NEPAL ALGEBRA PROJECT 2017
MODULE 2 — HOMEWORK #1: SOLUTIONS
WEDNESDAY, 24 MAY, 2017

ROGER AND SYLVIA WIEGAND

1. Milne, Exercise 1-1 (p. 25)

The systematic approach would be to use the Division Algorithm for the first part and the Euclidean Algorithm for the second part, but often it's easier just to try a few things and see what happens. Here goes: For the first problem, we have

$$(\alpha^2+\alpha+1)(\alpha^2-\alpha) = \alpha^4-\alpha = \alpha(\alpha^3-\alpha^2+\alpha+2)+\alpha^3-\alpha^2-3\alpha = (\alpha^3-\alpha^2+\alpha+2)-4\alpha-2\,,$$

so the answer is $-4\alpha-2$. For the second problem, we have

$$(\alpha-1)\alpha^2 = \alpha^3-\alpha^2 = -\alpha-2\,, \quad \text{and hence}$$
$$(\alpha-1)(\alpha^2+1) = (-\alpha-2)+(\alpha-1) = -3\,.$$

Therefore $(\alpha-1)^{-1} = -\frac{1}{3}\alpha^2 - \frac{1}{3}$. Let's check:

$$-\frac{1}{3}(\alpha^2+1)(\alpha-1) = -\frac{1}{3}(\alpha^3-\alpha^2+\alpha-1) = -\frac{1}{3}(-3) = 1\,.$$

Hurray!

2. Milne, Exercise 1-2 (p. 25)

Since $\sqrt{2}$ is irrational and is a root of X^2-2, we know that X^2-2 is the minimimal polynomial. Therefore $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. Next let's show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Assuming the contrary, we have $\sqrt{3} = a + b\sqrt{2}$ for suitable rational numbers a and b. Squaring both sides, we get $3 = a^2 + 2ab\sqrt{2} + 2b^2$, whence

$$2ab\sqrt{2} = 3 - a^2 - 2b^2\,.$$

This equation and the fact that $\sqrt{\frac{3}{2}}$ and $\sqrt{2}$ are irrational show that both a and b are non-zero. Thus we have

$$\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}\,,$$

contradiction. We have shown that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Since $\sqrt{3}$ is a root of $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$, it follows that $[Q(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$. By mulitplicativity of degrees, $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 2 \cdot 2 = 4$.

3. Milne, Exercise 1-5 (p. 25).

A picture showing degrees is helpful, but I won't even try to make a LaTeX picture. Please follow along with your own picture. Choose a field K containing E and also containing a root α of $f(X)$. Then $[F(\alpha):F] = n$. Let $\ell = [E(\alpha):E]$. Since α is a root of $f(X) \in E[X]$, the minimum polynomial $g(X) \in E[X]$ of α over E is a divisor of $f(X)$, whence $\ell = \deg(g) \leq n$. From your picture and multiplicativity of degrees, we see that $n \cdot [E(\alpha):F(\alpha)] = [E(\alpha):F] = m\ell$. In particular, $n \mid m\ell$. Since n and m are relatively prime, it follows that $n \mid \ell$. We already know that $\ell \leq n$, so in fact $\ell = n$. Therefore $f(X)$ and $g(X)$ have the same degree; since $g(X) \mid f(X)$ we have $f(X) = cg(X)$ for some non-zero constant c. Since $g(X)$ is irreducible over E, so is $f(X)$.

Remark: This illustrates a powerful method of showing that a polynomial $f(X) \in E[X]$ is irreducible: Adjoin a root α of $f(X)$ and show (somehow) that $[E(\alpha) : E] = \deg(f)$.

4. Milne, Exercise 2-1 (p. 33)

(a) Obviously $F^{\times 2} \subseteq S(E) \subseteq F^{\times}$. To show that $S(E)$ is a subgroup of $F^{\times}$, let $\alpha, \beta \in S(E)$ and choose $\gamma, \delta \in E$ such that $\gamma^2 = \alpha$ and $\delta^2 = \beta$. Then $(\gamma\delta)^2 = \alpha\beta$. This shows that $\alpha\beta \in S(E)$. Also, we have $(\gamma^{-1})^2 = \gamma^{-2} = (\gamma^2)^{-1} = \alpha^{-1}$, so $\alpha^{-1} \in S(E)$. (The hypotheses that $[E : F] = 2$ and $\text{char}(F) \neq 2$ are irrelevant to this part.)

(b) "if": Choose $\alpha \in E \setminus F$ with minimum polynomial $X^2 + aX + b \in F[X]$. Then $\alpha = \frac{-a \pm \sqrt{a^2-4b}}{2}$, and clearly $E = F(\gamma)$, where $\gamma = \sqrt{a^2 - 4b}$. (The Quadratic Formula works whenever the characteristic is different from two; a consequence is that every extension of degree 2 is obtained by adjoining a square root.) Put $c = \gamma^2 \in S(E)$. Then $X^2 - c$ is the minimal polynomial of γ. Since $c \in S(E)$ we know $c \in S(E')$, so there is an element $\gamma' \in E'$ with $(\gamma')^2 = c$. Since c is not a square in F, $\gamma' \notin F$, so $E' = F(\gamma')$. Moreover γ and γ' have the same minimum polynomial over f (namely, $X^2 - c$), so there's a uinque F-isomorphism $E = F(\gamma) \to F(\gamma') = E'$ taking γ to γ'.

"only if": Let $p \in S(E)$. Choose $q \in E$ such that $q^2 = p$. Then $(\varphi(q))^2 = \varphi(q^2) = \varphi(p) = p$, so $p \in S(E')$. This shows that $S(E) \subseteq S(E')$, and the reverse inclusion holds by symmetry.

(c) List the prime numbers: $p_1, p_2, p_3, \ldots$, and let $E_i = \mathbb{Q}(\sqrt{p_i})$. Then $p_i \in S(E_i)$ for each i. A slight modification of the argument used in Problem 2 (Milne, Exercise 1.2) shows that $p_i \notin S(E_j)$ if $i \neq j$. Now apply (b).

(d) Let $F = \mathbb{Z}/p\mathbb{Z}$, the prime field of order p. Now $F^{\times}$ is a (cyclic) group of even order, so it has an element of order 2. This means that the group homomorphism $\sigma : F^{\times} \to F^{\times}$ taking g to g^2 has non-trivial kernel. Thus this homomorphism is not injective and therefore not surjective. In other words, there's an element $a \in F^{\times} \setminus (F^{\times})^2$. Then $[F(\sqrt{2}) : F] = 2$, and hence $F(\sqrt{2})$ is a field of order p^2. This proves the existence of fields of order p^2.

For uniqueness, we suppose E is any field of order p^2. Then $[E : F] = 2$, and by the Quadratic Formula we have $E = F(\sqrt{b})$ for some $b \in F^{\times} \setminus (F^{\times})^2$. Now we use the fact that $F^{\times}$ is cyclic, so that there is a *unique* element of order two. This means that $(F^{\times})^2$, which is the image of the homomorphism σ above, has index 2 in $F^{\times}$. Therefore the only subgroup of $F^{\times}$ properly containing $(F^{\times})^2$ is $F^{\times}$ itself. Since $b \in S(E) \setminus (F^{\times})^2$, $S(E)$ contains $(F^{\times})^2$ *properly* and hence must be all of $F^{\times}$. Now apply (b).

5. Milne, Exercise 2.2 (p. 33)

Let α be a root of $f(X) = X^p - X - a$ in some extension field K. Notice that $f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a = \alpha^p + 1 - \alpha - 1 - a = f(\alpha) = 0$. Thus $\alpha, \alpha + 1, \ldots \alpha + p - 1$ are all roots of $f(X)$ in K. Therefore $f(X)$ factors as follows:

$$f(X) = (X - \alpha)(X - (\alpha + 1)) \cdots (X - (\alpha + p - 1)) \quad \text{in} \quad K[X]\,.$$

Now suppose $f(X) = g(X)h(X)$ in $F[X]$, where g and h are monic with positive degrees r and s, respectively. By unique factorization in $K[X]$, $g(X)$ has to be a product of r of the linear factors displayed above. The coefficient of X^{r-1} in $g(X)$ is the negative of the sum of the roots, that is, $-((\alpha+c_1)+(\alpha+c_2)+\cdots+(\alpha+c_r))$, where $c_1,\ldots,c_r$ are distinct elements of the prime field. This coefficient, which must be in F, is $-r\alpha-(c_1+\cdots+c_r)$. Since the c_i are in the prime field and since r is a non-zero element of the prime field, it follows that $\alpha \in F$. Therefore all roots of $f(X)$ are in F, and F splits into the product of p distinct linear factors in $F[X]$. This proves (a). For (b), Gauss's Lemma shows that if $f(X) = X^p - X - 1$ factors in $\mathbb{Q}[x]$, then it factors in $\mathbb{Z}[X]$, and hence in $(\mathbb{Z}/p\mathbb{Z})[X]$. By part (a) it splits into linear factors in $(\mathbb{Z}/p\mathbb{Z})[X]$ and, in particular, has a root $\beta \in \mathbb{Z}/p\mathbb{Z}$. But $\beta^p = \beta$ by Fermat's Theorem), so obviously $f(\beta) \neq 0$, contradiction.

6. Milne, Exercise 2.3 (p.33)

Let $\alpha = \sqrt[5]{2}$, and let $\zeta = e^{\frac{2\pi i}{5}}$, a primitive fifth root of one in $\mathbb{C}$. The roots of $X^5 - 2$ are $\alpha, \zeta\alpha, \zeta^2\alpha, \zeta^3\alpha$, and $\zeta^4\alpha$, so the splitting field is $K = \mathbb{Q}(\alpha,\zeta)$. Now $X^5 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein, so $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$. Also, ζ is a root of $g(X) = X^4 + X^3 + X^2 + X + 1$. By Eisenstein, $g(X+1)$ is irreducible over $\mathbb{Q}$, so $g(X)$ is also irreducible. (Any factorization of $g(X)$ would lead to a factorization of $g(X+1)$ by substituting.) Of course $[\mathbb{Q}(\alpha,\zeta) : \mathrm{Q}(\alpha)] \leq 4$, so $[K:\mathbb{Q}] \leq 20$. But $[K:\mathbb{Q}]$ has to be a multiple of both 4 and 5, so the degree is 20.

7. Milne, Exercise 2.6 (p.33)

Just apply Proposition 2.12 repeatedly, till the new polynomial is separable. (Sorry, no time for details.)

8. Find the splitting field, and its degree over $\mathbb{Q}$, for the polynomial $f(X) = X^4 + X^2 + 1 \in \mathbb{Q}[X]$. (Hint: Think about $(X^2-1)f(X)$.)

We have $(X^2-1)f(X) = X^6 - 1$. Let $\zeta = e^{\frac{2\pi i}{6}}$, a primitive sixth root of one in $\mathbb{C}$. The roots of $X^6 - 1$ are $1, \zeta, \zeta^2, \zeta^3 = -1, \zeta^4, \zeta^5$, so the roots of $f(X)$ are $\zeta, \zeta^2, \zeta^4, \zeta^5$, and the splitting field of $f(X)$ over $\mathbb{Q}$ is $\mathbb{Q}(\zeta)$. Since $\zeta^2 - \zeta + 1 = 0$, $[\mathbb{Q}(\zeta):\mathbb{Q}] = 2$.

9. Find an irreducible polynomial $f \in \mathbb{Q}[X]$, with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{C}$ such that

$$[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}] \neq [\mathbb{Q}(\alpha_3,\alpha_4):\mathbb{Q}]\,.$$

(In particular, the fields $\mathbb{Q}(\alpha_1,\alpha_2)$ and $\mathbb{Q}(\alpha_3,\alpha_4)$ are not isomorphic. The point of this exercise is to clarify the last sentence of Remark 2.9 (b), in Milne (on p. 30): We know that $\mathbb{Q}(\alpha_i) \cong \mathbb{Q}(\alpha_j)$ for all i, j, but adjoining *two* roots is very different.)

Let $f(X) = X^4 - 31$. It's irreducible by Eisenstein. The roots are $\pm\alpha$ and $\pm i\alpha$, where $\alpha = \sqrt[4]{31}$. We have $[\mathbb{Q}(\alpha,-\alpha):\mathbb{Q}] = 4$, but $[\mathbb{Q}(\alpha,i\alpha):\mathbb{Q}] = 8$. (Of course 31 could be replaced by your favorite prime number.)