PMATH 347 Groups and Rings, Solutions to Assignment 3

1: For $n\in\mathbb{Z}^+$, let $\mathbb{Z}_n[\,i\,]=\big\{a+ib\,\big|\,a,b\in\mathbb{Z}_n\big\}$, with addition and multiplication defined in the obvious way by $(a+ib)+(c+id)=(a+c)+i(b+d)$ and $(a+ib)(c+id)=(ac-bd)+i(ad+bc)$. You may assume, without proof, that $\mathbb{Z}_n[\,i\,]$ is a ring.

(a) Find all the units and all the zero divisors in the ring $\mathbb{Z}_4[i]$.

Solution: Let $a,b\in\mathbb{Z}_4$ with $a+ib\neq 0\in\mathbb{Z}_4[i]$. When $a=b=0\mod 2$ we have $(a+ib)(a-ib)=a^2+b^2=0+0=0$, so $a+ib$ is a zero divisor. When $a=b=1\mod 2$ we have $(a+ib)(a-ib)=a^2+b^2=1+1=2$, so $(a+ib)\big(2(a-ib)\big)=0$, and so again $a+ib$ is a zero divisor. On the other hand, when $a\neq b\mod 2$ we have $a^2+b^2=0+1=1$, so $a+ib$ is a unit.

(b) Without proof, list all of the subrings of $\mathbb{Z}_4[i]$.

Solution: There are 9 subrings, namely $\{0\}$, $\{0,2\}$, $\{0,2i\}$, $\{0,2+2i\}$, $\{0,1,2,3\}$, $\{0,2,2i,2+2i\}$, $\{0,2,1+i,3+i,2i,2+2i,1+3i,3+3i\}$, $\{0,1,2,3,2i,1+2i,2+2i,3+2i\}$ and $\mathbb{Z}_4[i]$.

(c) Find all primes p with $p<12$ such that $\mathbb{Z}_p[i]$ is a field.

Solution: Since $\mathbb{Z}_p[i]$ is a finite commutative ring with $1\neq 0$, it is a field if and only if it has no zero divisors. Let $0\neq a+ib\in\mathbb{Z}_p[i]$. Note that $a+ib$ is a zero divisor in $\mathbb{Z}_p[i]\iff$ there exists $0\neq x+iy\in\mathbb{Z}_p[i]$ such that $(a+ib)(x+iy)=0\in\mathbb{Z}_p[i]\iff$ there exists $0\neq(x,y)\in{\mathbb{Z}_p}^2$such that $ax-by=ay+bx=0\in\mathbb{Z}_p$ $\iff\det\begin{pmatrix}a&-b\\b&a\end{pmatrix}=0\in\mathbb{Z}_p\iff a^2+b^2=0\in\mathbb{Z}_p$. Thus we see that $\mathbb{Z}_p[i]$ has a zero divisor if and only if there exists $a,b\in\mathbb{Z}_p$ with $(a,b)\neq(0,0)$ such that $a^2+b^2=0\in\mathbb{Z}_p$. For each prime $p<12$, we list all of the possible values for x^2 and $-x^2$ and determine whether there exist $0\neq a,b\in\mathbb{Z}_p$ with $a^2+b^2=0$. Note that for $p>2$ it suffices to consider $1<x<\frac{p-1}{2}$ since $(p-x)^2=(-x)^2=x^2$ in $\mathbb{Z}_p$.

$\mathbb{Z}_2$

x	1
x^2	1
$-x^2$	1

$\mathbb{Z}_3$

x	1
x^2	1
$-x^2$	2

$\mathbb{Z}_5$

x	1	2
x^2	1	4
$-x^2$	4	1

$\mathbb{Z}_7$

x	1	2	3
x^2	1	4	2
$-x^2$	6	3	5

$\mathbb{Z}_{11}$

x	1	2	3	4	5
x^2	1	4	9	5	3
$-x^2$	10	7	2	6	8

We see that in $\mathbb{Z}_2$ we have $1^2+1^2=0$ and in $\mathbb{Z}_5$ we have $1^2+2^2=0$, so $\mathbb{Z}_p[i]$ is not a field when $p\in\{2,5\}$. On the other hand, when $p=3$, 7 or 11, the above tables show that there is no solution to $a^2+b^2=0$ with $0\neq a,b\in\mathbb{Z}_p$, and so $\mathbb{Z}_p[i]$ is a field when $p\in\{3,7,11\}$.

Although question 1(c) only asks us to consider primes $p<12$, it is interesting to consider the general case. In fact, for each prime p, there exists a solution to $a^2+b^2=0$ with $a,b\neq 0$ if and only if for every $k\in\mathbb{Z}_p$ there exists $a\in\mathbb{Z}_p$ with $a^2+k^2=0$, if and only if there exists $x\in\mathbb{Z}_p$ such that $x^2+1=0$. To prove this, suppose first that $a^2+b^2=0$ with $0\neq a,b\in\mathbb{Z}_p$. Then taking $x=ab^{-1}$, we have $x^2=(ab^{-1})^2=a^2(b^{-1})^2=-b^2(b^{-1})^2=-1$ so $x^2+1=0$. Conversely, suppose that $x^2+1=0$ in $\mathbb{Z}_p$. Then given any $k\in\mathbb{Z}^p$ we can take $a=xk$ and then $a^2=(xk)^2=x^2k^2=(-1)k^2=-k^2$ so $a^2+k^2=0$.

Next we claim that for each prime $p>2$, there exist $x\in\mathbb{Z}_p$ such that $x^2+1=0$ if and only if $p=1\mod 4$, that is if and only if $\frac{p-1}{2}$ is even. To prove this, let $p>2$ and suppose first that $x^2+1=0$. Then by Fermat's Little Theorem we have $(-1)^{(p-1)/2}=(x^2)^{(p-1)/2}=x^{p-1}=1$ and so $\frac{p-1}{2}$ is even. Conversely suppose that there is no $x\in\mathbb{Z}_p$ such that $x^2+1=0$. Then we can group the non-zero elements of $\mathbb{Z}_p$ into pairs $\{a_i,b_i\}$ with $a_ib_i=-1$. By Wilson's Theorem, we have $-1=(p-1)!=1\cdot 2\cdot\ldots\cdot(p-1)=(a_1b_1)(a_2b_2)\cdots\big(a_{\frac{p-1}{2}}b_{\frac{p-1}{2}}\big)=(-1)^{(p-1)/2}$ and hence $\frac{p-1}{2}$ is odd. To prove Wilson's Theorem (which states that $(p-1)!=-1$ in $\mathbb{Z}_p$) in the case $p>2$, let $f(x)=x^{p-1}-1$, note that $f(x)=0$ for all $0\neq x\in\mathbb{Z}_p$ (by Fermat's Little Theorem) so we must have $f(x)=(x-1)(x-2)\cdots(x-(p-1))$, then note that $-1=f(0)=(-1)(-2)\cdots(-(p-1))=(-1)^{p-1}(p-1)!=(p-1)!$.

From these two claims it follows that $\mathbb{Z}_p[i]$ is a field if and only if there do not exist $0\neq a,b\in\mathbb{Z}_p$ with $a^2+b^2=0$ if and only if there does not exist $x\in\mathbb{Z}_p$ with $x^2+1=0$ if and only if $p=3\mod 4$.

2: (a) Consider the ring $\mathcal{C}^0(\mathbb{R})$ of continuous functions $f : \mathbb{R} \to \mathbb{R}$ under addition and mutiplication. Prove that the units in $\mathcal{C}^0(\mathbb{R})$ are the nowhere zero functions, and the zero-divisors in $\mathcal{C}^0(\mathbb{R})$ are the functions which are not identically zero, but which are zero in some open interval.

Solution: Note that in the ring $\mathcal{C}^0(\mathbb{R})$, the identity element is the constant function 1 and the zero element is the constant function 0. Let $f \in \mathcal{C}^0(\mathbb{R})$. If f is nowhere zero, then the function $g = \frac{1}{f}$ is continuous, and we have $fg = 1$, so f is a unit. If f is a unit with say $fg = 1$, then for all $x \in \mathbb{R}$ we have $f(x)g(x) = 1$ so $f(x) \neq 0$, and so f is nowhere zero. Suppose that $f \neq 0$ but $f(x) = 0$ for all $x \in (a, b)$ where $a < b$. Define the function g by $g(x) = \begin{cases} 0 & \text{, if } x \notin (a,b) \\ (x-a)(b-x) & \text{, if } x \in [a,b] \, . \end{cases}$ Note that $g \neq 0$, $g \in \mathcal{C}^0(\mathbb{R})$ and $fg = 0$. Thus f is a zero-divisor. Conversely, suppose that f is a zero divisor, say $fg = 0$ with $f, g \neq 0$ and $g \in \mathcal{C}^0(\mathbb{R})$. Since $g \neq 0$ we can choose $a \in \mathbb{R}$ so that $g(a) \neq 0$. Since g is continuous, we can choose $\delta > 0$ so that for all $x \in (a-\delta, a+\delta)$ we have $\big|g(x) - g(a)\big| < |g(a)|$ so that $g(x) \neq 0$. Then for all $x \in (a-\delta, a+\delta)$ we have $f(x)g(x) = 0$ and $g(x) \neq 0$, and so $f(x) = 0$.

(b) Let F be a field and consider the ring $F\big[[x]\big]$ of formal power series in x. Find all the units and all the zero divisors in $F\big[[x]\big]$.

Solution: Write $u = \sum_{i \geq 0} a_i x^i$, $v = \sum_{j \geq 0} b_j x^j$. We have $uv = 1$ when

$$\begin{aligned} a_0 b_0 &= 1 \\ a_1 b_0 + a_0 b_1 &= 0 \\ a_2 b_0 + a_1 b_1 + a_0 b_2 &= 0 \\ &\vdots \\ a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n &= 0 \\ &\vdots \end{aligned}$$

To get $a_0 b_0 = 1$ we must have $a_0 \neq 0$. Given that $a_0 \neq 0$ we can solve for $b_0, b_1, b_2, \cdots$ by taking $b_0 = -\frac{1}{a_1}$, $b_1 = -\frac{1}{a_1}(a_1 b_0)$, $b_2 = -\frac{1}{a_1}(a_2 b_0 + a_1 b_1), \cdots, b_n = -\frac{1}{a_n}(a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1}), \cdots$ to get $uv = 1$. Thus the units in $F\big[[x]\big]$ are the elements $u = \sum_{i \geq 0} a_i x^i$ with $a_0 \neq 0$.

(c) Consider the group $S_\infty = \mathrm{Perm}(\mathbb{Z}^+)$ of bijective maps $\sigma : \mathbb{Z}^+ \to \mathbb{Z}^+$ under composition. Let H be the set of all elements of finite order in S_∞. Determine whether $H \leq G$.

Solution: H is not a subgroup of S_∞. For example, let $\alpha \in S_\infty$ be the permutation which interchanges $2k-1$ with $2k$ for all $k \in \mathbb{Z}^+$, and let $\beta \in S_\infty$ be the permutation which interchanges $2k$ with $2k+1$ for all $k \in \mathbb{Z}^+$ (with $\beta(1) = 1$). Then $|\alpha| = |\beta| = 2$, but for $\sigma = \beta\alpha$ we have $\sigma(1) = 3$, $\sigma^2(1) = \sigma(3) = 5$, $\sigma^3(1) = \sigma(5) = 7$, and so on, so that in general $\sigma^n(1) = 2n+1$ so that $\sigma^n \neq e$ for any $n \in \mathbb{Z}^+$ and hence $|\beta\alpha| = |\sigma| = \infty$.

3: (a) In S_9, let $\alpha=(1548)(2936)$ and $\beta=(16574)(38)$. Find $(-1)^{\alpha\beta}$ and $|\alpha\beta|$.

Solution: We have
$$\alpha\beta=(1548)(2936)(16574)(38)=(1293)(45786)$$
and so $(-1)^{\alpha\beta}=(-1)^{3+4}=-1$ and $|\alpha\beta|=\text{lcm}(4,5)=20$.

(b) In S_8, let $\beta=(123)(456)$. Find every element $\alpha\in S_8$ such that $\alpha^2=\beta$.

Solution: We have $\alpha^6=\beta^3=(1)$, so $|\alpha|=1,2,3$ or 6. We cannot have $|\alpha|=1$ since $\alpha\neq(1)$ (otherwise $\alpha^2=(1)\neq\beta$), and we cannot have $|\alpha|=2$ since $\alpha^2=\beta\neq(1)$. Thus $|\alpha|=3$ or 6. Case 1: if $|\alpha|=3$ then α is of the form (abc) or the form $(abc)(def)$. If $\alpha=(abc)$ then $\alpha^2=(acb)\neq\beta$. If $\alpha=(abc)(def)$ then $\alpha^2=(acb)(dfe)$, and so $\alpha^2=\beta \iff \alpha=(132)(465)$. Case 2: if $|\alpha|=6$ then α is of one of the following 5 forms: $(abc)(de)$, $(abc)(de)(fg)$, $(abc)(def)(gh)$, $(abcdef)$ or $(abcdef)(gh)$. If $\alpha=(abc)(de)$ or $(abc)(de)(fg)$ then $\alpha^2=(acb)\neq\beta$. If $\alpha=(abc)(def)(gh)$ then $\alpha^2=(acb)(dfe)$ and so $\alpha^2=\beta \iff \alpha=(132)(465)(78)$. If $\alpha=(abcdef)$ or $(abcdef)(gh)$ then $\alpha^2=(ace)(bdf)$, so we have $\alpha^2=\beta \iff \alpha=(142536)$, (152634) or (162435), or $\alpha=(142536)(78)$, $(152634)(78)$ or $(162435)(78)$. Thus there are 8 elements $\alpha\in S_8$ with $\alpha^2=\beta$, namely
$$\alpha\in\big\{(132)(465),(132)(465)(78),(142536),(152634),(162435),(142536)(78),(152634)(78),(162435)(78)\big\}.$$

(c) In S_{10}, let $\beta=(123)(456)(78)$. Find the number of elements $\alpha\in S_{10}$ such that $\alpha\beta=\beta\alpha$.

Solution: For $\alpha\in S_{10}$, we have $\alpha\beta=\beta\alpha$ when $\alpha\beta\alpha^{-1}=\beta$, and we know that, in cycle notation, we have
$$\alpha\beta\alpha^{-1}=\big(\alpha(1),\alpha(2),\alpha(3)\big)\big(\alpha(4),\alpha(5),\alpha(6)\big)\big(\alpha(7),\alpha(8)\big).$$
In order to have $\alpha\beta\alpha^{-1}=\beta$, either $\big(\alpha(1),\alpha(2),\alpha(3)\big)=(1,2,3)$ and $\big(\alpha(4),\alpha(5),\alpha(6)\big)=(4,5,6)$, or vice versa, and $\big(\alpha(7),\alpha(8)\big)=(7,8)$. There are 3 ways to choose $\alpha(1),\alpha(2),\alpha(3)$ so that $\big(\alpha(1),\alpha(2),\alpha(3)\big)=(1,2,3)$, and 3 ways to choose $\alpha(4),\alpha(5),\alpha(6)$ so that $\big(\alpha(4),\alpha(5),\alpha(6)\big)=(4,5,6)$, giving 9 ways to $\alpha(1),\cdots,\alpha(6)$ to have both. There are another 9 ways to choose $\alpha(1),\cdots,\alpha(6)$ so that $\big(\alpha(1),\alpha(2),\alpha(3)\big)=(4,5,6)$ and $\big(\alpha(1),\alpha(2),\alpha(3)\big)=(4,5,6)$, giving a total of 18 ways to select $\alpha(1),\cdots,\alpha(6)$. There are 2 ways to choose $\alpha(7)$ and $\alpha(8)$ to get $\big(\alpha(7),\alpha(8)\big)=(7,8)$. There are also $2!=2$ ways to choose $\alpha(9)$ and $\alpha(10)$. Altogether, there are $18\cdot2\cdot2=72$ ways to choose α so that $\alpha\beta\alpha^{-1}=\beta$.

4: (a) Find the number of cyclic subgroups of A_6.

Solution: We make a table showing the possible forms for $\alpha \in S_6$ and determine which forms lie in A_6:

form of α	$(-1)^\alpha$	$\lvert\alpha\rvert$	# of such α
$(abcdef)$	-1		
$(abcde)$	1	5	$\binom{6}{1}\cdot 4! = 144$
$(abcd)(ef)$	1	4	$\binom{6}{4}\cdot 3! = 90$
$(abcd)$	-1		
$(abc)(def)$	1	3	$5\cdot 4\cdot 2 = 40$
$(abc)(de)$	-1		
(abc)	1	3	$\binom{6}{3}\cdot 2! = 40$
$(ab)(cd)(ef)$	-1		
$(ab)(cd)$	1	2	$\binom{6}{4}\cdot 3 = 45$
(ab)	-1		
(a)	1	1	1

Thus the number of cyclic subgroups is $\frac{144}{\varphi(5)} + \frac{90}{\varphi(4)} + \frac{40+40}{\varphi(3)} + \frac{45}{\varphi(2)} + \frac{1}{\varphi(1)} = \frac{144}{4} + \frac{90}{2} + \frac{80}{2} + \frac{45}{1} + \frac{1}{1} = 167$.

(b) For $n \in \mathbb{Z}^+$, let $P(n)$ be the probability that when one of the $(2n)!$ elements $\sigma \in S_{2n}$ is selected at random and written using cycle notation, one of the cycles has length $\ell > n$. Find $\lim\limits_{n\to\infty} P(n)$.

Solution: First we note that when $\ell > n$, when a permutation $\sigma \in S_{2n}$ is written in cycle notation, it has at most one ℓ-cycle. The number of $\sigma \in S_{2n}$ which, when written in cycle notation, contain one (hence only one) ℓ-cycle, is equal to $\binom{2n}{\ell}(\ell-1)!\cdot(n-\ell)! = \frac{(2n)!}{\ell}$. The total number of elements $\sigma \in S_{2n}$ is equal to $(2n)!$, so we have

$$P(n) = \frac{\frac{(2n)!}{n+1} + \frac{(2n)!}{n+2} + \cdots + \frac{(2n)!}{2n}}{(2n)!} = \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} = \sum_{k=1}^{n} \frac{1}{n+k}.$$

Let $f:[1,2]\to\mathbb{R}$ be given by $f(x) = \frac{1}{x}$. Let $X = \{x_0, x_1, \cdots, x_n\}$ be the partition of $[1,2]$ into n-equal sub-intervals, so $x_k = 1 + \frac{k}{n}$ and $\Delta_k = x_k - x_{k-1} = \frac{1}{n}$ for all k. Taking the sample points t_k to be the right endpoints of the sub-intervals, that is letting $t_k = x_k = 1 + \frac{k}{n}$, the resulting Riemann sum for f on X is

$$S_n = \sum_{k=1}^{n} f(t_k)\Delta_k x = \sum_{k=1}^{n} \frac{1}{1+\frac{k}{n}}\cdot\frac{1}{n} = \sum_{k=1}^{n}\frac{1}{n+k} = P(n).$$

Since f is continuous, hence Riemann integrable, on $[1,2]$, we have $\lim\limits_{n\to\infty} S_n = \int_0^1 f(x)\,dx$ and so

$$\lim_{n\to\infty} P(n) = \lim_{n\to\infty} S_n = \int_1^2 \frac{1}{x}\,dx = \Big[\ln x\Big]_1^2 = \ln 2.$$