Hints to Exercises

Hints to Chapter 0

Exercise 0.22: Since you have to prove something for any subset of $\mathbb{Z}$, give it a name: let S be any subset of $\mathbb{Z}$. Then explain why any two elements $a, b \in S$ satisfy $a < b$, $a = b$, or $a > b$. If you think about the definition of a subset in the right way, your proof will be a lot shorter than the proof of Theorem 0.16.

Exercise 0.24: Try to show that $a - b = 0$.

Exercise 0.25: Use the definition of $<$.

Exercise 0.27: Let m, n be two smallest elements of S. Since m is a smallest element of S, what do you know about m and n? Likewise, since n is a smallest element of S, what do you know about m and n? Then...

Exercise 0.28: Here, "smallest" doesn't mean what you think of as smallest; it means smallest with respect to the definition. That is, you have to explain why there does *not* exist $a \in \mathbb{N}$ such that for all other $b \in \mathbb{N}$, we have $a > b$.

Exercise 0.29: This question is really asking you to find a new ordering $\prec$ of $\mathbb{Q}$ that is a linear ordering *and* that behaves the same on $\mathbb{Z}$ as $<$. To define $\prec$, choose $p, q \in \mathbb{Q}$. By definition, there exist $a, b, c, d \in \mathbb{Z}$ such that $p = a/b$ and $q = c/d$. What condition can you place on $ad - bc$ that would (a) order p and q, and (b) remain compatible with $<$ in $\mathbb{Z}$ in case $p, q \in \mathbb{Z}$ as well?

Exercise 0.44: Use Exercise 0.26(c).

Exercise 0.51: Pick an example $n, d \in \mathbb{Z}$ and look at the resulting M. Which value of q gives you an element of $\mathbb{N}$ as well? If $n \in \mathbb{N}$ then you can easily identify such q. If $n < 0$ it takes a little more work.

Hints to Chapter 1

Exercise 1.20: Don't confuse what you have to do here, or what the elements are. You have to work with elements of $P(S)$; these are *subsets of* S. So, if I choose $X \in P(S)$, I know that $X \subseteq S$. Notice that I use capital letters for X, even though it is an element of $P(S)$, precisely because it is a set. This isn't something you *have* to do, strictly speaking, but you might find it helpful to select an element of X to prove at least one of the properties of a monoid, and it looks more natural to select $x \in X$ than to select $a \in x$, even if this latter x is a set.

Exercise 1.22: To show closure, you have to explain how we know that the set specified in the definition of lcm has a minimum.

Exercise 1.30: By Definition **??**, you have to show that

- for any monoid M, $M \cong M$ (reflexive);
- for any two monoids M and N, if $M \cong N$, then also $N \cong M$ (symmetric); and
- for any three monoids M, N, and P, if $M \cong N$ and $N \cong P$, then $M \cong P$ (transitive).

In the first case, you have to find an isomorphism $f : M \longrightarrow M$. In the second, you have to assume that there exist isomorphisms $f : M \longrightarrow N$, then show that there exists an isomorphism $f : N \longrightarrow M$.

Hints to Chapter 2

Exercise 2.15: Remember that $-$ means the additive inverse. So, you have to show that the additive inverse of $-x$ is x.

Exercise 2.18: Use substitution.

Exercise 2.19: Work with arbitrary elements of $\mathbb{R}^{2\times 2}$. The structure of such elements is

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad \text{where } a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{R}.$$

Exercise 2.23: At least one such monoid appears in the exercises to this section.

Exercise 2.27: You probably did this in linear algebra, or saw it done. Work with arbitrary elements of $\mathbb{R}^{m\times m}$, which have the structure

$$A = \left(a_{i,j}\right)_{i=1\ldots m, j=1\ldots m}.$$

Exercise 2.34:

(a) Try $m = 2$, and find two invertible matrices A, B such that $(AB)\left(A^{-1}B^{-1}\right) \neq I_2$.

(b) Use the associative property to help simplify the expression $(ab)\left(b^{-1}a^{-1}\right)$.

Exercise 2.35: You may assume that composition of functions is associative in this problem.

(a) Use the fact that $(F \circ F)(P) = F(F(P))$ to show that $(F \circ F)(P) = I(P)$, and repeat with the other functions.

(b) One of closure, identity, or inverse fails. Which?

(c) Add elements to G that are lacking, until all the properties are now satisfied.

(d) A clever argument would avoid a brute force computation.

Exercise 2.45: To rewrite products so that ρ never precedes φ, use Theorem 2.38. To show that D_3 satisfies the properties of a group, you may use the fact that D_3 is a subset of $\mathrm{GL}(2)$, the multiplicative group of 2×2 invertiable matrices. Thus D_3 "inherits" certain properties of $\mathrm{GL}(2)$, but which ones? For the others, simple inspection of the multiplication table should suffice.

Exercise 2.48:

(a) You may use the property that $|P - Q|^2 = |P|^2 + |Q|^2 - 2P \cdot Q$, where $|X|$ indicates the distance of X from the origin, and $|X - Y|$ indicates the distance between X and Y.

(c) Use the hint from part (a), along with the result in part (a), to show that the distance between the vectors is zero. Also use the property of dot products that for any vector X, $X \cdot X = |X|^2$. Don't use part (b).

Exercise 2.49: Let $P = (p_1, p_2)$ be an arbitrary point in $\mathbb{R}^2$, and assume that ρ leaves it stationary. You can represent P by a vector. The equation $\rho \cdot \vec{P} = \vec{P}$ gives you a system of two linear equations in two variables; you can solve this system for p_1 and p_2.

Exercise 2.50: Repeat what you did in Exercise 2.49. This time the system of linear equations will have infinitely many solutions. You know from linear algebra that in $\mathbb{R}^2$ this describes a line. Solve one of the equations for p_2 to obtain the equation of this line.

Exercise 2.61: Use the product notation as we did.

Exercise 2.62: Use Theorem 2.59.

Exercise 2.63: Look back at Exercise 2.31 on page 65.

Exercise 2.65: Use denominators to show that no matter what you choose for $x \in \mathbb{Q}$, there is some $y \in \mathbb{Q}$ such that $y \notin \langle x \rangle$.

Exercise 2.66: One possibility is to exploit $\det(AB) = \det A \cdot \det B$. It helps to know that $\mathbb{R}$ is not cyclic (which may not be obvious, but should make sense from Exercise 2.65).

Hints to Chapter 3

Exercise 3.13: Start with the smallest possible subgroup, then add elements one at a time. Don't forget the adjective "proper" subgroup.

Exercise 3.16: Look at what L has in common with H from Example 3.8.

Exercise 3.19: Use Exercise 2.65 on page 83.

Exercise 3.21: Look at Exercise 3.18 on page 99.

Exercise 3.36: For (CE1), you have to show that two sets are equal. Follow the structure of the proof for Theorem 3.27 on page 102. Take an arbitrary element of eH, and show that it also an element of H; that gives $eH \subseteq H$. Then take an arbitrary element of H, and show that it is an element of eH; that gives $eH \supseteq H$. The two inclusions give $eH = H$.

As for (CE2) and (CE3), you can prove them in a manner similar to that of (CE1), or you can explain how they are actually consequences of (CE1).

Exercise 3.49: Use Corollary 3.44 on page 107.

Exercise 3.50: See Exercises 2.63 on page 83 and 3.49.

Exercise 3.69: Theorem 3.56 tells us that the subgroup of an abelian group is normal. If you can show that $D_m(\mathbb{R})$ is abelian, then you are finished.

Exercise 3.71: It is evident from the definition that $Z(G) \subseteq G$. You must show first that $Z(G) < G$. Then you must show that $Z(G) \triangleleft G$. Make sure that you separate these steps and justify each one carefully!

Exercise 3.72: First you must show that $H \subseteq N_G(H)$. Then you must show that $H < N_G(H)$. Finally you must show that $H \triangleleft N_G(H)$. Make sure that you separate these steps and justify each one carefully!

Exercise 3.73: List the two left cosets, then the two right cosets. What does a partition mean? Given that, what sets must be equal?

Exercise 3.74(c): The "hard" way is to show that for all $g \in G$, $g[G,G] = [G,G]g$. This requires you to show that two sets are equal. Any element of $[G,G]$ has the form $[x,y]$ for some $x, y \in G$. At some point, you will have to show that $g[x,y] = [w,z]g$ for some $w, x \in G$. This is an

existence proof, and it suffices to construct w and z that satisfy the equation. To construct them, think about conjugation.

An "easier" way uses the result of Exercise 3.67, showing that $gG'g^{-1} = G'$ for any $g \in G$. Exercise 2.37 should help you see why $gG'g^{-1} \subseteq G'$; to show the reverse direction, show why any $g' \in G'$ has the form $g^{-1}[x^g, y^g]\,g$ for any $g \in G$, so $gG'g^{-1} \supseteq G'$.

Exercise 3.86: Use Lemma 3.29 on page 103.

Exercise 3.109: There are one subgroup of order 1, three subgroups of order 2, one subgroup of order 3, and one subgroup of order 6. From Exercise 5.37 on page 161, you know that $S_3 \cong D_3$, and some subgroups of D_3 appear in Example 3.9 on page 98 and Exercise 3.18 on page 99.

Hints to Chapter 4

Exercise 4.15(b): Generalize the isomorphism of (a).

Exercise 4.25: Use the Subgroup Theorem along with the properties of a homomorphism.

Exercise 4.22: For a homomorphism function, think about the equation that describes the points on L.

Exercise 4.23: Since it's a corollary to Theorem 4.9, you should use that theorem.

Exercise 4.25: Denote $K = \ker f$. Show that $gKg^{-1} = K$ for arbitrary $g \in G$; then Exercise 3.67 applies. Showing that $gKg^{-1} \subseteq K$ is routine. To show that $gKg^{-1} \supseteq K$, let $k \in K$; by closure, $g^{-1}kg = x$ for some $x \in G$. Show that $x \in K$, then rewrite the definition of x to obtain $k \in gKg^{-1}$.

Exercise 4.28: Use induction on the positive powers of g; use a theorem for the nonpositive powers of g.

Exercise 4.29(b): Let $G = \mathbb{Z}_2$ and $H = D_3$; find a homomorphism from G to H.

Exercise 4.30: Recall that

$$f(A) = \{y \in H : f(x) = y \ \exists x \in A\},$$

and use the Subgroup Theorem.

Exercise 4.31(b): See the last part of Exercise 4.29.

Exercise 4.49(a): Consider $f : \mathbb{R}^2 \to \mathbb{R}$ by $f(a) = b$ where the point $a = (a_1, a_2)$ lies on the line $y = x + b$.

Exercise 4.50(b): You already know the answer from Exercise 3.64 on page 113; find a homomorphism f from Q_8 to that group such that $\ker f = \langle -1 \rangle$.

Exercise 4.64: Use some of the ideas from Example 4.54(c), as well as the Subgroup Theorem.

Exercise 4.66: We can think of D_3 as generated by the elements ρ and φ, and each of these generates a non-trivial cyclic subgroup. Any automorphism α is therefore determined by these generators, so you can find all automorphisms α by finding all possible results for $\alpha(\rho)$ and $\alpha(\varphi)$, then examining that carefully.

Hints to Chapter 5

Exercise 5.33: Life will probably be easier if you convert it to cycle notation first.

Exercise 5.36: List the six elements of S_3 as $\begin{pmatrix} 1 \end{pmatrix}$, α, α^2, β, $\alpha\beta$, $\alpha^2\beta$, using the previous exercises both to justify and to simplify this task.

Exercise 5.37: Show that f is an isomorphism either exhaustively (this requires $6 \times 6 = 36$ checks for each possible value of $f\left(\rho^a \varphi^b\right)$), or by a clever argument, perhaps using using the Isomorphism Theorem (since $D_3 / \{\iota\} \cong D_3$).

Exercise 5.40: Try computing $\alpha \circ \beta$ and $\beta \circ \alpha$.

Exercise 5.72: Lemma 5.61 tells us that any permutation can be written as a product of cycles, so it will suffice to show that any cycle can be written as a product of transpositions. For that, take an arbitrary cycle $\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$ and write it as a product of transpositions, as suggested by Example 5.60. Be sure to explain why this product does in fact equal α.

Exercise 5.73: You can do this by showing that any transposition is its own inverse. Take an arbitrary transposition $\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix}$ and show that $\alpha^2 = \iota$.

Exercise 5.75: Let α and β be arbitrary cycles. Consider the four possible cases where α and β are even or odd.

Exercise 5.76: See a previous exercise about subgroups or cosets.

Exercise 5.80: Use the same strategy as that of the proof of Theorem 5.79: find the permutation σ^{-1} that corresponds to the current confiuration, and decide whether $\sigma^{-1} \in A_{16}$. If not, you know the answer is no. If so, you must still check that it can be written as a product of transpositions that satisfy the rules of the puzzle.

Hints to Chapter 6

Exercise 6.23: At least you know that $\gcd(16, 33) = 1$, so you can apply the Chinese Remainder Theorem to the first two equations and find a solution in $\mathbb{Z}_{16 \cdot 33}$. Now you have to extend your solution so that it also solves the third equation; use your knowledge of cosets to do that.

Exercise 6.14: Since $d \in S$, we can write $d = am + bn$ for some $a, b \in \mathbb{Z}$. Show first that every common divisor of m, n is also a divisor of d. Then show that d is a divisor of m and n. For this last part, use the Division Theorem to divide m by d, and show that if the remainder is not zero, then d is not the smallest element of M.

Exercise 6.34: Use the properties of prime numbers.

Exercise 6.62: Consider Lemma 6.39 on page 194.

Exercise 6.65(c): Using the Extended Euclidean Algorithm might make this go faster. The proof of the RSA algorithm outlines how to use it.

Exercise 6.66:

(b) That largest number should come from encrypting ZZZZ.

(d) Using the Extended Euclidean Algorithm might make this go faster. The proof of the RSA algorithm outlines how to use it.

Exercise 6.67: There are a couple of ways to argue this. The best way for you is to explain why there exist a, b such that $ap + bq = 1$. Next, explain why there exist integers d_1, d_2 such that $m = d_1 a$ and $m = d_2 b$. Observe that $m = m \cdot 1 = m \cdot (ap + bq)$. Put all these facts together to show that $ab \mid m$.

Hints to Chapter 7

Exercise 7.13: The cases where $n = 0$ and $n = 1$ can be disposed of rather quickly; the case where $n \neq 0, 1$ is similar to (a).

Exercise 7.15:

(a) This is short, but not trivial. You need to show that $(-r)s + rs = 0_R$. Try using the distributive property.

(b) You need to show that $-1_R \cdot r + r = 0$. Try using a proof similar to part (a), but work in the additive identity as well.

Exercise 7.16: Proceed by contradiction. Show that if $r \in R$ and $r \neq 0, 1$, then something goes terribly wrong with multiplication in the ring.

Exercise 7.17: Use the result of Exercise 7.16.

Exercise 7.18: You already know that $(B, \oplus)$ is an additive group, so it remains to decide whether $\wedge$ satisfies the requirements of multiplication in a ring.

Exercise 7.33: Use the definition of equality in this set given in Example 7.24. For the first simplification rule, show the equalities separately; that is, show first that $(ac)/(bc) = a/b$; then show that $(ca)/(cb) = a/b$.

Exercise 7.34: For the latter part, try to find $f\,g$ such that f and g are not even defined, let alone an element of $\mathrm{Frac}(R)$.

Exercise 7.49: Proceed by induction on $\deg f$. We did *not* say that r was unique.

Exercise 7.56: Showing that φ is multiplicative should be straightforward. To show that φ is additive, use the Binomial Theorem

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^n y^{n-i}$$

along with the fact that p is irreducible.

Exercise 7.67: $\mathbb{Z}[x]$ is a subring of what Euclidean domain? But don't be too careless–if you can find the gcd in that Euclidean domain, how can you go from there back to a gcd in $\mathbb{Z}[x]$?

Exercise 7.68: Since it's a field, you should never encounter a remainder, so finding a valuation function should be easy.

Exercise 7.69: There are two parts to this problem. The first is to find a "good" valuation function. The second is to show that you can actually divide elements of the ring. You should be able to do both if you read the proof of Theorem 7.57 carefully.

Exercise 7.70: For correctness, you will want to show something similar to Theorem 6.8 on page 182.

Exercise 7.71(a,iii): A system of equations could help with this latter division.

Hints to Chapter 8

Exercise 8.16: Use the Division Theorem for Integers (Theorem 0.34).

Exercise 8.18: The Extended Euclidean Algorithm (Theorem 6.8 on page 182) would be useful.

Exercise 8.23: For part (b), consider ideals of $\mathbb{Z}$.

Exercise 8.37: Show that if there exists $f \in \mathbb{F}[x,y]$ such that $x, y \in \langle f \rangle$, then $f = 1$ and $\langle f \rangle = \mathbb{F}[x,y]$. To show that $f = 1$, consider the degrees of x and y necessary to find $p, q \in \mathbb{F}[x,y]$ such that $x = pf$ and $y = qf$.

Exercise 8.38: Use the Ideal Theorem.

Exercise 8.48: Follow the argument of Example 8.43.

Exercise 8.63:

(c) Let g have the form $cx + d$ where $c, d \in \mathbb{C}$ are unknown. Try to solve for c, d. You will need to reduce the polynomial fg by an appropriate multiple of $x^2 + 1$ (this preserves the representation $(fg) + I$ but lowers the degree) and solve a system of two linear equations in the two unknowns c, d.

(e) Use the fact that $x^2 + 1$ factors in $\mathbb{C}[x]$ to find a zero divisor in $\mathbb{C}[x] / \langle x^2 + 1 \rangle$.

Exercise 8.64: Try the contrapositive. If $\mathbb{F}[x] / \langle f \rangle$ is not a field, what does Theorem 8.57 tell you? By Theorem 7.69, $\mathbb{F}[x]$ is a Euclidean domain, so you can find a greatest common divisor of f and a polynomial g that is not in $\langle f \rangle$ (but where is g located?). From this gcd, we obtain a factorization of f.

Or, follow the strategy of Exercise 8.63 (but this will be very, very ugly).

Exercise 8.65:

(a) Look at the previous problem.

(b) Notice that

$$y\left(x^2 + y^2 - 4\right) + I = I$$

and $x(xy - 1) + I = I$. This is related to the idea of the *subtraction polynomials* in later chapters.

Exercise 8.80: Use strategies similar to those used to prove Theorem 4.9 on page 129.

Exercise 8.83: Follow Example 8.75 on page 260.

Exercise 8.84: Multiply two polynomials of degree at least two, and multiply two matrices of the form given, to see what the polynomial map should be.

Exercise 8.85(d): Think about $i = \sqrt{-1}$.

Hints to Chapter 10

Exercise 10.13: You could do this by proving that it is a subring of $\mathbb{C}$. Keep in mind that $\left(\sqrt{-5}\right)\left(\sqrt{-5}\right) = -5$.

Exercise 10.37(d): Proceed by induction on n.

Exercise 10.41: Think of a fraction field over an appropriate ring.

Hints to Chapter 11

Exercise 11.61(b): Use part (a).

Exercise 11.62(c): Don't forget to explain why $\langle G \rangle = \langle G_{\text{minimal}} \rangle$! It is essential that the S-polynomials of these redundant elements top-reduce to zero. Lemma 11.54 is also useful.

Index

References

[AF05] Marlow Anderson and Todd Feil. *A First Course in Abstract Algebra*. Chapman and Hall/CRC, second edition, 2005.

[AP] Alberto Arri and John Perry. The F5 Criterion revised. Submitted to the *Journal of Symbolic Computation*, 2009, preprint online at `arxiv.org/abs/1012.3664`.

[Bah08] Tavmjong Bah. *Inkscape: Guide to a Vector Drawing Program*. Prentice-Hall, second edition, 2008. Retrieved from `www.inkscape.org`.

[Bri] Rogério Brito. The `algorithms` bundle. Retrieved 16 October 2008 from `http://www.ctan.org/tex-archive/macros/latex/contrib/algorithms/`. Version 0.1.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalem Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)*. PhD thesis, Mathematical Insitute, University of Innsbruck, Austria, 1965. English translation published in the Journal of Symbolic Computation (2006) 475–511.

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag New York, Inc., New York, second edition, 1997.

[CLO98] David Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Springer-Verlag New York, Inc., New York, 1998.

[EP10] Christian Eder and John Perry. F5C: A variant of Faugère's F5 algorithm with reduced Gröbner bases. *Journal of Symbolic Computation*, 45(12):1442–1458, 2010.

[EP11] Christian Eder and John Perry. Signature-based algorithms to compute Gröbner bases. In *Proceedings of the International Symposium on Symbolic and Algebraic Manipulation*, 2011.

[Fau02] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In *International Symposium on Symbolic and Algebraic Computation Symposium - ISSAC 2002, Villeneuve d'Ascq, France*, pages 75–82, Jul 2002. Revised version downloaded from `http://fgbrs.lip6.fr/jcf/Publications/index.html`.

[GGV10] Shuhong Gao, Yinhua Guan, and Frank Volny. A new incremental algorithm for computing Groebner bases. In *Proceedings of the 2010 Inter-*

national Symposium on Symbolic and Algebraic Computation. ACM Press, 2010.

[GPS05] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005. `http://www.singular.uni-kl.de`.

[Grä04] George Grätzer. *Math into LaTeX*. Birkhäuser, Boston, third edition, 2004.

[HA88] Abraham P. Hillman and Gerald L. Alexanderson. *A First Undergraduate Course in Absract Algebra*. Wadsworth Publishing Company, Belmont, California, fourth edition, 1988.

[Knu84] Donald Knuth. *The TeXbook*. Addison-Wesley Professional, spi edition, 1984.

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra*, volume 1. Springer-Verlag, Berlin - Heidelberg - New York, 2000.

[Lam86] Leslie Lamport. *LaTeX: a Document Preparation System*. Addison-Wesley Publishing Company, 1986.

[Lau03] Niels Lauritzen. *Concrete Abstract Algebra: from Numbers to Gröbner Bases*. Cambridge University Press, Cambridge, 2003.

[LP98] Rudolf Lidl and Günter Pilz. *Applied Abstract Algebra*. Springer-Verlag, New York, second edition edition, 1998.

[Lyx] Lyx Team. *Lyx*, 2008–. Retrieved too many times to count from `http://www.lyx.org`.

[Pic06] Paul Pichaureau. *The mathdesign package*, 2006. Retrieved from `http://www.ctan.org/tex-archive/help/Catalogue/entries/mathdesign.html`.

[Pip07] Sebastian Pipping. *ccBeamer*, 2007. Retrieved from `http://www.hartwork.org/cgi-bin/download.cgi?file=CCBEAMER`.

[RO08] Sebastian Rahtz and Heiko Oberdiek. *Hypertext marks in LaTeX: a manual for* `hyperref`, 2008. Retrieved 21 April 2009 from `http://www.tug.org/applications/hyperref/manual.html`.

[Rot98] Joseph Rotman. *Galois Theory*. Springer-Verlag, New York, second edition, 1998.

[Rot06] Joseph J. Rotman. *A First Course in Abtract Algebra with Applications*. Pearson Education, Inc., New Jersey, third edition, 2006.

[Soc02] Americal Mathematical Society. *User's Guide for the* `amsmath` *Package*, version 2.0 edition, 2002. Retrieved 21 April 2009 from `http://www.ams.org/tex/amslatex.html`.

[Ste08] William Stein. *Sage: Open Source Mathematical Software (Version 3.1.1)*. The Sage Group, 2008. `http://www.sagemath.org`.

[vzGG99] Joachim von zur Gathen and Jurgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, 1999.