Practice problems for second midterm

midterm to be held Wednesday, April 8, in class

Dave Bayer, Modern Algebra

We will have a problem session in preparation for this midterm:

- Monday, April 6, 8:00pm - 10:00pm, 507 Mathematics

[**1**] 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?

[**2**] 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 $(x-1)f(x) = yf(y+1) = (y+1)^p - 1$. Study the binomial coefficients in the expansion of $(y+1)^p$, and apply the Eisenstein criterion to $f(y+1)$.

[**3**] Let p be a prime so $p-1$ is not a power of 2. Prove that the p-gon is not constructible:

(a) Let $\theta = 2\pi/p$, and let $z = \cos\theta + i\sin\theta$. Explain why, if $\cos\theta$ and $\sin\theta$ are constructible, then the degree of z over $\mathbb{Q}$ is a power of 2.

(b) Show that z is a root of $x^p - 1$ but not $x - 1$, so z is a root of the irreducible polynomial $f(x) = x^{p-1} + \ldots + x + 1$. Thus, the degree of z over $\mathbb{Q}$ is not a power of 2.

[**4**] Show that the set of constuctible numbers form a field.

[**5**] Prove that the cube root of 5 is not a constructible number.

[**6**] Show *algebraically* that it is possible to construct an angle of 30°.

[**7**] 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.

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

[9] 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 $M \subset R^3$.

[10] Suppose that the complex number α belongs to an extension K of $\mathbb{Q}$ of degree 9, and an extension L of $\mathbb{Q}$ of degree 12, but not to $\mathbb{Q}$ itself. What is the degree of α over $\mathbb{Q}$?

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

[12] Give a presentation of $\mathbb{F}_9$ of the form $\mathbb{F}_3[x]/(f(x))$. In terms of this presentation, find a generator α of the multiplicative group $\mathbb{F}_9^*$, i.e. an element of multiplicative order $9 - 1 = 8$.