. Thus $bab = a^{-1}$ and $G \simeq D_3$.
A similar argument works if G has order 10. Suppose that G is a non-abelian group of order 8. Then not every element has order 2 and there are no elements of order 8 so that there must be an element a of order 4. Let $H = \langle a \rangle$. Then H is a subgroup of index two so it must be normal. Pick $b \in G - H$. Then $bab \in H$ is an element of order 4, either a or a^3. If $bab = a$ then G is abelian and so $bab = a^{-1}$.
bH has order 2 in G/H and so $b^2 \in H$. If $b^2 = e$ then $G \simeq D_4$ as before. If $b^2 = a$ or a^3 then b has order 8, a contradiction. $b^2 = a^2$ is the only remaining possibility and this determines G. But there is another group of order 8, namely the quaternions,

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad ij = k.$$

So there are two non-abelian groups of order 8, D_4 and the quaternions.

4. (15pts) (i) State the second isomorphism theorem.

Solution: Let G be a group, let H be a subgroup and let N be a normal subgroup. Then

$$H \vee N = HN = \{\, hn \,|\, h \in H, n \in N \,\}.$$

Furthermore $H \cap N$ is a normal subgroup of H and the two groups $H/H \cap N$ and HN/N are isomorphic.

(ii) Prove the second isomorphism theorem.

Solution:
The pairwise products of the elements of H and N are certainly elements of $H \vee N$. Thus the RHS of the equality above is a subset of the LHS. The RHS is clearly non-empty and so it suffices to prove that the RHS is closed under products and inverses.
If x and y are elements of the RHS, then $x = h_1n_1$ and $y = h_2n_2$, where $h_i \in H$ and $n_i \in N$. Now $h_2^{-1}n_1h_2 = n_3 \in N$, as N is normal in G. So $n_1h_2 = h_2n_3$. In this case

$$\begin{aligned} xy &= (h_1n_1)(h_2n_2) \\ &= (h_1(n_1h_2)n_2 \\ &= (h_1(h_2n_3)n_2 \\ &= (h_1h_2)(n_3n_2), \end{aligned}$$

which shows that xy has the correct form. On the other hand, suppose $x = hn$. Then $hnh^{-1} = m \in N$ as N is normal and so $hn^{-1}h^{-1} = m^{-1}$. In this case

$$\begin{aligned} x^{-1} &= n^{-1}h^{-1} \\ &= hm^{-1}, \end{aligned}$$

so that x^{-1} is of the correct form. Hence the first statement.
Let $H \longrightarrow HN$ be the natural inclusion. As N is normal in G, it is certainly normal in HN, so that we may compose the inclusion with the natural homomorphism to get a homomorphism

$$\phi \colon H \longrightarrow HN/N.$$

This map sends h to hN. Suppose that $x \in HN/N$. Then $x = hnN = hN$, where $h \in H$. Thus the homorphism above is clearly surjective. Suppose that $h \in H$ belongs to the kernel. Then $hN = N$ the identity coset, so that $h \in N$. Thus $h \in H \cap N$ and the result follows by applying the First Isomorphism Theorem to ϕ.

5. (15pts) (i) State Sylow's theorems.

Solution: Let G be a group of order of order n and let p be a prime dividing n.
Then the number of Sylow p-subgroups is equal to one modulo p, divides n and any two Sylow p-subgroups are conjugate.

(ii) Let G be a group of order pqr, where p, q and r are distinct primes. Show that G is not simple.

Solution:
We may assume that $p < q < r$. The number n_r of Sylow r-subgroups is congruent to one modulo r and divides pqr, that is, n_r divides pq. Thus $n_r = 1$, p, q or pq. If $n_r = 1$ then there is a unique Sylow r-subgroup and this group is then automatically normal. Otherwise $n_r \geq r + 1$ so that $n_r > q > p$. The only remaining possibility is that $n_r = pq$. In this case there are $pq(r - 1)$ elements of order r.
Now consider the number n_q of Sylow q-subgroups. n_q is congruent to one modulo q and divides pqr. If $n_q = 1$ there is nothing to prove. Otherwise $n_q > q > p$. It follows that $n_q = r$ or pr.
If $n_q = pr$ then there are $pr(q - 1)$ elements of order q. In total there are then

$$pq(r - 1) + pr(q - 1) = 2pqr - p(q + r) = pqr + p(qr - q - r)$$

elements of order either q or r. This is more than the number of elements of G, a contradiction.
Thus $n_q = r$ and there are $r(q - 1)$ elements of order q.
Now consider the number n_p of Sylow p-subgroups. n_p is congruent to one modulo p and divides pqr. If $n_p = 1$ there is nothing to prove. Otherwise $n_p \geq q$ and there are at least $q(p - 1)$ elements of order p. In total there are then

$$pq(r - 1) + r(q - 1) + q(p - 1) = pqr + qr - r - 1,$$

elements of order p, q or r, which exceeds the number of elements of G, a contradiction.
Thus G is not simple.

6. (15pts) (i) If the prime ideal P contains the product IJ of two ideals then prove that P contains either I or J.

Solution:
Suppose that P does not contain J. Then we may find $j \in J$ not in P. Suppose that $i \in I$. Then $ij \in IJ \subset P$ so that $i \in P$ as P is prime. But then $I \subset P$.

(ii) Exhibit a natural bijection between the prime ideals of R/IJ and $R/I \cap J$.

Solution: Let

$$u \colon R \longrightarrow R/IJ \qquad \text{and} \qquad v \colon R \longrightarrow R/I \cap J$$

be the two natural ring homorphisms. Prime ideals of R/IJ are in bijection with prime ideals of R which contain IJ, and prime ideals of $R/I \cap J$ are in bijection with prime ideals of R which contain $I \cap J$. By (i) any prime ideal which contains IJ must contain either I or J, so that it must contain $I \cap J$. Conversely, IJ is the smallest ideal which contains all products ij, $i \in I$ and $j \in J$. As $ij \in I$ and $ij \in J$, $I \cap J$ is an ideal which contains all products ij so that $IJ \subset I \cap J$. Thus prime ideal which contain IJ are the same as prime ideals which contain $I \cap J$.

(iii) Give an example of a ring R, and ideals I and J such that IJ and $I \cap J$ are different.

Solution: Let $R = \mathbb{Z}$ and $I = J = \langle 2 \rangle$. Then $I \cap J = \langle 2 \rangle$ and $IJ = \langle 4 \rangle$.

7. (10pts) Does every UFD R, which is not a field, contain infinitely many irreducible elements which are pairwise not associates? If your answer is yes then prove it and if no then give an example.

Solution:
No. Let

$$R = \{\, r \in \mathbb{Q} \,|\, \text{there is an odd integer } m \text{ such that } mr \in \mathbb{N} \,\},$$

all those rational numbers whose denominator is odd. Then $2 \in R$ is not a unit so that R is not a field. If $r = a/b \in R$ then

$$r = u2^k,$$

where k is non-negative

$$u = c/d,$$

where c and d are odd integers. Thus

$$d/c \in R,$$

is the inverse of u so that u is a unit. It is clear that 2 is irreducible and so 2 is the only irreducible element of R. Thus every element of R can be factored into irreducibles and it is clear that this factorisation is unique up to associates.

8. (10pts) Give an example of an integral domain such that every element of R can be factored into irreducibles and yet R is not a UFD.

Solution: Let

$$R = \mathbb{Z}[\sqrt{-5}] = \{\, a + b\sqrt{5}i \,|\, a, b \in \mathbb{Z} \,\}.$$

Then R is an integral domain as it is a subring of $\mathbb{C}$, a field. Given $\alpha = a + b\sqrt{-5}$ let $N(\alpha) = a^2 + 5b^2$, the norm of α.

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Note that α is a unit if and only if $N(\alpha) = 1$ in which case $\alpha = \pm 1$.
Let $\alpha = a + b\sqrt{-5}$ be a non-zero element of R which is not a unit. We show that α can be factored into irreducibles by induction on $N(\alpha)$. If α is irreducible then there is nothing to prove.
Otherwise it factors as $\beta\gamma$, where neither β nor γ is a unit. As

$$1 < N(\alpha) = N(\beta)N(\gamma).$$

As neither β nor γ is a unit, we must $N(\beta)$ and $N(\gamma) > 1$. Hence $N(\beta)$, $N(\gamma) < N(\alpha)$. By induction both β and γ are products of irreducibles, so that α is a product of irreducibles.
Consider $6 \in \mathbb{Z} \subset R$. Then

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Now

$$N(2) = 4, \quad N(3) = 9, \quad N(1 + \sqrt{-5}) = 6, \quad \text{and} \quad N(1 - 1\sqrt{-5}) = 6.$$

Note that there are no elements of norm 2. Suppose that 2 is not irreducible in R. Then it is product of two elements of norm 2, a contradiction. Thus 2 is irreducible in R and it divides

$$(1 + \sqrt{-5})(1 - \sqrt{-5}).$$

But it doesn't divide either factor as 6 is not divisible by 4. Thus 2 is irreducible but not prime.

9. (15pts) (i) Show that $\mathbb{Z}[i]$ is a Euclidean domain.

Solution: Let $R = \mathbb{Z}[i]$.
Define a function

$$d\colon R - \{0\} \longrightarrow \mathbb{N} \qquad \text{by the rule} \qquad d(a+bi) = a^2 + b^2.$$

Suppose that α and $\beta \in R$. As d is nothing more than the square of the distance to the origin, we have $d(\alpha\beta) = d(\alpha)d(\beta)$.
Now let $\gamma = \frac{\alpha}{\beta} \in \mathbb{Q}[i] \subset \mathbb{C}$. Given γ we can find $q \in R$ such that if $s = q - \gamma$ then

$$|s| < 1.$$

Let $r = s\beta \in R$. Then

$$d(r) = d(\beta)|s| < d(\beta).$$

Thus $\alpha = q\beta + r$, either $r = 0$ or $d(r) < d(\beta)$
Thus R is a Euclidean domain.

(ii) Is $6 - i$ prime in $\mathbb{Z}[i]$?

Solution:
Suppose that $6 - i = \alpha\beta$. As $N(6-i) = 37$, which is prime, possibly reordering, we may assume that $N(\alpha) = a^2 + b^2 = 1$. But then $\alpha = \pm 1$, $\pm i$ is a unit. Thus $6 - i$ is irreducible so that it must be prime as R is a UFD.

10. (10pts) Write down all irreducible polynomials of degree 2 over the field $\mathbb{F}_5$.

Solution:
It suffices to write down all monic irreducible quadratic polynomial, as the other irreducible quadratic polynomials are given by multiplying through by one of 2, 3, or 4.
Let $f(x) = x^2 + ax + b$ be a monic quadratic polynomial over $\mathbb{F}_5$. Then f is irreducible if and only if f has no roots. 0 is a root if and only if $b = 0$. 1 is a root if and only if $1 + a + b = 0$. 2 is a root if and only if $2a + b = 1$. 3 is a root if and only if $3a + b = 1$. 4 is a root if and only if $a = 1 + b$.
If $a = 0$, then $b \neq -1$, 1, 1 and -1. If $a = 1$, then $b \neq -2$, -1, -2, 0. If $a = 2$, then $b \neq 2$, 2, 0, 1. If $a = 3$, then $b \neq 1$, 0, 2, 1. If $a = 4$, then $b \neq 0$, 3, 4, 3.
Thus

$$x^2 + 2, \quad x^2 + 3, \quad x^2 + x + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 3,$$
$$x^2 + 2x + 4, \quad x^2 + 3x + 3, \quad x^2 + 3x + 4, \quad x^2 + 4x + 1, \quad x^2 + 4x + 2.$$

are the irreducible monic quadratics.

11. (25pts) (i) State Gauss' Lemma and Eisenstein's criteria.

Solution: Let R be an integral domain and let F be its field of fractions. Suppose that $f(x) \in R[x]$. If $f = u_1 v_1$, where u_1 and $v_1 \in F[x]$ then we may find polynomials u, $v \in R[x]$ of the same degrees, such that $f = uv$.
Let $f \in \mathbb{Z}[x]$. If every coefficient of f, except the leading coefficient, is divisible by p and the constant term is not divisible by p^2, then $f \in \mathbb{Q}[x]$ is irreducible.
(ii) Show that the polynomial $1 + x^3 + x^6 \in \mathbb{Q}[x]$ is irreducible (**Hint: try a substitution**.)

Solution: Let $t = x^3$. It is clearly enough to show that

$$1 = x^3 + x^6 = 1 + t + t^2 \in \mathbb{Q}[t],$$

is irreducible. Note that

$$1 + t + t^2 = \frac{t^3 - 1}{t - 1}.$$

Consider the change of variable $s = t - 1$. Then

$$1 + t + t^2 = \frac{(s+1)^3 - 1}{s} = s^2 + 3s + 3.$$

By Eisenstein, applied to the prime 3, $s^2 + 3s + 3$ is irreducible over $\mathbb{Z}$. But then $1 + x^3 + x^6$ is irreducible over $\mathbb{Z}$, so that $1 + x^3 + x^6$ is irreducible over $\mathbb{Q}$ by Gauss' Lemma.

(iii) Show that the polynomial $1 - t^2 + t^5$ is irreducible over $\mathbb{Q}$ (**Hint: consider the ring $\mathbb{F}_2[t]$.**)

Solution:
By Gauss' Lemma it is enough to show that $f = 1-x^2+x^5$ is irreducible over $\mathbb{Z}$. Suppose not, suppose that f factors as gh, where g and $h \in \mathbb{Z}[x]$ are not units (that is, not ± 1). As the content of f is one, it follows that g and h have degree at least one.
The natural ring homomorphism

$$\mathbb{Z} \longrightarrow \mathbb{Z}_2$$

induces a ring homomorphism

$$\phi\colon \mathbb{Z}[x] \longrightarrow \mathbb{Z}_2[x].$$

Then $\phi(f) = \phi(g)\phi(h)$ is a factorisation of f into polynomials of degree at least one.
Therefore it suffices prove that $1 + x^2 + x^5$ is irreducible over $\mathbb{Z}_2$. $x^5 + x^2 + 1$ doesn't have any zeroes in the field $\mathbb{F}_2$ and so if $x^5 + x^2 + 1$ factors, it must factor as a product of an irreducible polynomial of degree 2 and an irreducible polynomial of degree 3. The only irreducible polynomial of degree two is $x^2 + x + 1$, since the other two $x^2 + x$ and $x^2 + 1$ have a zero. The only irreducible polynomials of degree three are $x^3 + x + 1$ and $x^3 + x^2 + 1$, since these are the only ones which don't have a zero. As

$$(x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1,$$

and

$$(x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1,$$

it follows that $x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ is irreducible, so that $f = 1 - x^2 + x^5$ is irreducible over $\mathbb{Q}$.