Math 113, Solutions to the Final Exam

(1) We have $[21] \cdot [11] = [-2] \cdot [11] = -[22] = -[-1] = 1$. Hence u^{-1} is the class of 21, and $u + u^{-1}$ is the class of 9.

(2) The smallest non-abelian group is the symmetric group S_3 which has order 6. Every group of prime order $2, 3, 5$ is cyclic and hence abelian. There are two groups of order 4, namely, $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and they are both abelian. Note that every group of order p^2, for p a prime number, is an abelian group. This was shown in Corollary 2.10.15.

(3) The number of units in $\mathbf{Z}/60\mathbf{Z}$ is the value of Euler's phi-function at 60. Using the formula in §1.8.3, we find

$$\psi(60) \;=\; 60 \cdot (1 - 1/2)(1 - 1/3)(1 - 1/5) \;=\; 16.$$

(4) We have $\Phi_{11}(x) \;=\; x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, by Exercise 4.10, since $p = 11$ is a prime number.

(5) We want $f(x) = x^3 + 2x^2 + a$ to be an irreducible polynomial, which is equivalent, by Proposition 4.6.3 (v), to $f(x)$ having no root in $\mathbf{F}_5$. Direct computation shows that

$$f(0) = f(3) = a, \;\; f(2) = f(4) = 1 + a, \;\; f(1) = 3 + a$$

Therefore $a = -2 = 3$ and $a = -4 = 1$ are the two choices for which $f(x)$ is irreducible, and precisely in these two cases is $\mathbf{F}_5[x]/\langle f(x)\rangle$ a field, by Proposition 4.6.3 (i).

(6) A computation shows that the reduced lexicographic Gröbner basis for the given ideal consist of the two polynomials

$$y - \frac{1}{2}x^3 + \frac{1}{2}x \quad \text{and} \quad x^4 - x^2 + 4.$$

Hence, by Theorem 5.9.1, the elimination ideal $I \cap \mathbf{Q}[x]$ is generated by $f(x) \;=\; x^4 - x^2 + 4$.

(7) This statement is not true: Take G to be the symmetric group S_3, and consider its two-element subgroups $H_1 = \{id, (12)\}$ and $H_2 = \{id, (13)\}$. Then the set $H_1 \cdot H_2$ consists of the four permutations $id, (12), (13)$ and (132), and this is not a subgroup of S_3. By Lemma 2.3.6, the statement would be true if either H_1 or H_2 were normal.

(8) This statement is true (and appears in Exercise 3.25): Ideals in R/I are in one-to-one correspondence with ideals J in R that contain I. If f is an element in R that generates the principal ideal J then its image in R/I will generate the image of J in R/I. See also Exercise 3.20.

(9) This statement is true: Let $v = (3, 5)$ and consider the weight term ordering $\leq_v$. Then y^2 is the leading term of the first polynomial y^2+x^3, and x^2 is the leading term of the second polynomial $x^2 + y$. The S-polynomial $x^2(y^2 + x^3) - y^2(x^2 + y) = x^5 - y^3$ reduces to zero upon division by $\{y^2 + x^3, x^2 + y\}$ and hence (by Buchberger's Criterion) the two given polynomials are a Gröbner basis. See also Exercise 5.20.

(10) This statement is false: The element y is irreducible in R but it is not prime because it divides xz but does not divide either of x or z. To prove this rigorously we use the fact that $\{xz - y^2\}$ is a Gröbner basis for the ideal it generates. Proof of *irreducible*: If $y = pq$ in R for some non-units p and q then p and q have positive degree. This is impossible because $y - pq$ cannot reduce to zero modulo the Gröbner basis. Proof of *not prime*: If $yq = x$ in R for some polynomial q then $qy - x$ is in the ideal. But it cannot reduce to zero modulo the Gröbner basis.