Practice Problems for Second Midterm Exam
Modern Algebra, Dave Bayer, March 29, 1999

This first set of problems are collected from various materials already posted on the web.

[1] Working in the Gaussian integers \( \mathbb{Z}[i] \), factor 2 into primes.

[2] Let \( a = 3 - i \) and \( b = 2i \) be elements of the Gaussian integers \( \mathbb{Z}[i] \).
(a) Find \( q_1, c \in \mathbb{Z}[i] \) so \( a = q_1 b + c \) with \( |c| < |b| \).
(b) Now find \( q_2, d \in \mathbb{Z}[i] \) so \( b = q_2 c + d \) with \( |d| < |c| \).
(c) Express \( (a, b) \subset \mathbb{Z}[i] \) as a principal ideal.

[3] The ideal \( I = (2, 1+3i) \subset \mathbb{Z}[i] \) is principal, where \( \mathbb{Z}[i] \) are the Gaussian integers. Find a single generator for \( I \). (Repeat for \( I = (3, 1+i) \), and \( I = (6, 3+5i) \).)

[4]
(a) Prove that every positive integer can be uniquely factored into primes, up to the order of the primes.
(b) How do you need to modify this proof so it works for a polynomial ring in one variable over a field?

[5] Let \( R \) be a principal ideal domain, and let
\[
I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots
\]
be an infinite ascending chain of ideals in \( R \). Show that this chain stabilizes, i.e.
\[
I_N = I_{N+1} = I_{N+2} = \cdots
\]
for some \( N \).

[6] Prove the Eisenstein criterion for irreducibility: Let \( f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \), and let \( p \) be a prime. If \( p \) doesn’t divide \( a_n \), \( p \) does divide \( a_{n-1}, \ldots, a_0 \), but \( p^2 \) doesn’t divide \( a_0 \), then \( f(x) \) is irreducible as a polynomial in \( \mathbb{Q}[x] \).
(a) First, what does \( f(x) \) look like mod \( p \)?
(b) Now, suppose that there is a nontrivial factorization \( f(x) = g(x)h(x) \) in \( \mathbb{Z}[x] \). What do \( g(x) \) and \( h(x) \) look like mod \( p \)? What would this imply about \( a_0 \)?

[7] Prove that \( f(x) = x^{p-1} + \ldots + x + 1 \) is irreducible when \( p \) is prime:
(a) Show that \( (x-1) f(x) = x^p - 1 \).
(b) Now set \( x = y + 1 \), so \( (x-1) f(x) = y f(y+1) = (y+1)^p - 1 \). Study the binomial coefficients in the expansion of \( (y+1)^p \), and apply the Eisenstein criterion to \( f(y+1) \).

[8] Show that the following polynomials in \( \mathbb{Z}[x] \) cannot be factored:
(a) \( x^3 + 6x^2 + 9x + 12 \)
(b) \( x^2 + x + 6 \)

[9] Let \( A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 8 & 8 & 8 \end{bmatrix} \). Reduce \( A \) to diagonal form, using row and column operations.

[10] Let \( G \) be the Abelian group \( G = \langle a, b, c \mid a^2 b^2 c^2 = a^2 b^2 = a^2 c^2 = 1 \rangle \). Express \( G \) as a product of free and cyclic groups.

[11] Let \( G \) be the Abelian group \( G = \langle a, b, c \mid b^2 c^2 = a^6 b^6 c^6 = a^6 b^4 c^4 = 1 \rangle \). Express \( G \) as a product of free and cyclic groups.

[12] Let \( R = k[x_1, \ldots, x_n] \) be the polynomial ring in \( x_1, \ldots, x_n \) over a field \( k \), and let \( f_1, \ldots, f_m \) be \( m \) polynomials in \( R \). Let \( R^m \) be the free \( R \)-module \( R^m = \{ (g_1, \ldots, g_m) \mid g_i \in R \text{ for } 1 \leq i \leq m \} \). Let \( M \subset R^m \) be the subset of syzygies \( M = \{ (g_1, \ldots, g_m) \mid g_1 f_1 + \ldots + g_m f_m = 0 \} \).
(a) Show that \( M \) is an \( R \)-module.
(b) Let \( R = \mathbb{Q}[x, y] \), \( m = 3 \), and \( f_1 = x^2 \), \( f_2 = xy \), \( f_3 = y^2 \). Find a set of generators for \( M \subset R^3 \).

[13] Show that every element of \( \mathbb{F}_{25} \) is a root of the polynomial \( x^{25} - x \).

[14] What is the minimal polynomial of \( \alpha = \sqrt{2} + \sqrt{3} \) over \( \mathbb{Q} \)?

This second set of problems are new, but are predicted by our assignments.

[15] Let \( F \) be a field, and let \( f(x) \) be a polynomial of degree \( n \) with coefficients in \( F \). Prove that \( f(x) \) has at most \( n \) roots in \( F \).

[16] Let \( f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \) be an integer polynomial, and let \( p \) be a prime integer which doesn’t divide \( a_n \). Prove that if the remainder \( \overline{f(x)} \) of \( f(x) \) mod \( p \) is irreducible, then \( f(x) \) is irreducible.

[17] Let \( F \) be a field of characteristic \( \neq 2 \), and let \( K \) be an extension of \( F \) of degree 2. Prove that \( K \) can be obtained by adjoining a square root: \( K = F(\delta) \), where \( \delta^2 = D \) is an element of \( F \).

[18] Let \( F \subset K \) be a finite extension of fields. Define the degree symbol \( [K : F] \).

[19] Let \( F \subset K \subset L \) be a tower of finite field extensions. Prove that \( [L : F] = [L : K][K : F] \).

[20] Consider the module \( M = F[x]/((x - 2)^3) \) over the ring \( R = F[x] \) for a field \( F \).
(a) What is the dimension of \( M \) as an \( F \)-vector space?
(b) Find a basis for \( M \) as an \( F \)-vector space, for which the matrix representing multiplication by \( x \) is in Jordan canonical form.