Mathematics 351. Final Review Sheet

General information. I am planning a test in two parts, consisting of 12 computational questions (120 points) and 5 more abstract questions (80 points), generally similar to what we have done in the past. (This may change; if I plan anything unusual you will hear about it in class.)
Review materials: the first two tests, this sheet, and the original review sheets—in that order.

Part I

1 Compute $1/44$ in $\mathbb{Z}_{103}$.

2 Factor the following polynomials in $\mathbb{Z}_{37}[x]$.
(*a*) x^2+3 (*b*) x^2+x+1

3 Find the g.c.d. of $2x^3-3x^2+4x-6$ and $3x^3-2x^2+6x-4$ in $\mathbb{Z}[x]$.

4 Compute $(x+1)^{30}$ in $\mathbb{Z}_3[x]$.

5 Factor the polynomial x^4-4 completely in each of the following cases:
(*a*) in $\mathbb{Q}[x]$; (*b*) in $\mathbb{R}[x]$; (*c*) in $\mathbb{C}[x]$; (*d*) in $\mathbb{Z}_5[x]$; (*e*) in $\mathbb{Z}_{11}[x]$; (*f*) in $\mathbb{Z}_{17}[x]$

6 Find all rational roots of the polynomial $6x^3-11x^2+6x-1$ and factor the polynomial completely over $\mathbb{Q}$.

7 Find the remainder of $x^{10}+10x^7+10x^4+25x^2+1$ on division by $x+2$

8 Find the greatest common divisor of 58 and $21+20i$ in $\mathbb{Z}[i]$.

9 Solve the equation $x^2+y^2=18685$ with $x, y \in \mathbb{Z}$ using complex arithmetic in $\mathbb{Z}[i]$. (Note: 18685 is divisible by 101.)

10 Factor 143 into irreducible factors in $\mathbb{Z}[i]$.

11 Exhibit an isomorphism between the group U_{13} and the group Z_{12}.

12 Find the order of each of the following groups:
(*a*) A_5 (*b*) U_{12} (*c*) $U(\mathbb{Z}[i]\times Z_7)$ (*d*) $U(\mathbb{Z}[i])\times Z_7$ (*e*) $\langle(12)(34567)\rangle$
(*f*) $\langle(12)(34167)\rangle$ (*g*) $\langle(12),(34567)\rangle$ (*h*) $\langle(12),(34167)\rangle$ (*i*) $\mathbb{Z}_{12}/4\mathbb{Z}_{12}$

13 For each of the following groups, state what orders its elements have, and how many elements there are of each order.
(*a*) $\mathbb{Z}_{13}$ (*b*) $\mathbb{Z}_{12}$ (*c*) $U(\mathbb{Z}[i])$ (*d*) $\mathbb{Z}_4\times\mathbb{Z}_4$ (*e*) S_6 (*f*) A_6

14 Find the least positive integer i such that:
(*a*) $[(123)(45678)]^i=(123)(46857)$; (*b*) $[(123)(45678)(132)]^i=1$.

15 Compute the dimension of the following fields over $\mathbb{Q}$.
(*a*) The field generated over $\mathbb{Q}$ by *all* the roots of the polynomial x^3-x^2+2x-2.
(*b*) The field generated over $\mathbb{Q}$ by the *real* root of the polynomial x^3+3x+1
(*c*) The field generated over $\mathbb{Q}$ by *all* the roots of the polynomial x^3+3x+1

16 Let F be the field obtained from $\mathbb{Q}$ by adjoining all complex roots of the equation $x^3=2$ to $\mathbb{Q}$.
(*a*) Prove that F is not a subfield of $\mathbb{R}$.
(*b*) Prove that the dimension of F over $\mathbb{Q}$ is 6.
(*c*) Give a basis for F over $\mathbb{Q}$.

17 Determine all the left and right cosets of each of the following subgroups explicitly. Give the order and the index of each subgroup.
(*a*) $\langle 4\rangle$ inside Z_{12}; (*b*) $\langle 3\rangle$ inside Z_{12}; (*c*) $\langle 3\rangle$ inside U_{13}; (*d*) $\langle(12)(34)\rangle$ inside A_4.

18 Write the following elements of S_5 as products of elementary transpositions $((12),(23),(34),(45))$:

$$(13),(14),(15),(13245),(15)(24)$$

19 Find an element $x\in A_6$ satisfying

$$x(123)(456)x^{-1}=(132)(456)$$

Part II

1 Prove that $\log_3(5)$ is irrational.

2 Prove that the polynomial $p(x) = \dfrac{x^5 - 1}{x - 1}$ is irreducible over $\mathbb{Q}$.

3 Prove that (a) the additive group $\mathbb{R}$ of real numbers is isomorphic to the multiplicative group $\mathbb{R}^{**}$ of positive real numbers, but (b) the corresponding claim is false for $\mathbb{Q}$ and $\mathbb{Q}^{**}$.

4 Prove that the quotient group $\mathbb{R}^*/(\pm 1)$ is isomorphic to the group $\mathbb{R}^{**}$.

5 Let $G = \mathrm{GL}(2, \mathbb{R})$ and $H = \mathrm{SL}(2, \mathbb{R})$. Show that for any nonzero real number r, the set of matrices in G with determinant r is a coset of H.

6 Prove that the angle 20° is not Euclidean constructible:
(a) Show that the number $2\cos 20^\circ$ satisfies the equation:

$$x^3 - 3x - 1 = 0$$

(b) Show that $\mathbb{Q}[\cos 20^\circ]$ has dimension 3 over $\mathbb{Q}$.
(c) Quote some big theorem.

7 If R is a ring and A, B are subrings of R, prove that the intersection $A \cap B$ is also a subring of R.

8 If G is a group and A, B are subgroups of G, prove that the intersection $A \cap B$ is also a subgroup of G.

9 Let R be a commutative ring, and $a \in R$ an element. Show that the set aR is an ideal of R.

10 Let R be a ring, $a \in R$ an element, and let S be the set of elements $r \in R$ which *commute with* a, that is:

$$S = \{r \in R : ar = ra\}$$

Show that S is a *subring* of R.

11 Let G be a group, $a \in G$ an element, and let H be the set of elements $g \in G$ which *commute with* a, that is:

$$H = \{g \in G : ag = ga\}$$

Show that H is a *subgroup* of G.

12 Let R, R', S, S' be rings and let $f_1 : R \to R'$, $f_2 : S \to S'$ be homomorphisms. Define $f : R \times S \to R' \times S'$ by

$$f(r, s) = (f_1(r), f_2(s))$$

Show that
(a) f is a homomorphism;
(b) the kernel of f is $\ker(f_1) \times \ker(f_2)$.

13 Let G, G', H, H' be groups and let $f_1 : G \to G'$, $f_2 : H \to H'$ be homomorphisms. Define $f : G \times H \to G' \times H'$ by

$$f(a, b) = (f_1(a), f_2(b))$$

Show that
(a) f is a homomorphism;
(b) the kernel of f is $\ker(f_1) \times \ker(f_2)$.

14 Let G, H be groups, $f : G \to H$ an isomorphism, and $a \in G$. Prove that $|a| = |f(a)|$.

15 Let G be a finite group and X a subset of G with $|X| > |G|/2$. Show that $X \cdot X = G$.

16 Let F be a finite field. Show that every element of F is a sum of two squares.

17 Let $N \subseteq K \subseteq G$ be groups with N normal in G and K/N normal in G/N. Show that K is normal in G.

18 Let H, K be normal subgroups of the group G with $H \cap K = (e)$. Show that the elements of H and K commute: $hk = kh$ for $h \in H$, $k \in K$.

Answers to Part I

1 Solve $44x = 1 + 103y$. Ans: $x = 96$

2 Find the roots: (*a*) compute $\sqrt{3}$; (*b*) use the quadratic formula. Ans: $(x-16)(x-21)$; $(x-10)(x+11)$

3 $x^2 + 2$

4 Use $30 = 3 + 27$. Ans: $x^{30} + x^{27} + x^3 + 1$.

5 $(a), (d)$ $(x^2-2)(x^2+2)$; (b) $(x+\sqrt{2})(x-\sqrt{2})(x^2+2)$; (c) $(x+\sqrt{2})(x-\sqrt{2})(x+i\sqrt{2})(x-i\sqrt{2})$; (e) $(x^2-2)(x-3)(x+3)$; (f) $(x+6)(x-6)(x+7)(x-7)$.

6 $1, 1/2, 1/3$: $(x-1)(2x-1)(3x-1)$.

7 Evaluate at $x = -2$: 5.

8 $5 + 2i$.

9 $102^2 + 91^2$ or $118^2 + 69^2$.

10 $(2+3i) \cdot (2-3i) \cdot 11$

11

$\mathbf{U_{13}}$:	1	2	3	4	5	6	7	8	9	10	11	12
$\mathbf{Z_{12}}$:	0	1	4	2	9	5	11	3	8	10	7	6

12 (*a*) 60; (*b*) 4; (*c*) 24; (*d*) 28; (*e*) 10; (*f*) 6; (*g*) 10; (*h*) 720; (*i*) 4.

13

Part	(*a*)	
Orders	1	13
#	1	12

Part	(*b*)					
Orders	1	2	3	4	6	12
#	1	1	2	2	2	4

Part	(*c*)		
Orders	1	2	4
#	1	1	2

Part	(*d*)		
Orders	1	2	4
#	1	3	12

Part	(*e*)					
Orders	1	2	3	4	5	6
#	1	75	80	180	144	240

Part	(*f*)				
Orders	1	2	3	4	5
#	1	45	80	90	144

14 (*a*) 7; (*b*) 5.

15 (*a*) 2; (*b*) 3; (*c*) 6. In (*a*) the polynomial is reducible; in (b, c) it is irreducible (rational root test).

16 (*a*) Evidently there is only one real root r, but three complex roots.
(*b*) The equation is irreducible (Eisenstein) and has a real root r. Over $\mathbb{Q}[r]$ the polynomial still has an irreducible quadratic factor since the other two roots are not real. So the dimensions in the tower $\mathbb{Q} - \mathbb{Q}[\alpha] - F$ must be 3 and 2.
(*c*) $(1, r, \omega, \omega r, \omega^2 r)$ with $r = \sqrt[3]{2}$ and ω a complex cube root of 1. (In other words, $[1, r] \cdot [1, \omega, \omega^2]$.)

17 In $(a - c)$ right and left cosets are the same:
(*a*) Order 3 and index 4. $\{0,4,8\}$, $\{1,5,9\}$, $\{2,6,10\}$, $\{3,7,11\}$.
(*b*) Order 4 and index 3, $\{0,3,6,9\}$, $\{1,4,7,10\}$, $\{2,5,8,11\}$.
(*c*) Order 3 and index 4. $\{1,3,9\}$, $\{2,6,5\}$, $\{4,12,10\}$, $\{8,11,7\}$,
(*d*) Order 2 and index 6.
Right cosets: $\{I, (12)(34)\}$, $\{(13)(24), (14)(23)\}$, $\{(123), (134)\}$, $\{(132), (234)\}$, $\{(124), (143)\}$, $\{(142), (243)\}$.
Left cosets: $\{I, (12)(34)\}$, $\{(13)(24), (14)(23)\}$, $\{(123), (243)\}$, $\{(132), (143)\}$, $\{(124), (234)\}$, $\{(142), (134)\}$.

18 $(13) = (23)(12)(23)$; $(14) = (34)(23)(12)(23)(34)$; $(15) = (45)(34)(23)(12)(23)(34)(45)$;
$(13245) = (23)(12)(23)(12)(34)(23)(12)(23)(34)(45)(34)(23)(12)(23)(34)(45)$;
$(15)(24) = (45)(34)(23)(12)(23)(34)(45)(34)(23)(34)$.

19 $x = (23)$ would work but it is an odd permutation; $x = (23) \cdot (14)(26)(35) = (14)(2635)$ also works and is in A_6 as required.

Ideas for Part II

1 Reduce to the equation $3^a = 5^b$ and use unique factorization in $\mathbb{Z}$.

2 Apply Eisenstein to $p(x+1)$ first (workshop problem).

3 (a) e^x; (b) $\mathbb{Q} = 2\mathbb{Q}$ but $\mathbb{Q}^{**} \neq (\mathbb{Q}^{**})^2$.

4 The function $f(x) = x^2$ defines a homomorphism from $\mathbb{R}^*$ onto $\mathbb{R}^{**}$ with kernel (± 1).

5 If g is a matrix with determinant r, show that $Hg = \{g' : \det(g') = r\}$.

6 (a) Use $(\cos 20\deg + i\sin 20\deg)^3 = \cos 60\deg + i\sin 60\deg$ and the binomial theorem.
(b) The polynomial in part (a) is irreducible (rational root test).
(c) If the angle were constructible the dimension would be a power of 2.

7 Check subtraction and multiplication.

8 Same argument as in #7.

9 Absorption: $(ax)r = a(xr)$; $r(ax) = a(xr)$ also, by commutativity.

10 Multiplication: $a(ss') = (as)s' = (sa)s' = s(as') = s(s'a) = (ss')a$.

11 Same argument as in #10.

12 Just check.

13 Same as #12.

14 $f(a^n) = f(a)^n$, so $a^n = e_G$ if and only if $f(a)^n = e_H$.

15 For $g \in G$, show $X^{-1} \cap (Xg^{-1}) \neq \emptyset$.

16 In #15, consider the additive group of F, with X the set of squares. Conclude $X + X = F$.

17 Taking $g \in G$ and $k \in K$ we claim $gk \in Kg$. We look at $gkN \in g(K/N) = (K/N)g$ and get $gkN = \hat{k}Ng$ so $gk \in KNg = Kg$.

18 Show that $hkh^{-1}k^{-1} \in H \cap K$ and conclude $hkh^{-1}k^{-1} = e$.