Math 122 Midterm 2 Fall 2014

Instructions

- Due: Wednesday, Dec 3, by noon (class time).
- You may use your class notes, my class notes, your past homework, homework solutions, and midterm solutions. But do not ask for help (or look for answers) on stack exchange, on math overflow, or on any other online source.
- All collaboration and writing policies in the syllabus apply.
- You may collaborate on Problems 1 - 6. You may not collaborate on the rest: Problems 7 - 12. The seemingly difficult problems are loads of fun to solve, so I encourage you to persist.
- Start early. Think deeply. Have fun.

1. Irreducibility

Let F be a field. For any $x \in F$, note that there is a function

$$F[t] \to F,$$

called *evaluation at* x. Explicitly, if $f = a_d t^d + \dots a_1 t + a_0$ is a polynomial, we send f to

$$f(x) = a_d x^d + \dots a_1 x + a_0 \in F.$$

Here, by x^d, we mean of course the element of F obtained by multiplying x with itself d times.

(a) Show that for any $x \in F$, evaluation at x is a ring homomorphism.

(b) Show that f can be factored by a linear polynomial if and only if there is some $x \in F$ for which $f(x) = 0$. (Hint: Use the division algorithm and induct on degree.)

Recall that a polynomial $f(t) \in F[t]$ is *irreducible* if the only polynomials dividing $f(t)$ are degree 0 (i.e., are constants) or have degree equal to f.

(c) If $F = \mathbb{C}$, show that $f(t) = t^2 + 1$ is not irreducible.

(d) If $F = \mathbb{R}$, show that $f(t) = t^2 + 1$ *is* irreducible. (Hint: If $f(t) = g(t)h(t)$, what can you say about the degrees of g and h? And what does that say about solutions to $f(t)$?)

(e) For each of the primes $p = 2, 3, 5, 7$, indicate which of the following polynomials has a solution in $\mathbb{Z}/p\mathbb{Z}$. (You'll need to just compute.)
   (a) $t^2 + \overline{1}$ (i.e., which of these finite fields has a square root to -1?)
   (b) $t^3 - \overline{2}$ (i.e., which of these fields has a cube root to 2?)
   (c) $t^2 + t + 1$ (i.e., for which of these fields does this polynomial factor?)

2. Principal ideal domains

Let R be an integral domain. We call R a *principal ideal domain* if every ideal $I \subset R$ is equal to (x) for some $x \in R$. That is, every ideal is generated by a single element.

(a) Show that $\mathbb{Z}$ is a principal ideal domain. (We've done this in class, so you can do it, too!)
(b) Let F be a field. Show that $F[t]$ is a principal ideal domain. (Hint: If $I \neq (0)$, let n be the least degree for which a degree n polynomial is in I. If $p(t)$ and $q(t)$ are both degree n polynomials, how are they related? Finally, given any $f(t) \in I$, what happens when you divide $f(t)$ by $p(t)$ and look at the remainder?)

3. The second isomorphism theorem

Fix a group G. Let $S \subset G$ be a subgroup, and $N \triangleleft G$ be a normal subgroup.

(a) Let SN be the set of all elements in G of the form sx where $s \in S$ and $x \in N$. Show this is a subgroup of G.
(b) Show that N is a normal subgroup of SN.
(c) Show that $S \cap N$ is a normal subgroup of S.
(d) Exhibit an isomorphism between $S/(S \cap N)$ and SN/N. (Hint: Does the equivalence class $[s]$ in the former group define an equivalence class $[sn]$ in the latter group? Does the n in $[sn]$ matter?)

4. Subgroups descend to quotient groups

Let G be an arbitrary group, and $H \triangleleft G$.

(a) Show that there is a bijection between the set of subgroups in G containing H, and the set of subgroups in G/H.
(b) Show that there is a bijection between the set of *normal* subgroups in G containing H, and the set of normal subgroups in G/H. (This time, this isn't extra credit.)

5. Solvable groups

A group G is called *solvable* if there exists a finite sequence of subgroups

$$1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

such that for all $i \geq 0$, $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is abelian.

(a) Show that any abelian group is solvable. (If this seems trivial, it's because it is.)
(b) Show any group of order pq, where p and q are distinct primes, is solvable.

(c) Show that if G is simple and non-abelian, G cannot be solvable.

The following is a great application of the isomorphism theorems, and of the previous problem.

(d) Show that if G is solvable, so is any subgroup of G.

(e) Show that if G is solvable, and $K \subset G$ is normal, then G/K is solvable.

6. $GL_n(\mathbb{F}_q)$

Let $\mathbb{F}_q$ be a finite field with q elements.

(a) Let $V = \mathbb{F}_q^n = \mathbb{F}_q^{\oplus n}$ be an n-dimensional vector space over $\mathbb{F}_q$. Show that $G = GL_n(\mathbb{F}_q)$ acts *transitively* on $V - \{0\}$. (That is, show that for any pair $x, y \in V$, there is some group element g so that $gx = y$.)

(b) Prove that $G = GL_n(\mathbb{F}_q)$ has

$$\left(\prod_{k=1}^{n}(q^k - 1)\right)\left(\prod_{k=1}^{n-1} q^k\right)$$

elements in it. (You can either count intelligently, or apply the orbit-stabilizer theorem inductively. Either way, use matrices.)

(c) Show that $GL_n(\mathbb{F}_q)$ has a normal subgroup of index $q - 1$. (Hint: The determinant is still a group homomorphism.)

(d) Consider $G = GL_2(\mathbb{F}_q)$. Assume p is the unique prime number dividing q. [1] Show that $|\operatorname{Syl}_p(G)|$ cannot equal 1. (Try thinking about upper-triangular and lower-triangular matrices, then think about special cases of them.)

(e) How many elements of order 3 are in $GL_2(\mathbb{F}_3)$? (You may want to start by determining the number of Sylow 3-subgroups. Either way, dig in.)

No more collaboration

7. Ring homomorphisms

(a) Show that a composition of two ring homomorphisms is a ring homomorphism.

(b) For a ring R, let $M_{k\times k}(R)$ denote the ring of $k \times k$ matrices with entries in R. Specifically, if (a_{ij}) is a matrix whose i, jth entry is a_{ij}, we define

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}), \qquad (a_{ij})(b_{ij}) = (\sum_{l=l}^{k} a_{il}b_{lj}).$$

[1] One can prove that any finite field has size p^k for some prime p. As pointed out to me by Kevin, it's not hard—a finite field of characteristic p is a module over $\mathbb{Z}/p\mathbb{Z}$, so is a finite-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. But how many elements must such a set have?

Show that if $f : R \to S$ is a ring homomorphism, then the function

$$F : M_{k\times k}(R) \to M_{k\times k}(S), \qquad (a_{ij}) \mapsto (f(a_{ij}))$$

is a ring homomorphism.

(c) Prove that

$$f(\det A) = \det(F(A)).$$

You may want to start by proving it for $k = 1$, then perform induction using the cofactor definition of determinants.

8. Invertible matrices

Let S be a ring. We say $x \in S$ is a *unit* if there is a multiplicative inverse to x—i.e., an element $y \in S$ so that $xy = yx = 1_S$. As an example, if S is the ring of $k \times k$ matrices in some ring R, then a matrix is invertible if and only if it is a unit.

(a) Determine which of the following matrices is a unit in $M_{k\times k}(\mathbb{Z})$:

$$\begin{pmatrix} 2 & 5 \\ 4 & 4 \end{pmatrix} \qquad \begin{pmatrix} 2 & 5 \\ 9 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 4 \\ 5 & 6 & 7 \end{pmatrix}$$

(b) For the primes $p = 2, 3, 5$, consider the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ sending $a \mapsto \overline{a}$. This induces a ring homomorphism $M_{k\times k}(\mathbb{Z}) \to M_{k\times k}(\mathbb{Z}/p\mathbb{Z})$ by the previous problem. Determine which of the matrices above is sent to a unit for each choice of $p = 2, 3, 5$.

9. Bases

Let $M = \mathbb{Z}/n\mathbb{Z}$.

(a) Show that M admits no basis as a module over $\mathbb{Z}$.

(b) Show that M admits a basis as a module over the ring $R = \mathbb{Z}/n\mathbb{Z}$.

10. Ideals are like normal subgroups

Let R be a commutative ring. Show that $I \subset R$ is an ideal if and only if it is the kernel of some ring homomorphism. (The kernel of a ring homomorphism $R \to S$ is the set of all elements sent to $0 \in S$.)

11. Characteristic

Let F be a field, and $1 \in F$ the multiplicative identity. The *characteristic* of F is the smallest integer n with $n \geq 1$ such that

$$1 + \ldots + 1 = 0$$

where the summation has n terms in it. For instance, the characteristic of $\mathbb{Z}/p\mathbb{Z}$ is p. If F is a field where $1 + \ldots + 1$ never equals 0 (like $\mathbb{R}, \mathbb{Q}, \mathbb{C}$) we say that F has *characteristic zero*.

Prove that any field (finite or not!) must have either characteristic zero, or characteristic p for some prime number p.

(By the way, there are in fact infinite fields of finite characteristic.)

12. Solvability of S_n.

(a) For $n \geq 3$, show that any cycle of length 3 is in A_n.
(b) Show by example that A_n is not abelian for $n \geq 4$.
(c) Assume A_n is simple for $n \geq 5$. (This is a theorem we stated, but never proved.) Explain why S_n is not solvable for any $n \geq 5$.
(d) Show that S_n is solvable for $n \leq 3$. So all that remains is S_4.
(e) Prove that S_4 is solvable. (One way: You can exhibit an abelian subgroup of order 4 in A_4.)