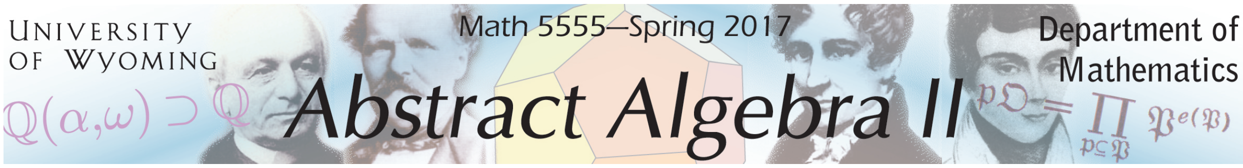

HW1 Due Friday 10 March, 2017

Instructions. Answer any three problems. You may use any available software (including Maple) to simplify labor, as long as you understand what you are doing.

---

1. Let F be an arbitrary field, and let $R = F[\varepsilon]$ be the ring of all formal expressions of the form $a+b\varepsilon$ for $a, b \in F$ satisfying $\varepsilon^2 = 0$; thus addition and multiplication in R are defined by

$$(a+b\varepsilon) + (c+d\varepsilon) = (a+c) + (b+d)\varepsilon;$$
$$(a+b\varepsilon)(c+d\varepsilon) = ac + (ad+bc)\varepsilon.$$

(We think of ε as a sort of first-order infinitesmal, whose square is a second-order infinitesmal of size negligible compared to constant and first-order terms.) Show that R has a unique maximal ideal (ε) and that $R/(\varepsilon) \cong F$. (The ring R is sometimes called the ring of *ideal numbers* over F, and may be denoted $R = F[\varepsilon]$.)

2. Let F be an arbitrary field, and let $f(X) \in F[X]$ be a polynomial of degree 2. Show that the quotient ring $R = F[X]/(f(X))$ is isomorphic to one of the following:
   (i) $F \oplus F$; or
   (ii) a field which is a quadratic extension of F; or
   (iii) the ring $F[\varepsilon]$ described in Question 1.

3. For each of the following polynomials $f(x) \in \mathbb{Q}[x]$, determine the splitting field $E \supseteq \mathbb{Q}$ of $f(x)$; the Galois group $G = G(E/\mathbb{Q})$; the subgroups of G and the subfields of E; and the explicit Galois correspondence between subgroups and subfields.
   (a) $f(x) = x^4 + 14x^2 + 9$
   (b) $f(x) = x^4 - 4x^2 + 2$

4. Compute each of the following to within 0.001 with respect to the appropriate p-adic norm $\|\ \|_p$, or indicate why there is no solution:
   (a) the zeroes of X^2+X+1 in $\mathbb{Q}_2$;
   (b) the zeroes of X^2+X+1 in $\mathbb{Q}_3$;
   (c) the zeroes of X^2+X+1 in $\mathbb{Q}_5$;
   (d) the zeroes of X^2+X+1 in $\mathbb{Q}_7$.

5. Determine the Galois group G of the extension $E = \mathbb{Q}[\zeta] \supset \mathbb{Q}$ where $\zeta = e^{\pi i/6}$ is a primitive complex 12th root of unity. Explicitly describe the Galois correspondence between subfields of E and subgroups of G.

6. **Newton's Method.** Let F be a field with a non-Archimedean norm $\|\cdot\|$, and consider the subring $\mathcal{O} = \{x \in F : \|x\| \leqslant 1\}$. Let $f(X) = a_0 + a_1 X + \cdots + a_d X^d \in \mathcal{O}[X]$. (We may assume that $a_d \neq 0$.) Suppose that $\alpha_0 \in \mathcal{O}$ is an approximate zero of $f(X)$ in the sense that $\|f(\alpha_0)\| < \|f'(\alpha_0)\|^2$. (Here $f'(X) = \sum_i i a_i X^{i-1}$ as usual.)

   (a) Define $\alpha_1 = \alpha_0 - \frac{f(\alpha_0)}{f'(\alpha_0)}$. Show that $\|f(\alpha_1)\| < \|f(\alpha_0)\|$.

   (b) Define the sequence $\alpha_0, \alpha_1, \alpha_2, \ldots \in \mathcal{O}$ recursively by $\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$. Show that

   $$\|f(\alpha_{n+1})\| \leq \frac{\|f(\alpha_n)\|^2}{\|f'(\alpha_0)\|^2}$$

   for all $n \geq 0$.

   (c) Show that the sequence $\alpha_0, \alpha_1, \alpha_2, \ldots$ is a Cauchy sequence, converging to a zero of $f(X)$ in $\mathcal{O}$. [Note that by (b) this convergence is quadratic.]

   Hint: Show that $f(X+\delta) = f(X) + \delta f'(X) + \delta^2 b(X)$ for all $\delta \in \mathcal{O}$, where the polynomial $b(X) \in \mathcal{O}[X]$ depends on f and δ. Evaluate at $\delta = -f(\alpha_0)/f'(\alpha_0)$ and $X = \alpha_0$ to obtain (a). The derivative of the previous expression yields $f'(X+\delta) = f'(X) + \delta g(X)$ for some $g(X) \in \mathcal{O}[X]$ depending on f and δ. Now evaluate at $\delta = -f(\alpha_n)/f'(\alpha_n)$ and $X = \alpha_n$ to show inductively that $\|f'(\alpha_n)\| = \|f'(\alpha_0)\|$ and that the bound in (b) holds.

7. Determine the minimal polynomial of each of the following numbers over $\mathbb{Q}$:

   (a) $\alpha + \alpha^2$ where $\alpha = 2^{1/3}$, the real cube root of 2;

   (b) $\sqrt{2} + \sqrt{3} + \sqrt{5}$;

   (c) $\sin \frac{2\pi}{7}$.