MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Sample Midyear Examination

This sample exam is deliberately longer than the actually midyear. It also includes only questions from the topics covered after the midterm exam, although the midyear exam will include some questions on topics covered before then.

Basic Questions

1. *Which of the following are rings: Justify your answers. [10 mins]*

   (a) The collection of integers with the usual addition and multiplication given by $a * b = ab + a + b$.

   This is not a ring because $*$ does not distribute over addition. For example $2 * (3 + 1) = 8 + 2 + 4 = 14$, but $2 * 3 + 2 * 1 = 11 + 5 = 16$.

   (b) The integers with the usual addition, and multiplication given by $a * b$ is the least common multiple of a and b.

   This is not a ring because $*$ does not distribute over $+$. For example $2 * (3 + 1) = 4$, but $2 * 3 + 2 * 1 = 6 + 2 = 8$.

   (c) The set of integers with the usual addition, and multiplication given by $a * b = 3ab$.

   This is a ring. We need to check that multiplication is associative: $(a * b) * c = (3ab) * c = 9abc = a * (b * c)$. We need to check that multiplication distributes over addition. $a * (b + c) = 3a(b + c) = 3ab + 3ac = a * b + a * c$, and since $*$ is commutative, the other distributivity follows.

   (d) The collection of subsets of a set X with 5 elements, with addition given by symmetric difference and multiplication given by intersection. [The symmetric difference of two sets A and B is the set of elements that occur in exactly one of them.]

   Symmetric difference is associative, since both $(A \triangle B) \triangle C$ and $A \triangle (B \triangle C)$ give the set of elements that are in exactly one or three of A, B or C.

2. *What are the units in the following rings: [15 mins]*

   (a) $\mathbb{Z}_{22}$.

   The units are the numbers coprime to 22. That is $\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$.

   (b) Numbers of the form $\frac{a+b\sqrt{2}i}{5}$ where a and b are integers.

   Suppose the number $\frac{a+b\sqrt{2}i}{5}$ is a unit in this ring. Then there is another number $\frac{c+d\sqrt{2}i}{5}$ in the ring, such that $\frac{a+b\sqrt{2}i}{5}\frac{c+d\sqrt{2}i}{5} = 1$, or eqivalently

$(a+b\sqrt{2}i)(c+d\sqrt{2}i) = ac-2bd+(ad+bc)\sqrt{2}i = 25$. This can only happen if $ad+bc=0$ and $ac-2bd=25$. Let $x=\frac{a}{c}=-\frac{b}{d}$, then we have $a^2x+2b^2x=25$ for some x such that ax and bx are both integers. We first consider cases where a and b are coprime. In this case, the fact that ax and bx are both integers means that x is an integer. Therefore, a^2+2b^2 must be a factor of 25. We consider the possibilities: $a^2+2b^2=1$ has only $a=\pm1, b=0$ as a solution. $a^2+2b^2=5$ has no solutions. $a^2+2b^2=25$ has only $a=\pm5$, $b=0$ as a solution. Therefore, the only units are $\frac{-1}{5}$, $\frac{1}{5}$,

3. *Show that the set of numbers of the form $a+b\sqrt{5}$ where a and b are rational numbers is a field. [10 mins]*

   Since these are all real numbers, we just need to show that this set is closed under addition and multiplication, contains the identity, and is closed under inverses. It is clear that this set is closed under addition, and for multiplication, we see $(a+b\sqrt{5})(c+d\sqrt{5}) = ac+5bd+(ad+bc)\sqrt{5}$, so the set is closed under multiplication.

   Finally, the inverse of $a+b\sqrt{5}$ is $\frac{a-b\sqrt{5}}{a^2+5b^2}$, which is $\frac{a}{a^2+5b^2}-\frac{b}{a^2+5b^2}$.

4. *Which of the following rings are integral domains: [7 mins]*

   (a) $\mathbb{Z}_{30}$.

   This is not an integral domain, because for example, $3\cdot 10=0$.

   (b) The ring of 2×2 upper triangular matrices over $\mathbb{Z}$.

   This is not an integral domain, because it is not commutative, and also

   $$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

   (c) The collection of rational numbers where the denominator is a power of 2.

   This is a subring of the rational numbers, so it is commutative and has no zero divisors, so we only need to check that it is unital, but this is obvious, since 1 is a rational number with denominator 1, which is a power of 2.

5. *Factorise $x^4+x^3+4x^2+24$:*

   (a) over $\mathbb{Z}_5$. [5 mins]

   We check for linear factors by looking for zeros:

x	$x^4+x^3+4x^2+24$
0	4
1	0
2	4
3	3
4	3

   so $x-1$ is a factor. By long division, we get $x^4+x^3+4x^2+24 = (x-1)(x^3+2x^2+x+1)$. We know that 0, 2, 3, and 4 cannot be zeros of x^3+2x^2+x+1, since then they would be zeros of $x^4+x^3+4x^2+24$, which we have seen they are not. However, we see that 1 is a zero of x^3+2x^2+x+1, so we factor it as $x^3+2x^2+x+1=(x-1)(x^2+3x-1)$. 1 is not a zero of x^2+3x-1, so it has no zeros, so it is irreducible. Therefore, we have $x^4+x^3+4x^2+24=(x-1)^2(x^2+3x-1)$ in $\mathbb{Z}_5$.

(b) over $\mathbb{Z}$. [6 mins]

We know that the factors must be congruent to products of $(x-1)^2$ and (x^2+3x-1) modulo 5. Furthermore, the constant terms must be factors of 24, so we can try a few possibilities — we first check for zeros (which must be factors of 24).

x	$x^4+x^3+4x^2+24$
-24	320280
-12	19608
-8	4864
-6	1248
-4	280
-2	48
-1	28
1	30
2	64
4	408
6	1680
8	4888
12	23064
24	347928

[In fact, it should be obvious that there are no zeros, since x^4+x^3 must be non-negative for any integer, and $4x^2+24$ must be positive.]

Therefore the only possible factorisation is as two quadratic factors, which must be congruent to (x^2-2x+1) and (x^2+3x-1) modulo 5. We try to divide by (x^2+3x-1), and we get $x^2-2x+11$, with a remainder of $-35x+35$. Next, we try to divide by (x^2+3x+4), and we get x^2-2x+6, with a remainder of $10x$. We try to divide by (x^2-2x-1), and we get $x^2+3x+11$, with a remainder of $-25x+35$. We try to divide by (x^2-2x+4), and we get x^2+3x+6, with no remainder.

We therefore conclude $x^4+x^3+4x^2+24=(x^2-2x+4)(x^2+3x+6)$.

6. *Show that $f(x)=x^4-x^3+3x^2-22x+40$ is irreducible over $\mathbb{Z}$. [Hint: consider $x=y+1$ and use Eisenstein's criterion.] [5 mins]*

   If we let $x=y+1$, the polynomial becomes $(y+1)^4-(y+1)^3+3(y+1)^2-22(y+1)+40=y^4+3y^3+6y^2-15y+21$. Using Eisenstein's criterion with $p=3$, we see that this is irreducible.

7. *Find all solutions to the equation $x^2-3x+8=0$ in $\mathbb{Z}_{12}$. [5 mins]*

By inspection, we see that $x = -1$ is a solution. This allows us to factorise $x^2 - 3x + 8 = (x + 1)(x - 4)$. Now in order for this product to be zero, there are several possibilities: We can have that one factor is zero, or we could have one factor divisible by 2 and the other by 6 — however this is impossible since they differ by an odd number, so cannot both be even — or one factor could be divisible by 4, and the other by 3. This gives the following possibilities:

x	$(x + 1)$	$(x - 4)$
11	0	7
8	9	4
7	8	3
4	5	0

Therefore, the solutions are 4, 7, 8 and 11.

8. *Find all prime numbers p such that $x-7$ is a factor of $x^4-4x^3+5x^2+4x-2$ in $\mathbb{Z}_p[x]$. [5 mins]*

   $x-7$ is a factor of $x^4-4x^3+5x^2+4x-2$ in $\mathbb{Z}_p[x]$ if and only if 7 is a zero of $x^4-4x^3+5x^2+4x-2$ in $\mathbb{Z}_p$. We have that $7^4-4\times 7^3+5\times 7^2+4\times 7-2 = 1272$, so $x-7$ is a factor of $x^4-4x^3+5x^2+4x-2$ in $\mathbb{Z}_p[x]$ if and only if p divides $1272 = 8 \times 3 \times 53$, so the prime numbers for which this happens are 2, 3, and 53.

9. *Find a generator for the multiplicative group of non-zero elements of $\mathbb{Z}_{29}$. [10 mins]*

   We know that the order of any element in this group divides 28, so is one of 1, 2, 4, 7, and 14. If we consider 2, we know that $2^4 = 16$, so the order of 2 must be larger than 4. $2^7 = 128 \equiv 12 \pmod{29}$, and $2^{14} \equiv 12\times 12 \equiv -1 \pmod{29}$. Therefore 2 is a generator in this group.

   Suppose we started by trying 7, we would find that $7^7 \equiv 1 \pmod{29}$, so 7 is not a generator. We could then try a different number (not a power of 7). Suppose we try 17. We would then discover that $17^4 \equiv 1 \pmod{29}$. We could then deduce that $7 \times 17 \equiv 3 \pmod{29}$ must have order the least common multiple of 7 and 4, which is 28, so this is a generator of the group.

10. *Show that $f(x) = x^3 - 2x^2 + 2$ is irreducible in $\mathbb{Z}_5$. [5 mins]*

    If f is not irreducible, then it must have a factor of the form $x - a$ for some $a \in \mathbb{Z}_5$. But this would mean that a is a zero of f, so we just need to check whether f has any zeros in $\mathbb{Z}_5$.

x	$f(x)$
0	2
1	1
2	2
3	1
4	4

f has no zeros in $\mathbb{Z}_5$ so it is irreducible over $\mathbb{Z}_5$.

11. *Find the remainder of* 6^{1022} *when divided by 11. [2 mins]*

    By Fermat's Little Theorem, $6^{10} \equiv 1 \pmod{11}$, so $6^{1020} \equiv 1 \pmod{11}$, and therefore, $6^{1022} \equiv 6^2 \equiv 3 \pmod{11}$.

12. *Find the remainder when* 11^{123456} *is divided by 21. [4 mins]*

    $\phi(21) = 2 \times 6 = 12$, so by Euler's theorem, $11^{12} \equiv 1 \pmod{21}$. Now 123456 is divisible by 3 (since the sum of its digits is), and divisible by 4 (since 56 is), so it is divisible by 12. Therefore, $11^{123456} \equiv 1 \pmod{21}$.

13. *Find the remainder when* $5^{5^{5^{5^{5^{5^{5^{5}}}}}}}$ *is divided by 13. [6 mins]*

    Since $5^{12} \equiv 1 \pmod{13}$, we just need to calculate $5^{5^{5^{5^{5^{5^{5}}}}}}$ modulo 12. Now $\phi(12) = 4$, so we need to calculate $5^{5^{5^{5^{5^{5}}}}}$ modulo 4. Now since $5 \equiv 1 \pmod{4}$, we know that $5^{5^{5^{5^{5^{5}}}}} \equiv 1 \pmod{4}$, so $5^{5^{5^{5^{5^{5^{5}}}}}} \equiv 5^1 \equiv 5 \pmod{12}$, and therefore $5^{5^{5^{5^{5^{5^{5^{5}}}}}}} \equiv 5^5 \equiv 5 \pmod{13}$.

14. *Solve: [8 mins]*

    (a) $8x \equiv 6(mod 19)$

    This has a unique solution. In this case, the easiest way is to see that by inspection $8 \times 12 \equiv 1 \pmod{19}$, so $8 \times 12 \times 6 \equiv 6 \pmod{19}$, so the solution is $x = 12 \times 6 \equiv 15 \pmod{19}$.

    Alternatively, we know that $8^{18} \cong 1 \pmod{19}$, so the inverse of 8 in $\mathbb{Z}_{19}$ is 8^{17}. We can then compute $8^2 \equiv 7$, $8^4 \equiv 11$, $8^8 \equiv 7$ [At this point, we can see that $8^6 \equiv 1$, (which we already know since $8^6 = 2^{18}$ so that the inverse of 8 is $8^5 \equiv 11 \times 8 \equiv 12$)] and $8^{16} \equiv 11$, so that $8^{17} \equiv 12$.

    (b) $2x \equiv 6(mod 18)$

    All the numbers are divisible by 2, so this has 2 solutions in $\mathbb{Z}_{18}$. The solutions can be obtained as the solutions to $x \equiv 3 \pmod{9}$, so they are $x \equiv 3$ and $x \equiv 12$.

15. *Describe the field of quotients of the integral domain* $\{a + b\sqrt{2}i | a, b \in \mathbb{Z}\}$. *[10 mins]*

    We know that by choosing the denominator to be an integer (i.e. $b = 0$), we can get all numbers of the form $x + y\sqrt{2}i$ where x and y are rational numbers. However, we can show that the set of these numbers is a field, and so must be the field of quotients of this integral domain. To show it is a field, it is obviously closed under addition and multiplication, so we just need to show that it is closed under inverses. However, $(a + b\sqrt{2}i)^{-1} = \frac{a - b\sqrt{2}i}{a^2 + 2b^2}$, which is of the form $x + y\sqrt{2}i$ for rational x and y.

Theoretical Questions

16. *(a) Show that the intersection of two subrings of a ring is a ring. [5 mins]*

    (b) Show that the intersection of two subfields of a field is a subfield. [5 mins]

17. *Show that the characteristic of an integral domain must be prime or 0. [5 mins]*

18. *Show that there is no field with exactly 6 elements. [10 mins]*

19. *Prove addition and multiplication are well-defined in the field of quotients of an integral domain. [7 mins]*

20. *Prove that a finite integral domain is a field. [10 mins]*

21. *Let D be an integral domain, and let F be a field of quotients of D. Let L be any field containing D. Prove that there is a homomorphism $\phi : F \longrightarrow L$ such that $\phi(x) = x$ for all $x \in L$. [10 mins]*

22. *State and prove the factor theorem for the polynomial ring over a field. [7 mins]*

23. *(a) Show that a polynomial of degree n in $F[x]$ for a field F can have at most n zeros. [7 mins]*

    (b) Deduce that the multiplicative group of non-zero elements in a finite field is cyclic. (Recall the classification theorem for finitely generated abelian groups.) [7 mins]