NAP PROBLEM SET #2: SOLUTIONS

ROGER AND SYLVIA WIEGAND

1. Let G be an abelian group, and let m and n be positive integers.

(a) If G has an element of order n and $m \mid n$, prove that G has an element of order m.
(b) If G has an element x of order m and an element y of order n, and if m and n are relatively prime, prove that xy has order mn.
(c) If G has an element x of order m and an element y of order n, prove that G has an element whose order is the least common multiplie $\mathrm{LCM}(m,n)$. (You may use without proof the standard fact that $\mathrm{GCD}(m,n) \cdot \mathrm{LCM}(m,n) = mn$.)
(d) Assume G is finite and n is the maximum of orders of elements of G. (In other words there is an element x such that $\mathrm{o}(x) = n$, and $\mathrm{o}(y) \le n$ for every $y \in G$.) Prove that $g^n = 1$ for every $g \in G$.
(e) Conclude that the multiplicative group $\mathbb{F} \setminus \{0\}$ of a finite field $\mathbb{F}$ must be cyclic.

Solution: (a) Let $\mathrm{ord}(x) = n$, and write $n = rm$. Put $y = x^r$. Then $y^m = (x^r)^m = x^{rm} = x^n = 1$. Also, if $1 \le \ell < m$, then $1 \le r \le r\ell < rm = \mathrm{ord}(x)$, so $x^{r\ell} \ne 1$, that is, $y^\ell \ne 1$. Thus m is the least positive integer for which $y^m = 1$, so $m = \mathrm{ord}(y)$.

(b) $(xy)^{mn} = x^m y^n = 1$ (since G is abelian). Suppose now that $1 \le \ell$ and $(xy)^\ell = 1$. We want to show that $\ell \ge mn$. We have $x^\ell = y^{-\ell} \in \langle x \rangle \cap \langle y \rangle$. Lagrange's Theorem says that $|\langle x \rangle \cap \langle y \rangle|$ is a common divisor of $|\langle x \rangle| = m$ and $|\langle y \rangle| = n$, and hence $\langle x \rangle \cap \ \langle y \rangle = \{1\}$. Therefore $x^\ell = 1$, whence $m \mid \ell$; and $y^\ell = 1$, whence $n \mid \ell$. Therefore $\ell \ge \mathrm{LCM}(m,n) = mn$. (Probably there's a direct proof that doesn't use Lagrange's Theorem.)

(c) (Ugh! I don't see how to use the hint, so I will do a direct and messy approach.) Write $m = p_1^{e_1} \cdots p_m^{e_m}$ and $n = p_1^{f_1} \cdots p_s^{f_s}$, where the p_i are the distinct prime divisors of mn and e_i, f_i are non-negative integers. For each i, let $g_i = \max\{e_i, f_i\}$. The LCM of m and n is is $p_1^{g_1} \cdots p_s^{g_s}$. For each i there is an element of order $p_i^{g_i}$, by part (a). Now, using part (b) repeatedly, we build elements whose orders are $p_1^{g_1}, p_1^{g_1}p_2^{g_2}, p_1^{g_1}p_2^{g_2}p_3^{g_3}, \ldots, p_1^{g_1} \cdots p_s^{g_s}$. (I really hope someone finds a more elegant approach!)

(d) Suppose, by way of contradiction, that there exists an element g for which $g^n \ne 1$, and let m be the order of g. Then m is not a divisor of n, so the LCM ℓ of m and n is strictly bigger than n. But by (c) there is an element of order ℓ, contradiction.

(e) Let G be the multiplicative group $F \setminus \{0\}$, and choose an element $x \in G$ of largest order, say n. By (d), we have $g^n = 1$ for every $g \in G$. Since the polynomial $X^n - 1 \in F[X]$ has at most n roots in F, we have $|G| \le n$. Now

$$n = |\langle x \rangle| \le |G| \le n\,,$$

and hence $\langle x \rangle = G$.

2 An element g of a group G is a *square* provided there exists an element $h \in G$ such that $g = h^2$.

(a) If G is a finite cyclic group and g_1 and g_2 are elements of G, neither one of which is a square, prove that $g_1 g_2$ *is* a square.
(b) Let p be any prime number. Using the fact that the multiplicative group $\mathbb{F}_p \setminus \{0\}$ is cyclic, show that $X^4 - 10X^2 + 1$ is reducible in $\mathbb{F}_p[X]$. (That is, fill in the details of Footnote 3 at the bottom of page 13 of Milne.)

Solution: (a) Let $H = \{g^2 \mid g \in G\}$, and note that H is a subgroup of G since G is abelian. Also G/G^2 is a cyclic group in which every element has order 1 or 2, and it follows that $|G/H| \leq 2$. But the existence of the elements g_1 and g_2 says that $|G/H| = 2$. The cosets $\overline{g_1}$ and $\overline{g_2}$ in G/H are then the same element of G/H, namely the non-identity element. Their product must then be the identity element, that is, $g_1 g_2 \in H$. (By the way, $|G/H| = 1$ if and only if $|G|$ is odd.)

(b) By Problem 1, $G = \mathbb{F}_p \setminus \{0\}$ is a cyclic group. The argument on page 13 of Milne shows that $f(X) := X^4 - 10x^2 + 1$ factors non-trivially in $\mathbb{F}_p$ if either 2 or 3 is a square in G. In the remaining case, part (a) says that 6 must be a square, and then the argument in Milne again shows that $f(X)$ factors non-trivially.

3. Let $F \subseteq K$ be a field extension. Let α be an element of K whose degree over F is odd. Prove that $F(\alpha) = F(\alpha^2)$.

Solution: Since α is a root of the polynomial $X^2 - \alpha^2 \in F(\alpha^2)[X]$, we know that $[F(\alpha) : F(\alpha^2)] \leq 2$. If $[F(\alpha) : F(\alpha^2)] = 2$, we have

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F] = 2[F(\alpha^2) : F]\,,$$

contradicting the fact that $[F(\alpha) : F]$ is odd. Therefore $[F(\alpha) : F(\alpha^2)] = 1$, that is, $F(\alpha) = F(\alpha^2)$. (The argument is much easier to follow if you draw the appropriate picture and label degrees.)

4. Again, draw the picture and label the degrees. Let $F \subseteq K$ be a field extension, and let α and β be elements of of K whose degrees over F are m and n, respectively. Prove that if $\mathrm{GCD}(m, n) = 1$, then $[F(\alpha, \beta) : F] = mn$.

Solution: Let $r = [F(\alpha, \beta) : F(\alpha)]$ and $s = [F(\alpha, \beta) : F(\beta)]$. Let $f(X) \in F[X]$ be the minimal polynomial of β over F; thus $m = \deg(f(X)$. Since $f(X) \in F(\alpha)[X]$ and $f(\beta) = 0$, we see that $r \leq n$. By multiplicativity of degrees, we have $rm = sn$; thus $n \mid rm$, and since m and n are relatively prime we know that $n \mid r$. Since $\leq n$ it follows that $r = n$. Now $[F(\alpha, \beta) : F = mr = mn$.

5. Let $F \subseteq K$ be a field extension, and let α and β be elements of K whose degrees over F are m and n, respectively. Prove that α has degree m over $F(\beta)$ if and only if β has degree n over $F(\alpha)$.

Solution: Exactly the same picture as for Problem #4 applies here, with the same degree labels. Now r is the degree of β over $F(\alpha)$ and s is the degree of α over $F(\beta)$. The equation $rm = sn$ makes it obvious that $s = m \iff r = n$.

6. Let $F \subseteq K$ be a field extension, and let $f(X) \in F[X]$ be a monic polynomial of degree d. Let α be an element of K with $f(\alpha) = 0$. Prove that $d = [F(\alpha) : F]$ if and only if $f(X)$ is the minimal polynomial of α over F.

Solution: The "if" direction is the Fundamental Theorem on Degrees of Simple Extensions (FTDSE). For the "only if" direction, assume $d = [F(\alpha) : F]$ and let $g(X) \in F[X]$ be the minimal polynomial of α over F. Then $g(X) \mid f(X)$ in $F[X]$. Also, by FTDSE, $d = \deg g(X)$. Therefore $f(X) = cg(X)$ for some non-zero constant $c \in F$. Since both polynomials are monic, $c = 1$, so $f(X) = g(X)$.

Please turn the page for three more nice problems! And the rules.

7. Let $\alpha = \sqrt{3} + \sqrt{7} \in \mathbb{C}$.

(a) Find the minimal polynomial of α over $\mathbb{Q}$, and *prove* that it is the minimal polynomial.
(b) Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

Solution: First we show that $\sqrt{7} \notin \mathbb{Q}(\sqrt{3})$. Suppose, by way of contradiction, that $\sqrt{7} = a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$. Squaing both sides, we get

$$7 = a^2 + 2ab\sqrt{3} + 3b^2 .$$

If $a = 0$ we have $7 = 3b^2$, which is impossible, since $3X^2 - 7$ has no rational roots (by Eisenstein or Impossible Rational Roots). If $b = 0$ we have $a^2 = 7$, which is also impossible (since $X^2 - 7$ has no rational roots). Thus both a and b are non-zero. Now the equation shows, since $2ab \neq 0$, that $\sqrt{3}$ is rational, again a contradiction (since $X^2 - 3$ has no rational roots).

Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$ and $E = \mathbb{Q}(\sqrt{3})$. We know that $[E : \mathbb{Q}] = 2$, and since $\sqrt{7} \notin E$ we have $[K : E] > 1$. But also $[K : E] \leq 2$ since $\sqrt{7}$ is a root of $X^2 - 7 \in E[X]$. Thus $[K : E] = 2$, and by multiplicativity of degrees we have $[K : \mathbb{Q}] = 4$.

Now we prove (b): By direct computation we have

$$\alpha^2 = 10 + 2\sqrt{3}\sqrt{7} \quad \text{and} \quad \alpha^3 = 10\sqrt{3} + 10\sqrt{7} + 6\sqrt{7} + 14\sqrt{3} = 16\alpha + 8\sqrt{3} .$$

Therefore $\sqrt{3} = \frac{1}{8}\alpha^3 - 2\alpha \in \mathbb{Q}(\alpha)$, and $\sqrt{7} = \alpha - \sqrt{3} = -\frac{1}{8}\alpha^3 + 3\alpha \in \mathbb{Q}(\alpha)$, and we have $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{7}) \subseteq \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\alpha)$.

For (a), we square both sides of the equation $\alpha^2 - 10 = 2\sqrt{3}\sqrt{7}$, getting

$$\alpha^4 - 10\alpha^2 + 100 = 84, \quad \text{that is} \quad \alpha^4 - 10\alpha^2 + 16 = 0 .$$

Now $f(X) = X^4 - 20X^2 - 16$ is a monic polynomial of degree 4 having α as a root. Since, by (b) and the initial computations, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, Problem #6 implies that $f(X)$ is the minimal polynomial for α over $\mathbb{Q}$.

8. Let R be an integral domain, and let $x, y \in R$. Prove that $Rx = Ry \iff x = yu$ for some unit $u \in R$.

Solution: Suppose $Rx = Ry$. Then there are elements $r, s \in R$ such that $x = ry$ and $y = sx$. If $x = 0$, then $y = 0$ too, and we have $x = 1y$. If $x \neq 0$ we note that $1x = x = rsx$; canceling the non-zero element x, we get $1 = rs$. Thus r is a unit, and we take $u = r$.

For the converse, assume $x = yu$ where u is a unit. That equation shows that $x \in Ry$ and hence that $Rx \subseteq Ry$. The equation $xu^{-1} = y$ shows that $y \in Rx$, so $Ry \subseteq Rx$.

9. For the polynomials $f(X) = X^4 + 3X^2 + 1$ and $g(X) = X^3 + 2X + 1$, find their GCD $h(X)$, and find polynomials $a(X)$ and $b(X)$ such that

$$h(X) = a(x)f(X) + b(X)g(X)$$

(a) in $\mathbb{Q}[X]$, and
(b) in $\mathbb{F}_2[X]$.

Solution: We refer to the top four equations in the second display of 1.8 in the book. They describe the first four division steps in the Euclidean algorithm. (Actually the fourth division step is part of the "…"—the line of dots to indicate that it is similar to the rest, but is not displayed— in the display.) Here are these equations:

$$\begin{aligned} f &= q_0 g + r_0 \\ g &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \end{aligned}$$

I will not show here the actual divisions, but just say what the results are, when working $\mathbb{Q}[X]$:

$$\begin{gathered} q_0 = X \qquad r_0 = X^2 - X + 1 \\ q_1 = X + 1 \qquad r_1 = 2X \\ q_2 = \frac{1}{2}(X-1) \qquad r_2 = 1 \\ q_3 = 2X \qquad r_3 = 0 \end{gathered}$$

Recall that the GCD is the last non-zero remainder; so in $\mathbb{Q}[X]$ the GCD is $r_2 = 1$. In $\mathbb{F}_2[X]$, the first two equations are the same, but now $r_1 = 0$, and the GCD is $r_0 = X^2 - X + 1$.

Using the first display, we can write each remainder as a linear combination of f and g, as follows:

$$\begin{aligned} r_0 &= \qquad f - q_0 g \\ r_1 &= g - q_1 r_0 = g - q_1(f - q_0 g) = \qquad -q_1 f + (1 + q_1 q_0) g \\ r_2 &= r_0 - q_2 r_1 = (f - q_0 g) - q_2\big(-q_1 f + (1 + q_1 q_0) g\big) \\ &= (1 + q_2 q_1) f + (-q_0 - q_2 - q_2 q_1 q_0) g \end{aligned}$$

(a) We already know that the GCD is 1. This is r_2, and we get the coefficients in the expression we want by plugging the values of q_0, q_1, and q_2 into the last equation:

$$1 = \big(1 + \frac{1}{2}(X^2 - 1)\big) f + \big(-X - \frac{1}{2}(X-1) - \frac{1}{2}(X-1)(X-2)X\big) g\,,$$

or, somewhat more palatably:

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

Actually, we might as well declare the GCD to be 2 (since in $F[X]$ every non-zero constant multiple of a GCD is a GCD). Then we can write

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

We actually multiplied this out and found, to our amazement that it worked. Hurray!

(b) This is much easier. Recall that the GCD is $r_0 = X^2 - X + 1$. The relevant equation is just $r_0 = f - q_0 g$, that is,

$$X^2 - X + 1 = 1(X^4 + 3X^2 + 1) - X(X^3 + 2X + 1)$$

Of course, since $2 = 0$, $+$ and $-$ are the same, and this can be rewritten as follows:

$$X^2 + X + 1 = 1(X^4 + X^2 + 1) + X(X^3 + 1)\,.$$