MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Homework Sheet 7
Due: Wednesday 14th November: 3:30 PM

Basic Questions

1. *Which of the following are rings:*

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

   This is not a ring because multiplication does not distribute over addition. $a * (b + c) = ab + ac + a + b + c$, while $a * b + a * c = ab + ac + 2a + b + c$.

   (b) The collection of positive rational numbers with multiplication and exponentiation. [That is $a + b = ab$ and $a \cdot b = a^b$.]

   This is not a ring because exponentiation is not associative. Also, exponentiation is left distributive, since $(ab)^c = a^c b^c$, but it is not right distributive, since $a^{bc} \neq a^b a^c$.

   (c) The set of real numbers which occur as solutions to quadratic equations with rational coefficients.

   This is not a ring, since it is not closed under addition; for example, $\sqrt{2}$ and $\sqrt{3}$ both satisfy quadratic equations, but $\sqrt{2} + \sqrt{3}$ does not satisfy a quadratic equation with rational coefficients. [We can see this either directly from the quadratic formula, or by considering $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, which is not a sum of a rational number and a rational multiple of $\sqrt{2} + \sqrt{3}$.] [It is also not closed under multiplication.

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

   This is a ring, isomorphic to $3\mathbb{Z}$.

2. *What are the units in the following rings:*

   (a) 2×2 matrices over $\mathbb{Z}$.

   The units are matrices whose determinant is invertible. The invertible elements of $\mathbb{Z}$ are 1 and -1, so the units of the ring of 2×2 matrices over $\mathbb{Z}$ are matrices with determinant 1 or -1.

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

   The modulus of $a + \frac{b}{\sqrt{2}}i$ is $a^2 + \frac{b^2}{2}$. Since the modulus of 1 is 1, and moduli are multiplicative, for an element to be invertible, its modulus must be invertible among the set of moduli of numbers of the given form.

That is, we must have $\left(a^2+\frac{b^2}{2}\right)\left(c^2+\frac{d^2}{2}\right)=1$ for integers a, b, c, and d. Multiplying each bracket by 2, we see that $2a^2+b^2$ must be a factor of 4. The only possibilities for this are $a=\pm 1, b=0$, $a=0, b=\pm 1$ and $a=0, b=\pm 2$. That is, the only units are 1, -1, $\frac{i}{\sqrt{2}}$, $\frac{-i}{\sqrt{2}}$, $\sqrt{2}i$ and $-\sqrt{2}i$.

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

   We just need to show that this set is closed under addition, multiplication, additive inverse and multiplicative inverse of non-zero element, and that it contains 0 and 1. It is easy to see that it contains 0 and 1, and is closed under addition and additive inverse, so we just need to show that it is closed under multiplication and multiplicative inverse. $(a+b\sqrt{3})(c+d\sqrt{3}) = ac+3bd+(ad+bc)\sqrt{3}$ is clearly of the required form, while $(a+b\sqrt{3})^{-1}=\frac{a-b\sqrt{3}}{a^2-3b^2}$ is also of the required form.

4. *Which of the following rings are integral domains:*

   (a) $\mathbb{Z}_3\times\mathbb{Z}_5$.

   This is not an integral domain, since, for example, $(1,0)(0,1)=(0,0)$.

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

   This is not an integral domain, since $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

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

   This is a subring of the real numbers, so must be an integral domain, since any zero-divisors would also be zero-divisors in the real numbers.

5. *Are the rings $\mathbb{Z}_3\times\mathbb{Z}_5$ and $\mathbb{Z}_{15}$ isomorphic?*

   If there were an isomorphism ϕ, it would need to preserve the unit, so it must be given by $\phi(n)=(n(\mod 3), n(\mod 5))$. This is an isomorphism, since we know that addition and multiplication are preserved by modular arithmetic.

6. *Show that the only unital rings whose additive group is isomorphic to the integers, are the usual ring of integers, and multiplication given by $x*y=-xy$.*

   Let R be a unital ring whose additive group is isomorphic to the additive group of integers. Let n be the unit of this ring, and let $1*1=m$. Now we have that $n=n*n=(1+\cdots+1)(1+\cdots+1)=n^2m$. This gives $nm=1$, so n must be a unit of the usual multiplication on the integers.

   Suppose 1 is the unit of R. Now for any integers m and n we have $m*n=(1+\cdots+1)n=n+\cdots+n=mn$, so that R is just the usual ring of integers. On the other hand, if -1 is the unit of R, then $0=1*(-1+1)=1*-1+1*1=1+1*1$, so $1*1=-1$. Now $m*n=(1+\cdots+1)n=(-n)+\cdots+(-n)=-mn$ as required.

Standard Questions

7. *A ring R is a Boolean ring if for any element $x \in R$, $x^2 = x$. Show that any Boolean ring is commutative.*

   Let x and y be two elements of a Boolean ring. We have that $x + x = (x + x)^2 = (x + x)(x + x) = x + x + x + x$, so $x + x = 0$. Furthermore, $x + y = (x + y)^2 = x^2 + y^2 + xy + yx$, so we get $xy + yx = xy + xy = 0$, and therefore, $xy = yx$, so the ring is commutative.

8. *(a) Show that the intersection of two subrings of a ring is a ring.*

   Let S and T be subrings of R. We need to show that $S \cap T$ is a subring of R. That is, we need to show that it is closed under addition, additive inverse and multiplication, and that it contains 0. However, since $0 \in S$ and $0 \in T$, we have $0 \in S \cap T$. Similarly, for $a, b \in S \cap T$, we have $a+b \in S$, $a+b \in T$, $-a \in S$, $-a \in T$, $ab \in S$ and $ab \in T$, so $a+b \in S \cap T$, $-a \in S \cap T$ and $ab \in S \cap T$, so $S \cap T$ is a ring.

   (b) Show that the intersection of two subfields of a field is a subfield.

   We have already shown that it is a subring, so we just need to show it is closed under multiplicative inverses, and contains 1. However, S and T both contain 1 and are closed under inverses, so the same is true of $S \cap T$.

9. *For a set X, let $P(X)$ denote the set of all subsets of X (this is called the power set of X). Show that $P(X)$ is a ring with the operations of symmetric difference and intersection.*

   We need to show that $P(X)$ is an abelian group under symmetric difference, that intersection is associative, and that intersection distributes over intersection.

   The identity for symmetric difference is the empty set. $(a \triangle b) \triangle c$ and $a \triangle (b \triangle c)$ are both the set of elements which occur in an odd number of the sets a, b and c, so symmetric difference is associative. Every subset is self-inverse under symmetric difference. Symmetric difference is clearly commutative. Intersection is clearly associative, since $(a \cap b) \cap c$ and $a \cap (b \cap c)$ are both equal to the set of elements in all three subsets. Finally, we need to show that $a \cap (b \triangle c) = (a \cap b) \triangle (a \cap c)$. We will show this by showing both inclusions. Let $x \in a \cap (b \triangle c)$. Suppose, without loss of generality that $x \in b$ and $x \notin c$. Now $x \in a \cap b$ and $x \notin a \cap c$. Therefore, $x \in (a \cap b) \triangle (a \cap c)$. Conversely, suppose $x \in (a \cap b) \triangle (a \cap c)$. Suppose without loss of generality that $x \in a \cap b$ and $x \notin a \cap c$. This gives $x \in a$, $x \in b$ and $x \notin c$, so $x \in b \triangle c$, and thus $x \in a \cap (b \triangle c)$.

10. *Show that the characteristic of an integral domain must be prime or 0.*

    Suppose R is a ring with unit of characteristic mn with $m, n > 1$, then if we define $m = 1 + \cdots + 1$ and $n = 1 + \cdots + 1$, then by distributivity, $mn = 1 + \cdots + 1 = 0$. This means that R cannot be an integral domain.

11. *Show that there is no field with exactly 6 elements.*

    The characteristic of a field must be prime or 0. Let F be a field with 6 elements. The additive subgroup generated by 1 must have 1, 2, 3, or 6 elements. It can't have 1 or 6 elements, since the characteristic of F is prime. Suppose F has characteristic 3. Now all the non-zero elements can be partitioned into pairs of the form $\{x, 2x\}$. However, there are 5 non-zero elements, so this is not possible. Therefore, F must have characteristic 2. However, the additive group of F is an abelian group with 6 elements, so must be isomorphic to $\mathbb{Z}_6$, or $\mathbb{Z}_2 \times \mathbb{Z}_3$. However, either possibility involves an element of order 3, but this contradicts characteristic 2.

12. *Show that the intersection of two subdomains of an integral domain is another subdomain.*

    Let E and F be subdomains of the integral domain D. $E \cap F$ is clearly a subring of D, and contains 1, since both E and F do, so we just need to show that it has no zero-divisors. However, if $xy = 0$ in $E \cap F$, then $xy = 0$ in E, and in F, which contradicts the assumption that E and F are integral domains.

Bonus Questions

13.