Partial solutions of Moed.B, Algebraic Structures

(201.1.7031) 04.03.2018 Ben Gurion University

(1) The polynomial $3x^2+5x+1$ is irreducible (as it has no roots in $\mathbb{Q}$). Thus the ideal $(3x^2+5x+1)$ is prime. As $\mathbb{Q}[x]$ is a PID, the ideal is maximal. Therefore the quotient $\mathbb{Q}[x]/(3x^2+5x+1)$ is a field.

(2) (a) We claim that $\mathbb{Z}[1+\sqrt{-7}]$ is not UFD, hence cannot be a Euclidean domain. Indeed, in $\mathbb{Z}[1+\sqrt{-7}]$ one has: $(1+\sqrt{-7})(1-\sqrt{-7})=8=2\cdot 2\cdot 2$. We claim that 2 is irreducible in $\mathbb{Z}[1+\sqrt{-7}]$. Indeed, use the standard norm $N(a+b\sqrt{-7})=\sqrt{a^2+7b^2}$ to get: $(a+b\sqrt{-7})\mid 2$ iff $b=0$ and $a\in\pm1,\pm2$.
On the other hand, neither of $(1+\sqrt{-7})$, $(1-\sqrt{-7})$ is divisible by 2.

(b) Obviously $2\in\sqrt{I}$. Suppose $a+bi\in\sqrt{I}$. We can reduce modulo 2. If a is even then $(2)+(a+bi)=(2)+(bi)$. Similarly for the case of b even. Therefore the only case to check is, whether $\pm1\pm i\in\sqrt{I}$. Note that these elements are related by multiplication by invertibles (by ±1 and by $\pm i$). Thus it is enough to consider just $1+i$. And $(1+i)^2=2i\in I$, hence $1+i\in\sqrt{I}$. Therefore $\sqrt{I}$ is generated by $\{2,\pm1\pm i\}$. Note that this is not a minimal system of generators, as $(1+i)(1-i)=2$. Thus as a minimal system of generators one can take either of $1+i$, $1-i$, $-1+i$, $-1-i$.

(3) (a) Solution 1. We look for the decomposition $g=xy$ in the form $x=g^a$, $y=g^b$. Then the exponents must satisfy: $a+b=1$, $as\mid st$, $at\mid st$. Thus $a=t\tilde{a}$ and $b=s\tilde{b}$, with $t\tilde{a}+s\tilde{b}=1$. And this later condition is resolvable as s,t are coprime. This gives the needed decomposition.

Solution 2. Consider the subgroup $\langle g\rangle$ of G. By the assumptions: $\langle g\rangle\approx\mathbb{Z}/st\mathbb{Z}\overset{gcd(s,t)=1}{\approx}\mathbb{Z}/s\mathbb{Z}\times\mathbb{Z}/t\mathbb{Z}$. Fix some generators, $<a_s>=\mathbb{Z}/s\mathbb{Z}$ and $<a_t>=\mathbb{Z}/t\mathbb{Z}$. Then the element $a_s\cdot a_t$ generates the whole $\mathbb{Z}/st\mathbb{Z}$, being of order st. Therefore $g=(a_sa_t)^n$, for some $n\in\mathbb{N}$. Thus $g=(a_s)^n\cdot(a_t)^n$ is the needed decomposition. Note that $ord(a^n_s)=s$ and $ord(a^n_t)=t$, because $gcd(n,s)=1=gcd(n,t)$.

(b) Suppose there are two such decompositions, $g=x_1y_1=x_2y_2$. Then $y^s_2=g^s=y^s_1$ and $x^t_2=g^t=x^t_1$. As $gcd(s,t)=1$ there exists the presentation $s\cdot s^\vee+t\cdot t^\vee=1$. Thus we get $y_2^{s\cdot s^\vee}=y_1^{s\cdot s^\vee}$. As $y^t_2=1=y^t_1$ we get: $y_2=y_1$. And similarly $x_2=x_1$.

(4) Denote by $R^\times$ the subset of invertible elements of R, thus $R^\times$ is a group. We prove: $Up/Up^{(1)}\xrightarrow{\sim}(R^\times)^n$.
proof: Note, if $A\in Up$ then all the diagonal entries of A belong to $R^\times$. Consider the map $Up/Up^{(1)}\to\underbrace{R^\times\times\cdots\times R^\times}_{n}$ defined by $A\cdot Up^{(1)}\to(a_{11},\dots,a_{nn})$. This map is well defined, as multiplying by elements of $Up^{(1)}$ does not change the diagonal. This map is multiplicative. This map is surjective.
To check that the map is injective we prove: any element of $Up/Up^{(1)}$ has a diagonal representative. In other words, for any $A\in Up$ exists $B\in Up^{(1)}$ such that AB is a diagonal matrix. It is simpler to make this transition by steps. Take $B_1=\begin{bmatrix}1&-\frac{a_{12}}{a_{11}}&0&\cdot\\0&1&-\frac{a_{23}}{a_2}&0\\\dots&\dots&\dots&\\\dots&\dots&\dots&1\end{bmatrix}$. Then AB_1 has zeros in all the entries $(i,i+1)$. Now take $B_2=\begin{bmatrix}1&0&-\frac{a_{13}}{a_{11}}&0&\cdot\\0&1&0&-\frac{a_{24}}{a_2}&0\\\dots&\dots&\dots&&\\\dots&\dots&\dots&1&\end{bmatrix}$. Then AB_1B_2 has zeros in all the entries $\{(i,i+1)\}$, $\{(i,i+2)\}$. And so on.
Summarizing, we have constructed a homomorphism of groups, which is injective and surjective, hence an isomorphism.

(5) Recall that over a PID any submodule of a free module is free. Therefore M is free and minimally generated by 3 elements. Thus $rank(M)=3$.

(6) Fix the cardinalities: $|G|=p^n\cdot m$, $|K|=p^n$, $|H|=p^l\cdot\tilde{m}$, for some $l\le n$ and some $\tilde{m}\mid m$. Apply the standard formula $|H\cdot K|\cdot|H\cap K|=|H|\cdot|K|$. Note that $H\cdot K\le G$, thus $|H\cdot K|=p^{\tilde{n}}m'$ for some $\tilde{n}\le n$ and $m'\mid m$. Thus we get: $|H\cap K|=\frac{p^l\tilde{m}p^n}{p^{\tilde{n}}m'}$. We must have $\tilde{m}=m'$, as $H\cap K\le K$, and we must have $l+n-\tilde{n}\le l$, as $H\cap K\le H$. Therefore $n=\tilde{n}$ and we get: $|H\cap K|=p^l$, hence $H\cap K\in Syl_p(H)$.